CSIS Public Report

2025

Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

Canada

ISSN: 1495-0138

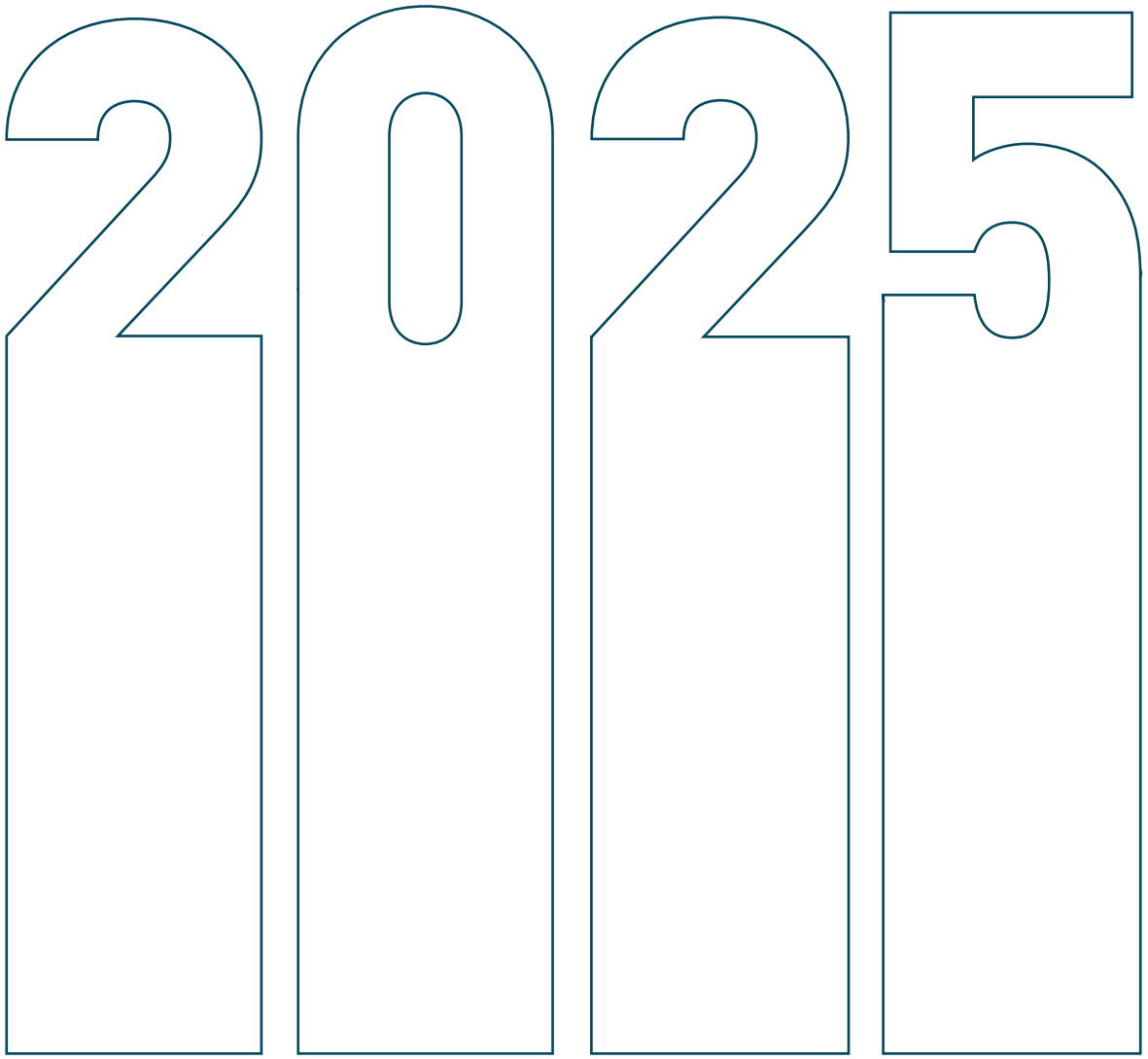
Catalogue number: PS71E-PDF

Published in March 2026

www.canada.ca/CSIS

Aussi disponible en français sous le titre : *Rapport public du SCRS 2025*

CSIS Public Report



Land acknowledgement

The Canadian Security Intelligence Service acknowledges that its 2025 Public Report was written and published on the traditional and unceded territory of the Algonquin Anishinaabeg People.

Table of contents

Message from the Director

Year in review: Adapting to a changing environment

The year 2025 has been one of turbulence for Canada, as it has for many countries in a less certain world. As the Government of Canada navigates increasing geopolitical and security challenges, the Canadian Security Intelligence Service (CSIS) is playing an essential role in protecting national security and providing an intelligence advantage. In our 41-year history, our role has never been more critical.

This year's Public Report reflects the complexity of Canada's current national security environment. It highlights the impact of the demands on us and how we continue to meet the ever-growing challenges facing Canada.

While CSIS is often limited in what it can say publicly, it is my hope that this report strikes the right balance. Our goal is to be accurate, clear, and forthcoming while protecting the information that must remain secret to preserve the integrity of our operations. In a world where diplomacy and engagement are ever more important to our country's security and prosperity, we will increasingly seek to resolve national security issues by working with foreign agencies who seek to defend our common interests, and by engaging and confronting foreign agencies who act against them. We will continue to collect intelligence, give advice, take action to protect Canada, and inform Canadians when it is in their interest. Even when we cannot speak about the actions we take and the information we hold, we remain accountable to Parliament, and under constant review by agencies who validate that our activities are in the best interests of Canada and Canadians.

Looking back, 2025 was full of major achievements and stark reminders. We achieved a number of counterterrorism successes that led to law enforcement action, including the arrests of Hide & Stalk members in Québec, and of a minor who intended to violently target Jewish people and police in Montréal. This report highlights examples of the progress we made in counterintelligence and counter-foreign interference efforts, how we countered life-threatening transnational repression, and how we prevented cyber intrusions by foreign states. Importantly, we also provided critical intelligence and advice to support Canada's security as the Government pursued an ambitious economic growth and diversification agenda.

In 2025, we also took important strides to invest in our capabilities and to reprioritize our work around initiatives that drive the greatest value and impact. We received focused funding in Budget 2025, including $60 million to support Canada's defence capabilities and increase our direct intelligence support to the North Atlantic Treaty Organization (NATO). The Budget also provided $25.7 million to CSIS and the Royal Canadian Mounted Police (RCMP) to support national security safeguards in the *Consumer-Driven Banking Act*.

Budget 2025 also required that federal organizations find annual savings as a result of the Comprehensive Expenditure Review (CER), and CSIS was not exempt from that exercise. While we developed options to reduce our budget by up to 15%, the Government chose to set CSIS' annual savings target at just 2%, aligned with the targets of some of our intelligence, defence, and law enforcement partners. This means finding savings of $14.4M on an ongoing basis starting in 2026. CSIS will achieve these savings by finding efficiencies in the way we work, reducing the number of executive positions, and adjusting existing programs rather than through any reduction in our highly specialized and security-vetted workforce.

Throughout 2025, we continued to build new bilateral and multilateral relationships and deepen our international partnerships. Our Five Eyes alliance remains strong, but we have found opportunity and advantage in deepening our work with regional partners in Europe, the Indo-Pacific, the Middle East, and elsewhere. Our many trusted intelligence relationships around the globe allow us to cooperate to defend shared interests, and to develop greater, more trusted alliances in service of our broader national interests. While not all of the foreign partners we engage with share all of the same values and interests as Canada, we work with them when our interests align and engage with them candidly to advance Canada's interests when they do not. As we move into 2026, all of these efforts and more will be needed to build a more sovereign and resilient Canada.

Within CSIS, we focused on developing the leadership, skills, and workplace environment necessary for us to be at our best. Setting clear expectations and accountability for executives, addressing workplace conduct issues, and building trust across all levels and branches within CSIS through honest and direct engagement were areas of focus for me personally, and for my senior executive team. We appointed the first CSIS Ombuds and published our first annual report on misconduct and wrongdoing, which will each enable the organization to better address workplace issues transparently, ensuring that all within CSIS are held accountable for their obligation to foster an inclusive, engaged, positive, and supportive workplace. Our employees dedicate themselves to the service of their country and, more than ever, Canadians need them to work at their full potential—something that is only possible when they feel able to come to work as they are and contribute at their best.

As in previous years, this report shares details about what we have seen and what we have done over the last year. It is intended to arm Canadians with a better understanding of their national security context and the work we do to keep them safe, secure and prosperous. The examples shared about what we have seen are provided to help Canadians be more resilient against threats and to make more informed decisions. As Canadians read it, I hope that they also find reassurance that CSIS, and the rest of Canada's security and intelligence community, is here and continues to work tirelessly in their service.

Dan Rogers
Director, Canadian Security Intelligence Service

National security in 2025

January

- Publication of the Final Report from the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions

February

- Government of Canada lists seven transnational criminal organizations as terrorist entities: Cártel del Golfo, Cártel de Sinaloa, La Familia Michoacana, Cárteles Unidos, La Mara Salvatrucha, Tren de Aragua, and Cártel de Jalisco Nueva Generación

March

- Man from Winnipeg is charged with three terrorism-related offences in relation to nihilistic violent extremism

Image source: Reuters

Listed terrorist entities

Cartels, Bishnoi Gang, 764, Maniac Murder Cult, Terrorgram Collective, Islamic State-Mozambique.


Image source: Reuters

April

- 45th General Election
- CSIS chairs the Security and Intelligence Threats to Elections Task Force. The *Retrospective Report on the 45th General Election* findings state that while foreign attempts to undermine the election were detected, the Critical Election Incident Public Protocol Panel assessed that none of the incidents detected had a material impact on Canadians' ability to have a free and fair election

May

- The Honourable Gary Anandasangaree, P.C., K.C., M.P., becomes the new Minister of Public Safety

June

- 40th anniversary of the Air India attack, the deadliest terrorist attack in Canadian history that claimed 329 lives

July

- Woman from Montréal pleads guilty and becomes the first person to be convicted of providing support to a terrorist entity, namely the Islamic State of Iraq and Syria (ISIS), through family support as a spouse
- Four members of Hide & Stalk are arrested and face weapons-related charges. Three of them are also charged with facilitating terrorist activity
- Launch of the CSIS Ombuds Office
- Multinational joint statement on Iranian State threat activity in Europe and North America
- Publication of the first annual *Addressing Misconduct and Wrongdoing at CSIS* report


Image source: The Canadian Press/Ethan Cairns

August

- CSIS Director participates in the Canadian Institute for Arctic Security Latitude conference in Haines Junction, Yukon
- Montréal minor arrested and charged with terrorism offences for intending to carry out at least one attack on behalf of the Islamic State

September

- Government of Canada lists Lawrence Bishnoi Gang as a terrorist entity
- CSIS issues an alert: Safeguarding Western Tech Startups: Exploitation of International Pitch Competitions
- Publication of the National Security and Intelligence Committee of Parliamentarians (NSICOP) *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations*
- Neo-Nazi propagandist known as “Dark Foreigner” is sentenced to 10 years in prison for three terrorism-related offences

October

- Trial of a former Hydro-Québec employee for economic espionage
- A founding member of the Terrorgram Collective pleads guilty to three terrorism-related offences

November

- CSIS Director’s first annual speech on threats to safety and security in Canada

December

- Government of Canada lists four new terrorist entities: 764, Maniac Murder Cult, Terrorgram Collective, and Islamic State-Mozambique (ISIS affiliate)
- A Canadian Armed Forces member is arrested and charged in joint police operation into foreign interference and security of information


Image source: RCMP

Image source: Reuters

Highlights

Intelligence reports

In 2025, CSIS produced
1,518 intelligence products

Threat reduction measures (TRMs)

In 2025, CSIS conducted

- **1** warranted TRM
- **15** non-warranted TRMs

Security screening

Government Screening Program

- Requests received in 2025: **129,130**
- Requests completed in 2025: **129,740**

*This difference in number is a result of catching up on the inventory.

Immigration and Citizenship Screening Program

- Referrals received in 2025: **438,600**
- Referrals completed in 2025: **427,100**

Investment Canada Act (ICA)

- ICA notifications screened in 2025 for national security concerns: **1,106**

CSIS partnerships

Domestic arrangements

- **86** arrangements

Foreign arrangements

- **323** arrangements in 158 countries and territories

Warrants and judicial authorizations

obtained in 2025

- **100** warrants
- **15** court orders
- **7** assistance orders
- **1** production order

Access to information and privacy

For 2025, the on-time compliance rates stood at

- **62%** for *Access to Information Act* requests
- **43%** for *Privacy Act* requests from Canadians only
- **14%** for all *Privacy Act* requests*

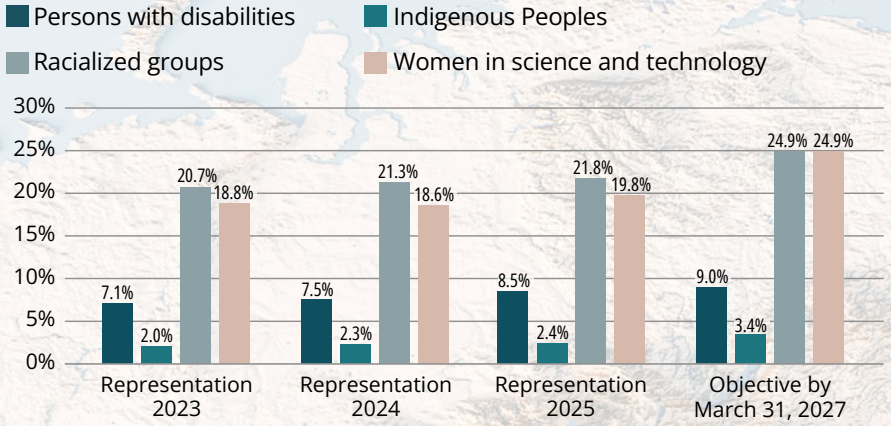
*Approximately 90% of all *Privacy Act* requests relate to individuals seeking information on the status of their immigration files.

Number of reviews by NSIRA and NSICOP

Ongoing reviews: **30**
Completed reviews: **8**
Requests for information: **71**

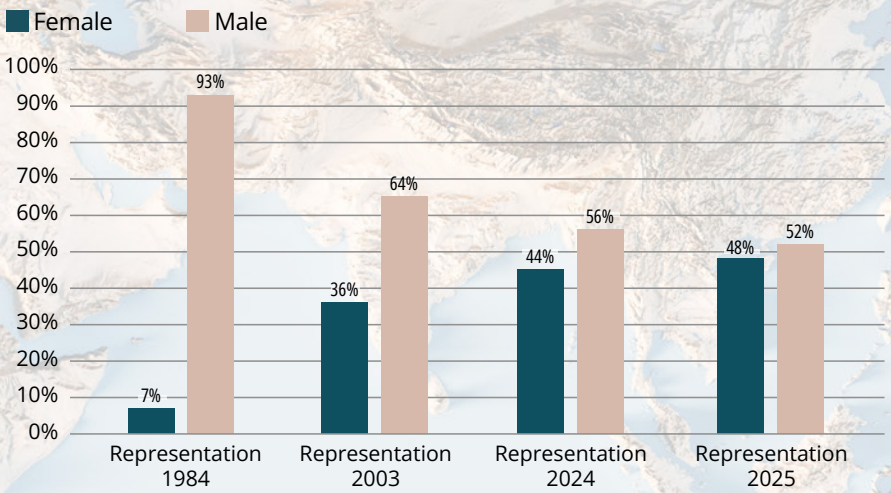
Human resources

Employee demographics

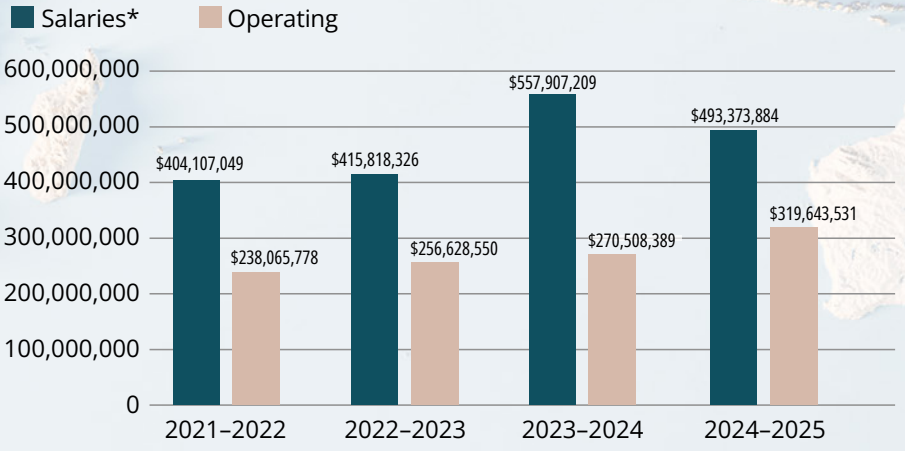


Note: The statistics included in the above table exclude the Director of CSIS, casual employees and students.

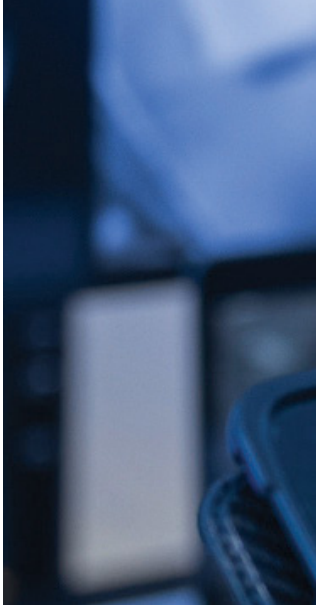
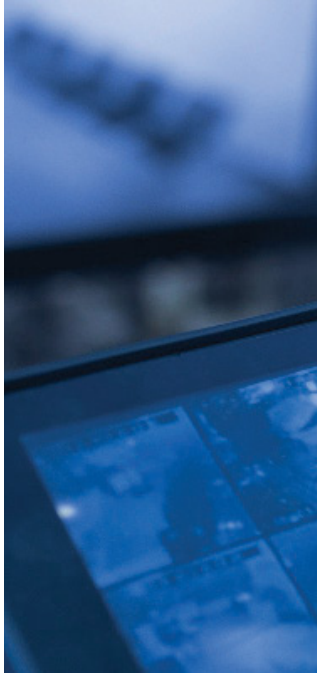
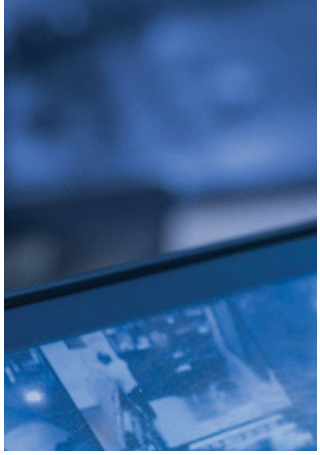
Intelligence officer demographics



Expenditures



*Salary costs include employee benefits payments.


Operations and analysis

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.

In 2025, CSIS developed guidance on the type and amount of risk the organization takes to deliver on its mission to protect Canada's prosperity, national security interests, and the safety of Canadians. In some circumstances, a more flexible and open approach to taking justified risks is appropriate, and in others, CSIS seeks to avoid risk and maintain a strong control environment.

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 Integrated Threat Assessment Centre (ITAC) assessments that inform the Government of Canada's decisions and actions relating to the terrorism threat.

Threat reduction measures

Since 2015, CSIS has had the authority to undertake threat reduction measures (TRMs). 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.

TRMs generally fall into three categories:

- 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 2025, CSIS conducted 1 warranted and 15 non-warranted TRMs.

Foreign interference and espionage

Foreign interference and espionage activities by state actors in Canada continue, despite an increased public conversation on these threats. Foreign states continue attempts to advance their interests in ways that are harmful to Canada's national security, social cohesion, and sovereignty. 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.

Foreign interference includes activities that are, as defined in the CSIS Act, detrimental to the interests of Canada and are clandestine or deceptive, or involve a threat to any person. Foreign interference undermines Canada's democratic institutions, stifles public discourse, erodes trust in government, and can involve intimidation or coercion of members of ethnic, religious, and cultural communities in Canada.

In 2025, the main perpetrators of foreign interference and espionage against Canada remained the People's Republic of China (PRC), India, the Russian Federation, the Islamic Republic of Iran, and Pakistan. However, with shifting geopolitical realities and an increasingly multipolar global environment, these were not the only foreign states that sought to interfere in Canada. During the past year, a number of states, their intelligence services, and other affiliated organizations engaged in foreign interference and espionage activities to advance their objectives, while undermining Canada's national security, values, and economic prosperity.

Foreign actors undertake various activities to increase their influence within Canada, some of which are clandestine, deceptive or threatening and cross the line from legitimate diplomatic engagement to interference.

Threat actors target and cultivate covert relationships with current and former Canadian politicians, journalists, public servants, academics and community members. The goal is to influence Canadian decision-makers to align with positions, narratives, and policies that promote a positive image of their country. These actions fall outside traditional diplomatic relationship building.

When conducting foreign interference and espionage, foreign states 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.

They use proxies to conduct social and political interference activities, including media manipulation and disinformation through various channels (both social media and traditional media). Some communities in Canada are particularly at risk of being unduly influenced to support these actors' objectives, or harassed and intimidated by them to silence perceived threats to the foreign state.

Historically, India has cultivated covert relationships with Canadian politicians, journalists, and members of the Indo-Canadian community, to exert its influence and advance its interests. This has included transnational repression (TNR) activities, such as surveillance and other coercive tactics meant to suppress criticism of the Government of India and create fear in the community. Given the presence in Canada of supporters of the Khalistan separatist movement, Canada must remain vigilant regarding potential TNR activities. India acts to counter perceived threats to its domestic stability, including Khalistan separatism. In Canada, advocacy for Khalistan separatism is lawful political activity.

Iran remains an aggressive perpetrator of TNR. Following the interruption of several Iranian plots in 2025, Canada and 13 other countries issued a joint communiqué in July 2025 condemning "the attempts of Iranian intelligence services to kill, kidnap, and harass people in Europe and North America in clear violation of our sovereignty."

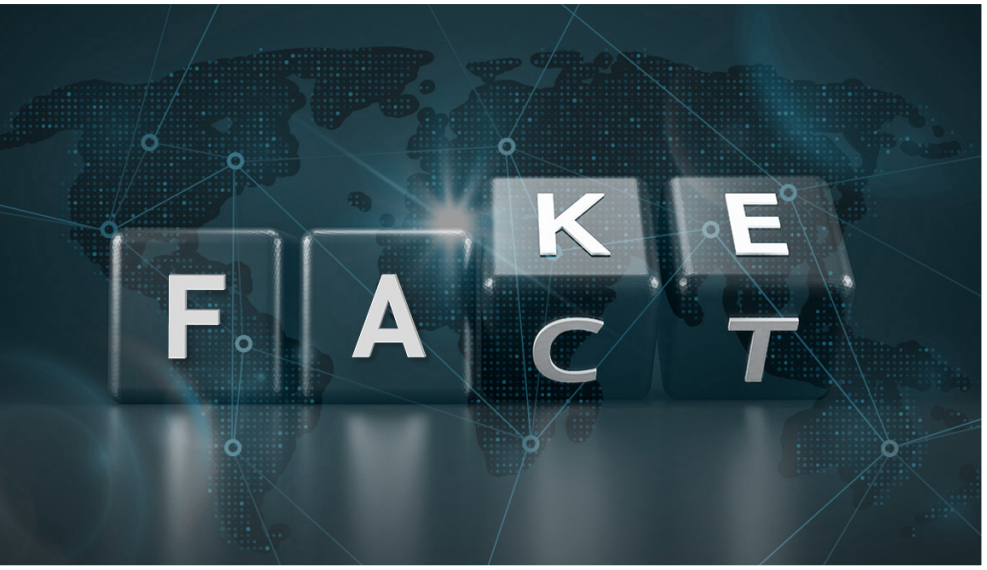
For example, in July 2025, alleged "hacktivist" group "Handala Hack Team" claimed to have hacked the "systems, servers, and communication infrastructure" of Iran International, a Farsi-language satellite television channel with English, Arabic, and Farsi online news operations based in London, United Kingdom (UK), and Washington, D.C. Iran International maintains a highly critical reporting line vis-à-vis the Iranian regime, and several online security and threat intelligence firms have linked the Handala Hack Team to the Iranian Intelligence Services. The Handala Hack Team subsequently doxed* several Iran International-linked journalists, including a Canadian resident. The Canadian's photos, provincial driver's license, permanent resident card, and Iranian passport details were released on the internet and social media platforms. The hacktivist group reproached the Canadian for, among other things, their promotion of 2SLGBTQIA+ issues in Iran.

Within days of being doxed, the Canadian resident began receiving hundreds of violent threats, and their family in Iran was harassed by the authorities. The objective of this harassment—whether in Canada or elsewhere—is to silence these journalists and compel them to stop working for a media outlet that is highly critical of the Government of Iran. CSIS worked with domestic and foreign partners to respond to this incident.

On September 12, 2025, the members of the G7 Rapid Response Mechanism and associate members (Australia, the Netherlands, New Zealand, and Sweden) issued another communiqué drawing attention to and condemning Iranian TNR activities, including Iran's lethal plotting in Europe and North America.

CSIS assesses that these foreign actors will continue to use proxies, such as individuals involved with transnational organized crime networks, to target perceived enemies living in foreign countries, including Canada. To address this evolving threat landscape, CSIS is adapting its tradecraft and strengthening its investigative efforts in relation to TNR conducted by these foreign actors. CSIS will work with its counterparts directly to address these concerns.

*Doxing or doxxing is the act of publishing private or identifying information about an individual online, without his or her permission. Doxing is an example of malinformation, which is accurate information shared publicly to cause harm.



Misinformation

is false, misleading or inaccurate information that is spread unintentionally.

Disinformation

is false or misleading information created deliberately with a malicious intent to manipulate a narrative. Misinformation becomes disinformation when hostile actors weaponize it for political influence and interference.

Since its 2022 invasion of Ukraine, Russia has been seeking to undermine Canadian support for Ukraine following contributions to global efforts to degrade Russia's military and economic capacity to wage war, including through sanctions. Hostile Russian state actors, and those working on their behalf, have carried out several information and malign influence operations against Canada, exploiting various contentious social topics aimed at discrediting the Government of Canada's position on Ukraine by polarizing segments of both political and public spectrums. As part of this, Russian state-linked actors often hide behind networks of proxies who amplify the Kremlin's messaging or generate their own versions using powerful new technologies, such as artificial intelligence (AI) and social media. CSIS continues to identify, investigate, and reduce Russia's adaptive and sophisticated disinformation methods in support of the Government of Canada's broader efforts to protect Canadians against the harmful effects of misinformation and hostile disinformation campaigns.

To mitigate foreign interference threats, CSIS continues to provide information to elected officials at all levels of government, including sergeants-at-arms and provincial security officials, on the nature of the threats and various ways they and their staff can protect themselves, as well as to ethnic, religious and cultural communities and organizations. CSIS does this both independently, and in concert with other government departments. In 2025, CSIS also used its threat reduction mandate and undertook covert activities to disrupt and degrade foreign actor-affiliated networks engaged in foreign influenced activities against Canadian interests. Based on credible evidence, CSIS has had to reprioritize its operations to counter the actions of foreign intelligence services and their proxies who have targeted individuals they perceive as threats. In more than one case, this involved detecting, investigating, and disrupting potentially lethal threats against individuals in Canada.

Transnational repression

Transnational repression (TNR) takes place when foreign governments, or those acting on their behalf, reach beyond their borders to harass, threaten or harm individuals or groups to advance their interests or to silence criticism and dissent. TNR activities typically target political dissidents, human rights and democracy defenders, and ethnic, religious and cultural communities. TNR also increasingly targets the people and organizations that defend the victims. This can include activists, international students and scholars, lawyers and doctors, as well as journalists.

Hostile state actors use a variety of tactics to try to extend their reach into Canada:

- **Physical intimidation and violence:** Monitoring and surveillance, vandalism, threats, abduction, assault, or attempted murder. Actors can use coercion or assault as punishment or to influence opinion, and hostile state actors sometimes hire organized crime groups or proxies for this.
- **Threats against overseas relatives and other connections:** Threats against relatives and acquaintances in the home country, to relay messages or force an action in Canada. This creates a sense of vulnerability, as close relations abroad may be victim to the laws and regulations of a non-democratic country.
- **Legal manipulation/lawfare:** Foreign states abusing legal mechanisms for coercive purposes, like libel suits, extradition agreements, bounties for information on individuals, Interpol red notices, imposing sanctions, forced repatriations, and refusing visa applications for personal or professional travel.
- **Community ostracism:** Rejection from community associations, use of labels such as "extremist" or "traitor," or loss of access to social events and employment opportunities.
- **Malicious digital activity:** Hacking, cyberbullying, targeted deepfakes, online defamation and disinformation, doxing, or threatening online messages.
- **Extortion:** Using threats, intimidation, or violence to force someone to give up something of value, such as money, property, or services, against their will. The threat doesn't have to be physical; it can also involve damaging someone's reputation, business, or personal relationships.

Espionage activity, as well as attempted sabotage, also continued this past year. Working closely with domestic partners, as well as trusted foreign governments, CSIS continues to identify members of the Russian intelligence community and those working on their behalf to disrupt their efforts. Mitigations can range from denying certain actors' entry into Canada to working with foreign partners to undermine the activities of Russian agents operating in Europe and elsewhere. These activities pose a direct threat to the security of Canada, as well as several of our North Atlantic Treaty Organization (NATO) allies and non-NATO partners. Russia is likely to continue engaging in hostile behaviour for the foreseeable future.

The Russian state directs or supports the combined use of a range of hostile activities—commonly referred to as hybrid warfare—including acts of espionage, sabotage, and foreign influence activities. Over the past year, Russia has consistently demonstrated that it is willing to engage in aggressive and covert activities, while accepting the risk of collateral damage in applying its evolving tactics. These ongoing activities, representing Russia's asymmetrical response to Western assistance to Ukraine, are an example of Russia's violations of the international norms of conduct. As a NATO member that actively supports Ukraine, Canada is considered a legitimate target and CSIS continues to identify and investigate, often in collaboration with allied countries, Russia's adaptive and sophisticated threat activities.

Canada is a geostrategically important country for foreign actors and is home to cutting-edge technology, a robust economy, and an abundance of critical minerals. This makes Canada an attractive target for foreign intelligence services who will undertake espionage activities to advance their own strategic interest by gathering a range of information, including privileged and sensitive information, as well as intellectually protected information, like patents. Acts of foreign espionage represent a long-term threat to Canada's economy and our collective prosperity.

CSIS continued to observe an evolution of PRC espionage tactics targeting the Canadian public, private, and academic sectors. In 2025, the PRC Intelligence Services (PRCIS), both civilian and military, started posting job ads via cover companies to an expanding number of online job marketing sites to recruit Canadians with access to proprietary or classified information. Rather than only identifying potential targets of recruitment, this approach allows the PRCIS to engage with a much larger number of Canadians, who unknowingly apply to work for a hostile intelligence service. The PRCIS takes advantage of the financial difficulties and career ambitions that drive some applicants to apply to these job postings. Although most Canadians who apply to these jobs have no direct access to privileged Government of Canada information, providing their resumes and other personal information to the PRCIS may facilitate future targeting of an applicant's close contacts who could have direct or indirect access to such information.

In 2025, CSIS released security alerts highlighting PRCIS tradecraft to raise public awareness of these evolving PRCIS tactics. An espionage alert was released on a PRCIS-affiliated individual targeting Canada's academic research community to disrupt the threat posed by this individual. Over the past two years, CSIS took measures, in coordination with Public Safety Canada and other Government of Canada partners, to successively disrupt the PRC recruitment of current and former Canadian military personnel to train PRC military aviators.

45th General Election

Foreign interference is a persistent threat to Canada and to the conduct of our democratic institutions inside and outside of election cycles. Election periods provide an opportunity for increased and focused efforts by foreign states.

In 2025, CSIS chaired the Security and Intelligence Threats to Elections Task Force (SITE TF), which, in line with its mandate, conducted enhanced monitoring of foreign interference and violent extremism threats directed at democratic processes in Canada. For 2025, this included monitoring and reporting on the Liberal Party of Canada leadership campaign, the 45th General Election (GE45), and the by-election in Battle River—Crowfoot.

CSIS participated in the development of the SITE After Action Report for GE45. This report provided an overview of the SITE TF's expected threat landscape for GE45, its observations of threat activities targeting the election, and the actions it undertook following meetings of the Critical Election Incident Public Protocol Panel ("the Panel").

While none of the incidents observed by the SITE TF during GE45 were assessed by the Panel to have had a material impact on Canada's ability to have a free and fair election, CSIS continues to assess that attempts to interfere in electoral processes at all levels by foreign states, whether directly or through proxies, remain a threat to Canada's democratic processes and public trust in the electoral system.

Threats to public officials are becoming more regular and complex. Government of Canada departments and agencies, in collaboration with domestic and international partners and police services, work to ensure the safety and security of those who choose to take on the important role of political office. Between elections, the SITE TF continues to meet to share information and best practices, and to preserve institutional readiness for general elections and by-elections.

In addition, CSIS regularly briefs elected officials on foreign interference threats, including upon request and when CSIS becomes aware of potential threats against them or their families.

Violent extremism

Violent extremism, motivated by an increasingly diverse range of beliefs and convictions, continues to pose a significant threat to Canada's national security and remains a critical operational priority for CSIS. Numerous factors, including the availability of violent extremist-created content on the internet, personalized and hybridized worldviews, and domestic and international events have contributed to create an environment where more Canadians are radicalizing and mobilizing to violence.

While RCMP and CSIS mandates are distinct, both agencies share an important goal: to address national security threats and ensure public safety, which is especially important to combat violent extremism. Given CSIS' mandate, it will often have visibility on the emergence of a threat ahead of the RCMP. Leveraging the One Vision 3.0 framework, CSIS and the RCMP work hand-in-hand to determine the most effective approach to address a threat. If a criminal investigation is undertaken, both organizations will collaborate to reduce the risk of sensitive CSIS information being subject to law enforcement's disclosure obligation.

Over the past year, CSIS and Integrated Threat Assessment Centre assessments attested to the complexity of the threat environment and did not provide any indication that the national security threat posed by ideologically motivated violent extremism (IMVE) and religiously motivated violent extremism (RMVE) will decline in the short or medium term. A diverse range of ideologies and motivations were present, making it harder to distinguish hate from extremism. Threats were characterized by a mix of factors, including xenophobia, accelerationism, nihilism, misogyny, and extreme interpretations of religion. In addition, various drivers impacted the conditions for extremism, ranging from degrading social cohesion to permissive foreign environments, as well as advanced and emerging technologies. Security and intelligence partners continued to work together to address challenges posed by violent extremism. CSIS sought to stay ahead of the curve in terms of understanding the drivers of mobilization to violence and the tactics used by extremists and violent extremist organizations, which is becoming increasingly difficult in the current threat environment.

In 2025, CSIS observed an overlap in content, aesthetics, conspiracy theories and grievance narratives, including those that are anti-liberal, anti-2SLGBTQIA+, antisemitic, and Islamophobic between IMVE and RMVE. On occasion, similar violent content is consumed, including gore sites, jihadi beheading videos, and attack manuals. This shared interest suggests there may be a greater interest in the "how" to commit acts of violence rather than the "why." Violent extremists with these different ideologies are increasingly finding common causes. They find inspiration and motivation in the events and trends that polarize society or cause them to lose hope for the future. They easily access and amplify content online that radicalizes them and reinforces their view that violence is justified to achieve their extremist goals.

Eroding social cohesion, increasing polarization, and significant global events provide fertile ground for radicalization to violence. Many who turn to violence radicalize exclusively online—often without direction from others. They use technology to do so secretly and anonymously, seriously challenging the ability of CSIS investigators to keep pace, and to identify and prevent acts of violence.

Only a small number of youth or adults with extreme views resort to violence. When they do, the consequences are devastating. Since 2014, there have been 20 violent extremist attacks in Canada resulting in 29 deaths, and at least 60 victims injured. These numbers would have been higher if not for disruptive actions taken by CSIS and our law enforcement partners. Since 2022, CSIS has been involved in the disruption of at least 24 violent extremist actions, each resulting in arrests or the imposition of a terrorism peace bond.

Addressing violent extremism requires a whole-of-society approach, including strong and ongoing collaboration with intelligence and law enforcement partners. Countering violent extremism remains a significant portion of CSIS' work.

Religiously motivated violent extremism

In Canada, the RMVE threat has been particularly concerning. Internationally, several key developments are shaping a complex global terrorism environment that is increasingly permissive for violent extremists. These include reduced international pressure on terrorist actors, increased DAESH external operations efforts, increased online and youth radicalization, and the ongoing Israel-HAMAS conflict.

The RMVE threat, and the threat of a domestic lone-actor attack in Canada, increased significantly since the beginning of the Israel-HAMAS conflict. In 2025, at least seven of CSIS' priority investigations involving mobilization to violence have been assessed as motivated by this conflict in whole or in part. This conflict has also fuelled violent extremist organization narratives, and has the potential to inspire a new generation of extremists. The conflict will likely continue to motivate some extremists in the near term, but understanding the true impact of the conflict will only be clear over time.

Globally, DAESH remains the most significant threat to Western interests, with its enduring objective to seize territory to establish a caliphate. That said, the Al Qaeda threat has not gone away. CSIS has witnessed a rise in Al Qaeda associated threat activity aimed at the West, including Canada. DAESH also continues to draw upon multiple international issues to inspire and enable attack planning in the West. In the near term, DAESH will continue to attempt to influence supporters—particularly from Syria, Afghanistan and Pakistan—to plan attacks on targets related to world events, and enable them to do so, while Al Qaeda will continue efforts to reconstitute itself in permissive territories, including through the rise of the Islamic State in Somalia and increased Al-Shabaab terrorism activities in North Africa.

In 2025, two returned Canadian extremist travellers (CETs) were convicted of participating in the activities of a terrorist group (DAESH). One of these represented the first ever conviction of a returned female CET in Canada and represents the sustained efforts of over a decade of DAESH-CET investigations by CSIS and the RCMP.

Developments in Syria brought into question the future status of CETs detained in prisons controlled by the Syrian Democratic Forces and could expedite timelines associated with their possible repatriation to Canada. Absent of sufficient mitigation measures, CSIS assessed that some of these CETs would likely pose national security and public safety risks.

Antisemitism

Antisemitism continues to persist in Canada, manifesting itself in different ways: vandalism and graffiti, circulation of hate propaganda, intolerant and racist statements, bomb threats to Jewish schools and community centres, etc. Not all hateful behaviour or online posts, including antisemitic speech, constitute threats to the security of Canada as defined in the CSIS Act. However, such hate has, on occasion, motivated individuals to mobilize to violence.

Since 2014, there has been one attack and five disrupted plots targeting Canadian Jewish institutions or interests. This includes the August 2025 arrest of a minor in Montréal who intended to target Jewish people and police.

Ideologically motivated violent extremism

The IMVE landscape is complex, diverse, chaotic, and constantly evolving, which challenges our understanding of the national security threat. Threat actors are progressively driven by a range of often seemingly contradictory grievances and personalized narratives from across the traditional left/right ideological spectrum that are often deeply intertwined with conspiracy theories. Referred to as "salad bar" grievances, they include individuals who form a simplistic, yet dangerous, worldview from differing narratives. The landscape is also transnational in nature, as individuals from around the world gather in online communities to share their grievances, ideas, hatred, and attack plans.

CSIS, international partners, and academics now have a more comprehensive understanding of some types of violence that were previously not considered national security threats. As the boundaries of IMVE continue to expand, a new threat has emerged referred to as nihilistic violent extremism (or NVE), particularly among youth (under 18) and younger adults in Canada.

In 2025, CSIS completed a demographic study of CSIS IMVE subjects of investigations from 2018 to June 2025. While the average age of IMVE subjects has remained largely consistent since 2022 (around 34 years of age), there has since been an increase in youth and those over the age of 48 since, reflecting the diffuse nature of the IMVE landscape. The study also found that these subjects are overwhelmingly male, at 93%.

Islamophobia

Islamophobia—rooted in racism, prejudice, fear, stereotypes, and sometimes outright hostility towards Muslims—can be perpetuated at individual, institutional, and societal levels. Not all hateful behaviour or online posts, such as those relating to Islamophobia, constitute threats to the security of Canada as defined in the CSIS Act. However, they do undermine the safety and dignity of Canadian Muslims and have led to occasions where individuals motivated by such hate have mobilized to violence, in some instances resulting in deaths.

Since 2017, there have been two mass attacks against Muslims in Canada. In January 2017, a shooting at the Islamic Cultural Centre in Québec resulted in the tragic killing of six Quebec Muslim men and 19 wounded. The perpetrator was convicted of several counts of murder and attempted murder. On June 6, 2021, in London, Ontario, a driver of a truck rammed into and killed four members of the same family, and injured a young boy who was orphaned in the attack. The perpetrator, a self-described white nationalist, was convicted of several counts of murder, as well as terrorism. CSIS is aware of increased and credible reporting of Islamophobic hate speech and hate-motivated crimes conducted by individuals in Canada, but did not observe any violent extremist plots targeting the Muslim community in 2025.

Nihilistic violent extremism

Defined as serious violence based on the rejection or negation of traditional moral, religious and social values, NVE promotes the belief that life lacks inherent meaning or purpose. The ultimate objective for followers of NVE is to engage in violent chaos. NVE falls within IMVE—most commonly within the "xenophobic violence" subcategory. CSIS works closely with its security and intelligence partners to better understand the national security elements of emerging NVE threats.

While a portion of the NVE space is considered within CSIS' national security remit, the majority of the NVE space is considered criminal in nature, and below a national security threshold. This includes sextortion, child sexual exploitation, animal torture and bestiality, forced drug use and encouraging/sanctioning suicide, and often involves youth. In March 2025, the RCMP charged a 19-year-old from Winnipeg with three terrorism-related offences for his alleged involvement in the international extremist group known as MKY or "Maniac Murder Cult."

In July 2025, four members of Hide & Stalk, an anti-authority IMVE militia in Québec composed primarily of current and former Canadian Armed Forces members, were arrested after CSIS and RCMP investigations and monitoring. Three of the individuals are now facing terrorism-related charges, the first of their kind against militia members in Canada. The fourth is facing charges including for possession of firearms, prohibited devices and explosives, possession of controlled items under the *Criminal Code* and other federal laws. These arrests came after the RCMP conducted searches on the individuals in January 2024 and seized 16 explosive devices, 83 firearms and accessories, approximately 11,000 rounds of ammunition of various calibres, nearly 130 magazines, four pairs of night vision goggles and military equipment.

While new types of IMVE emerged, others persisted. Militant accelerationism remains persistent across the IMVE landscape and is exemplified in the Terrorgram Collective, a collection of violent neo-Nazi Telegram channels that generate original content and manifestos for online dissemination. In October 2025, a founding member of the Terrorgram Collective, pleaded guilty to three terrorism-related offences in connection with his role in the Collective. CSIS intelligence was instrumental in leading to this outcome. The violent tenets of Terrorgram's content and manifestos have inspired at least three violent attacks in Slovakia, Brazil, and Türkiye, two plots to attack critical infrastructure in the United States (US), and the attempted assassination of a foreign government official in Australia.

In September 2025, a neo-Nazi propagandist known as "Dark Foreigner" was sentenced to 10 years in prison for three terrorism-related offences. His objective was to inspire others to engage in violence through his graphic designs and videos he produced in support of Atomwaffen Division (AWD).

Youth radicalization

In recent years, Canada has seen a growing trend of youth (some as young as 13) involved in select counter-terrorism investigations. Nearly one in ten CSIS terrorism investigations now includes at least one subject of investigation under the age of 18.

CSIS counter-terrorism investigations regularly encounter minors mobilizing to violence. In Canada, there were five minors arrested in 2023, two in 2024, and four in 2025. This includes a Montréal minor who was arrested for allegedly planning an attack on behalf of DAESH and an Edmonton area minor who was arrested for terrorism-related offences related to The COM and 764, a transnational violent online network that targets children and youth across widely accessible online platforms. This trend not only raises concerns about the radicalization of young people, but it also creates difficulties in identifying extremist actors and determining whether their activities pose a genuine threat to national security.

CSIS has identified the prevalence of youth within various online neo-Nazi and NVE ecosystems who create and share violent content, idolize past IMVE attackers, and desensitize one another to serious violence, including through illegal activities. There has also been recent growth in online accelerationist and neo-Nazi groups (including Canadian groups) that link across multiple platforms. These entities (which include youth) self-identify as current incarnations of listed terrorist entities, such as AWD, or appear to be directly inspired by AWD texts and imagery.

The main challenge of RMVE youth radicalization is determining which teen engaging with terrorist materials and violent content online is a genuine threat and could mobilize to violence. Youth can take 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 them with 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.

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, to establish new political systems or entities.

This past year marked the 40th anniversary of the bombing of Air India Flight 182, whose suspects were members of Canada-based Khalistani extremist (CBKE) groups. It remains to this day the deadliest terrorist attack in Canadian history, with 329 people killed, most of them Canadians.

There were no CBKE related attacks in Canada in 2025. Ongoing involvement in violent extremist activities by CBKEs continues to pose a national security threat to Canada and to Canadian interests. Some CBKEs are well connected to Canadian citizens who leverage Canadian institutions to promote their violent extremist agenda and collect funds from unsuspecting community members that are then diverted toward violent activities.

Some Canadians participate in legitimate and peaceful campaigning to support the Khalistan separatist movement. Non-violent advocacy for the creation of a state of Khalistan is not considered

extremism. Only a small group of individuals who use Canada as a base to promote, fundraise, or plan violence primarily in India are considered Khalistani extremists.

CSIS continues to monitor emerging threats and contribute to the Government of Canada terrorist listing process. In 2025, 12 groups were added as a terrorist entity under the *Criminal Code*. They include: transnational criminal organizations, including cartels, Bishnoi Gang, 764, Maniac Murder Cult, Terrorgram Collective, and the Islamic State of Iraq and Syria (ISIS, also known as DAESH) affiliate Islamic State-Mozambique.

Economic and research security

As a trading nation and global leader in the research and technology sector, Canada is a target for states who seek to acquire sensitive research and technology to advance their own strategic political, economic, and military advantage. Threats to economic and research security will likely increase as states look to exploit opportunities for their advantage in a more competitive global economy. For example, state actors, whose entities/individuals are often obfuscated, seek to collaborate with leading Canadian companies and academic institutions through research and collaboration agreements. In turn, this allows them direct access to leading edge intellectual property and know how.

The year 2025 saw significant changes to the global economy. Increased geopolitical tensions have intensified competition, including for new technology, which has led to increased concerns for national security. State actors continue to take advantage of changes to the global economy to find opportunities to advance their interests using a combination of overt and covert means at Canada's expense. CSIS and government partners will continue to take action to protect Canada's national interest.

In early 2025, CSIS delivered briefings, including on foreign interference, to stakeholders in the banking and insurance sectors in support of the Office of the Superintendent of Financial Institutions' (OSFI) enhanced security and integrity mandate. The briefings discussed the national security landscape and aimed to bolster the financial sector's resilience and awareness of evolving and emerging threats and vulnerabilities. This included co-hosting the National Security Threat Forum for Federally Regulated Financial Institutions with the Communications Security Establishment Canada (CSE) and OSFI.

Cryptocurrencies, or virtual assets, while not yet considered mainstream financial instruments in the Canadian financial sector, have become a complex and dynamic market. In doing so, they are also increasing related national security threats in this space. For example, state actors and their proxies are masking their identity by using Western front companies, leveraging the strength of cryptocurrency and its weaknesses, and are using it to enable their threat activities in largely unregulated or under regulated markets globally. CSIS notes that centralized stablecoin issuers introduce an additional risk factor as they could manipulate the market—a potentially powerful tool in the hands of adversaries.

CSIS participated in the Financial Action Task Force (FATF) Mutual Evaluation of Canada, an assessment of the compliance and effectiveness of Canada's anti-money laundering, counter-terrorist financing, and counter-proliferation financing frameworks. As part of its mandate, CSIS supports Canada's adherence to FATF standards by identifying and analyzing terrorist financing, including the examination of emerging trends, patterns, and threats. Through close collaboration with other government departments and agencies, such as the Department of Finance Canada (FIN) and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), CSIS contributes to a nuanced understanding of the Canadian threat landscape, ultimately enhancing the country's ability to protect national security.

Trade and investment

In 2025, CSIS observed certain state actors seeking to exploit Canada's trade and investment relationships to obtain Canadian technologies (and the expertise behind them). They have sought privileged knowledge of Canada's plans, priorities, and intentions for navigating the current geo-strategic and economic environment, including advance knowledge of Canadian policy and regulatory decision-making.

CSIS increased its engagement with other orders of government, the private sector, and with industry to raise their awareness and build resiliency against national security threats. CSIS worked with Canadian businesses to develop the knowledge and tools they need to pursue the opportunities that advance Canada's economic prosperity and national security.

CSIS also began participating in national security reviews of payment service providers (PSPs) under the *Retail Payment Activities Act*—administered by the Bank of Canada (BOC) and coordinated by FIN. Within the scope of the CSIS Act, CSIS advises the BOC and FIN on assessed threats including insider threat, data security, and illicit financing. In addition, CSIS supported the Minister of Finance in assessing national security threats associated with PSPs to help inform the Minister's decision on whether to approve their operations in Canada.

CSIS, in collaboration with members of the Canadian security and intelligence community, also continues to provide Government of Canada policymakers with intelligence to inform their decisions on mitigating national security risks posed by foreign direct investment under the *Investment Canada Act* (ICA). In 2025, CSIS screened 1,106 ICA notifications for potential national security concerns.

Research security

This past year saw the development and protection of emerging and sensitive technologies, such as AI, quantum computing, and biotechnology, which are crucial to Canada's economic security and national sovereignty. The loss of Canadian intellectual property and sensitive technology in these areas weakens the economy and jeopardizes national security, while strengthening the capabilities of threat actors.

Sensitive technology

Canada's Sensitive Technology List identifies eleven broad technology areas that the Government of Canada considers to be sensitive. This list consists of advanced and emerging technologies, such as quantum computing, AI, biotechnology and others. These technologies 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 include 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.

As part of the National Security Guidelines for Research Partnerships and the Policy on Sensitive Technology Research and Affiliations of Concern, CSIS reviews federal research funding for national security concerns. This work supports the Government of Canada's efforts to strengthen research security and ultimately safeguard Canadian research and industry. CSIS engages on a regular basis with universities, academia, research associations, and companies to increase their awareness of threat activities targeting Canada's research sector.

In 2025, CSIS continued to focus on the protection of these Canadian industries—defending against the exploitation of economic activities and research partnerships by states seeking to acquire access to and transfer of sensitive technologies, expertise, data, and other strategic resources. This past year, CSIS worked to identify strengths and vulnerabilities within these sectors. In efforts to harden the environment, CSIS has been advising and engaging with partners to help protect Canadians and Canada's national security.

Through regular engagement and briefings, CSIS aims to provide universities, academics, research associations, and the private sector with tools to protect themselves, their research, and their intellectual property against efforts by threat actors to exploit Canada's research ecosystem.

Secure Innovation Initiative

CSIS and its Five Eyes partners continue to work collaboratively against states who target and steal technology and research from Five Eyes economies. The Secure Innovation Initiative provides the technology sector with a set of cost-effective best practices to companies to better protect their ideas, reputation, and future successes. Businesses in Canada, Australia, New Zealand, the UK, and the US can take advantage of a collection of Secure Innovation resources, guidance, and products.

In 2025, CSIS hosted a successful Secure Innovation workshop, providing Five Eyes partners with an opportunity to share their experiences and grow their strong relationships in the research security space. CSIS will continue to engage with its Five Eyes partners on this important initiative and will seek to release additional resources to assist Canadian 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 disruption and intellectual property theft.

Projects of national importance

In June 2025, the *Building Canada Act* (BCA) came into force, with the aim of facilitating the development and execution of major projects that are deemed to be in Canada's national interest due to their potential to enhance Canada's prosperity, national security, economic security, national defence, and national autonomy.

National security considerations play an important role in the decision-making process to identify projects of national interest and the nature of the support they receive from the federal government. States who seek to advance their interests at the expense of Canada may target public and private sectors working on these projects.

As part of the BCA, the Minister responsible for it must undertake a national security review for all state-owned or foreign investments from hostile countries in any national interest project and the Minister must be satisfied that, with regard to any foreign investments in the project, all necessary measures have been taken to protect national security interests.

CSIS, along with other members of Canada's security and intelligence community, is supporting the Government's efforts by providing intelligence and analysis to help inform decision-making on the national security aspects of projects under consideration. In 2025, CSIS provided briefings and briefing material to the Major Projects Office describing the threat landscape and outlining the potential risks for each project.

CSIS defines threats to the financial sector security as activities that are harmful to Canada's financial institutions and markets, and to the interests of Canada and Canadians in the integrity of their operations. In the financial sector, disruptions caused by malicious actors could result in an erosion of confidence in the resiliency and integrity of Canada's financial sector, harming Canada's economic security.

The growth of financial technology companies and digital currencies (e.g., stablecoins) are recent examples of constant evolution in this sector, which threat actors are often quick to adopt and exploit in their activities. From a strategic perspective, irrespective of the financial instrument in question, threat actors maintain the same intent: the concealment of the movement of financial value to their benefit.

The ingenuity of threat actors creates challenges for the security and intelligence community to detect new tactics, techniques, and procedures. To counter this, CSIS collaborates with partners, including FINTRAC, OSFI, FIN, and the Canadian Revenue Agency, to collect, analyze and advise on national security threats.

Critical minerals

The intensifying global competition for critical minerals continues to pose significant risks to Canada's national security and prosperity. Canada's dependence on other states, including the PRC, for supply of these essential resources threatens to undermine our access to the critical minerals needed for emerging technologies and defence applications. CSIS is working to address this threat by building awareness of the risks to Canada's critical mineral industries and promoting resilience. CSIS' intelligence and advice help support Canada's efforts to diversify its trade partnerships and secure reliable market-based access to critical minerals. By leveraging our intelligence and international networks, CSIS aims to safeguard Canada's position as a trusted supplier of critical minerals, ensuring the long-term prosperity and security of our country and its allies.

Canada's Arctic

The Arctic is a region of increasing geo-strategic competition. Melting sea ice is increasing accessibility, which in turn is increasing activity of both Arctic and non-Arctic states in the region, and amplifying sovereignty and security concerns. Foreign interest in Canada's Arctic continues to grow due to the economic and strategic opportunities it presents, including the opening up of new trade routes, the rich critical mineral resources present, and opportunities to conduct valuable scientific research.

As Canada's Arctic becomes more accessible, the growing political and economic interest in land and seascapes is leading to more intensive industrial activities. Foreign states, such as Russia and the PRC, also have a significant intelligence interest in our Arctic and those who influence or develop its economic or strategic potential. This includes access to the region's natural resources, such as oil, gas, and minerals. This past year, CSIS has seen certain states look to establish and maintain commercial or scientific operations (i.e., a physical presence) in Canada to provide them with a platform or cover to engage in threat activities against Canada and Canadians.

For example, state actors are seeking to partner with companies, governments, and communities to invest in critical infrastructure (e.g., ports, communications, energy networks) and natural resources to secure long-term influence in the region. This influence could be exploited to advance geopolitical and foreign influence activities that are counter to Canada's sovereignty and national interest.

States are also using scientific diplomacy to engage researchers in Arctic countries to help establish, entrench, and legitimize their presence and interests. This would increase their chance of gaining long-term access to land and resources that may not be in Canada's national interest.

CSIS is developing more robust capabilities in the Arctic. CSIS collects intelligence to identify activities that undermine Canada's security in the Arctic, including those that seek to use commercial activity as a pretense. CSIS will continue to work with key partners in Canada, including territorial governments, Indigenous governments and organizations, industry, and communities. CSIS engages regularly with Indigenous and Arctic rights holders to learn from their insights and help build resilience to threats. For example, CSIS is enhancing information sharing with Inuit and territorial governments to empower them to consider national security interests as they make decisions about economic and research opportunities with foreign companies and investors.

Indigenous and Arctic engagement

In 2025, CSIS engaged with a multitude of Arctic and Northern partners, including territorial and Indigenous governments and organizations, communities, community development organizations, local leadership, and research institutes. Throughout the year, CSIS officials regularly travelled to Nunavut, the Northwest Territories, and the Yukon to meet with partners and participate in a series of events. CSIS also hosted senior officials and leadership from key

Indigenous and Northern partner organizations at CSIS' national headquarters in Ottawa. These efforts help to ensure that partners have up-to-date information to build and maintain resiliency against current and emerging threats. They also support CSIS in building meaningful partnerships in the Arctic and North to better inform CSIS' understanding of the context and realities of diverse Indigenous communities.

Last year, CSIS continued to develop new relationships and strengthen existing ones with First Nations, Inuit, and Métis organizations and governments. CSIS also continued to work with Indigenous partners to implement its commitments under the Government of Canada's *United Nations Declaration on the Rights of Indigenous Peoples Act* by actively integrating the UN Declaration's principles into its operations, policies, and training to build trust, respect Indigenous rights, and address systemic issues. CSIS is the only intelligence service in the world to have made UN Declaration commitments.

In early 2025, the Canadian Institute for Arctic Security (CIAS) was launched through joint efforts by the Government of Yukon and the Canadian Northern Economic Development Agency. During the inaugural launch of CIAS' Conference Zero, in March 2025, CSIS presented the current and emerging threat landscape in the North and highlighted how CSIS can work with Indigenous and Northern partners to advance shared priorities, raise awareness on threats, and build resiliency against them.

CSIS representatives participated in numerous other conferences throughout the year. In August, the Director of CSIS participated in the CIAS LATITUDE conference in Haines Junction, Yukon, along with other key leaders in security sectors, to discuss Arctic security realities, challenges, and potential solutions. In September, CSIS representatives participated in the Arctic Security Conference in Whitehorse, jointly organized by Konrad Adenauer Stiftung (Canada), CIAS, the Asia Pacific Foundation of Canada, and the Macdonald-Laurier Institute. CSIS was also present at the Assembly of First Nations Yukon Open House on Political Interference and Economic Security and at the Yukon First Nations Defence and Security Industry Conference in April. These engagements further reinforce CSIS' commitment to building and maintaining strong and meaningful relationships with Indigenous partners across Canada.

Counter proliferation

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

CSIS 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 constitute 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 advanced conventional weapon and WMD threats to Canada.

In 2025, Russia maintained its capability and intent to illicitly procure export controlled and sanctioned technology from the West, including Canada. Russian illicit procurement efforts focused on non-sensitive and advanced technologies to sustain its military-industrial complex and support its war against Ukraine. Specifically, Russia sought to procure Canadian technology, such as microelectronics, satellite communication technology, and precision firearms.

To counter these efforts, CSIS worked closely with Canadian manufacturers and exporters, government departments and agencies, as well as foreign partners to identify how Canadian goods were being acquired and shipped to Russia, ultimately stopping them before they reached their destination.

Cyber security

Canada's strong democratic institutions, advanced economy, innovative research sectors, and leading academic institutions make it 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 escalate in scope and sophistication, making it essential for Canadians to be aware of the risks and take proactive measures to protect our country's interests.

CSIS' role in cyber security

CSIS plays a crucial role in safeguarding Canada's cyber security by investigating and mitigating threats from hostile cyber actors. Through close collaboration with domestic and foreign partners, CSIS utilizes its full range of investigative techniques to counter these threats. CSIS also employs its threat reduction mandate to protect Canadian critical infrastructure and national security.

CSIS provides high-quality intelligence assessments to government partners allowing them to make informed decisions. To support the integrity of the global information infrastructure, CSIS shares these assessments and investigative leads with foreign partners. In recent years, CSIS has expanded its role by working closely with industry, Indigenous groups, and governments to raise awareness and build resilience to the evolving cyber threat landscape. CSIS also works in close partnership with CSE, including its Canadian Centre for Cyber Security (CCCS).

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.

State-sponsored cyber activity

In 2025, Salt Typhoon, a PRC-linked cyber threat, is believed to have targeted Canadian telecommunications firms, potentially compromising customer communications data. It is concerning that Salt Typhoon has been able to compromise major telecommunication companies in the US and in other countries and access sensitive information, including call and text message data. It is possible that similar breaches could occur in Canada, which means that Canadians' personal information, such as phone calls and text messages, could be at risk of being accessed by hackers.

In August 2025, 25 intelligence services, including CSIS, released a cybersecurity advisory noting that, since 2021, Salt Typhoon has targeted networks globally. This includes, but is not limited to, telecommunications, government, transportation, lodging, and military infrastructure networks. CSIS continues to investigate, analyze, and reduce the threat posed by Salt Typhoon, in concert with CCCS. It is likely that this threat actor will remain a concern.

As part of the Government of Canada's Indo-Pacific Strategy, CSIS has made strategic investments in the Indo-Pacific region and has undertaken more frequent and targeted discussions with partners, including on cyber security. CSIS continues to exchange intelligence and advice with Indo-Pacific partners on the cyber threats they are facing, providing timely and actionable information to support their efforts to build resilience. A strong and resilient cyber security posture is essential to preventing and responding to cyber threats. By working more closely with its partners, CSIS aims to promote a more secure and stable cyber environment, and to support Canada's national interests in the region.

Another significant threat to global security is the malicious cyber activity conducted by Russia's intelligence agencies, which continue to target NATO allies as the war in Ukraine continues. For example, the Main Intelligence Directorate (GRU) Unit 26165 (also known as APT28 or Fancy Bear), has used various methods to hack into email accounts, steal information, and disrupt the activities of its targets, including companies involved in delivering aid to Ukraine.

Non-state cyber actors

Non-state actors, including cybercriminals and so-called "hacktivists," continued to play a significant role in the cyberspace threat landscape, posing a threat to Canadian critical infrastructure, sensitive information, and democratic values. Ransomware campaigns remain a major concern, as they can disrupt the operations of critical infrastructure and sensitive sectors, and put Canadians' personal identifiable information at risk. While cybercriminals are often motivated by financial gain, their activities can have significant national security implications, especially when they are leveraged or condoned by state actors to advance geopolitical interests. Russia-aligned

non-state actors, who are ideologically motivated in support of Russia's geopolitical goals, have been actively engaged in cyber operations targeting critical infrastructure in NATO countries. Occasionally, these groups are able to achieve disruptive effects. These groups' activities are consistent with Russia's broader strategy of using deniable cyber operations to support its military and economic interests, as seen in its activities in Ukraine and other regions.

It has become increasingly difficult to distinguish between state-sponsored and non-state actor cyber activities. The commercial proliferation of cyber capabilities has increased access to malicious tools and techniques, enabling a growing array of actors to conduct cyber attacks and other malicious activities. Authoritarian regimes use these tools to target individuals and groups they see as threats. As a result, it is essential for Canada to remain vigilant and proactive in its efforts to prevent and respond to cyber threats.

Security screening

As the world becomes more unstable, CSIS serves as an important line of defence against those who could threaten Canada's national security, including the advice it provides through its Government Security Screening and Immigration and Citizenship Screening programs.

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. CSIS security assessments enable sponsoring departments and agencies to make more informed, risk-based decisions regarding security clearances and site access clearances. The decision to grant, deny, or revoke clearances rests with each sponsoring department or agency, and not with CSIS. In 2025, CSIS received 129,130 requests for GSS, which follows the previous downward trend in requests. As the threat environment continues to evolve, there continues to be an increase in the number of security clearance applications that have a foreign interference nexus.

Screening regarding security and inadmissibility is a necessary and important requirement under Canada's immigration legal framework. The Government of Canada's Immigration Security Screening Program (ISS) is a trilateral program between Immigration, Refugees and Citizenship Canada (IRCC), the Canada Border Services Agency (CBSA), and CSIS. Under this program, IRCC can refer applications to CSIS and CBSA for comprehensive security screening on persons applying for refugee status in Canada, temporary resident visas, permanent residency, and citizenship. CSIS also undertakes the security screening for all in-Canada asylum claimants. CSIS then 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. CSIS' advice is taken into consideration when a final decision is made on the inadmissibility of an applicant.

In 2025, CSIS received 438,600 immigration security screening referrals.

As Canada's immigration levels were reduced, the overall number of new applications received by CSIS was also reduced. However, due to the previous increases in immigration levels and special immigration measures as part of the Government of Canada's humanitarian commitments made in response to world events, the overall number of immigration applications awaiting security screening remains at a historic high.

CSIS remains actively engaged in the security screening, under Government of Canada special immigration measures, of foreign nationals who are fleeing international conflicts. This includes, for example, individuals in Gaza. Public policy programs significantly impact the security screening inventory, particularly when security risks are elevated and the complexity of cases extends screening timelines. In 2025, CSIS dedicated considerable effort to immigration screening for Gaza, with the majority of files completed by CSIS. The organization continues to prioritize the remaining files.

In addition to the existing inventory of security screening files, an increase in mandamus applications filed in court by applicants seeking a decision on their immigration screening file, combined with complaints to the National Security and Intelligence Review Agency (NSIRA) concerning CSIS timelines for processing immigration security screening referrals, have increased pressures on CSIS' security screening program. In response, CSIS continues to make ongoing efforts, both internally and in collaboration with its partners, to improve the security screening process, including processing timelines. These efforts are expected to increase capacity and efficiency, lessen the impact of mandamus applications and NSIRA complaints, and allow program standards to be reviewed more frequently. CSIS, as a security screening partner, operates in an ever-changing national security threat environment and must constantly adapt to respond through IRCC to immigration priorities and requirements as directed by the Government of Canada.

CSIS works diligently to apply the necessary rigour to effectively execute its security screening mandate for all applications, and ensure the safety of Canada and all Canadians.

Government Screening Program	Requests received in 2025*	Requests completed in 2025*
Federal government departments	60,300	61,100
Free and Secure Trade (FAST)	2,500	2,400
Transport Canada (Marine and Airport)	38,200	38,200
Parliamentary Precinct	2,100	2,100
Nuclear facilities	14,900	14,600
Provinces	70	70
Foreign screening**	360	570
Major events	8,400	8,400
Others	2,300	2,300
Total	**129,130**	**129,740**

Immigration and Citizenship Screening Program	Requests received in 2025*	Requests completed in 2025*
Permanent residents inside and outside Canada	15,200	16,900
Refugees (front-end screening***)	97,600	96,600
Citizenship	297,700	289,600
Temporary residents	28,100	24,000
Total	**438,600**	**427,100**

* Figures have been rounded.

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

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

The Integrated Threat Assessment Centre

The Integrated Threat Assessment Centre (ITAC) is a specialized organization in the Canadian intelligence community, providing timely and cross-institutional assessments based on all-source information and intelligence. Its mission is to enable decision makers and security partners to safeguard Canadians and advance Canadian interests at home and abroad.

ITAC brings together experts from various fields, including policing, security intelligence, and border security, to provide foresight on converging topics like terrorism, criminality, global insecurity, state activity, technology, and climate change. ITAC delivers forecasts and advice through a collaborative hub, where intelligence from diverse sources and databases is analyzed and disseminated. Alerts and threat levels provide awareness and assist in the decision-making process. ITAC publishes evaluations covering several regions of the world (including Africa, the Americas, and Europe), while also focusing on domestic issues such as threats to public officials and national threat levels. ITAC is regularly asked to provide expertise in support of other government departments and agencies through requests for information.

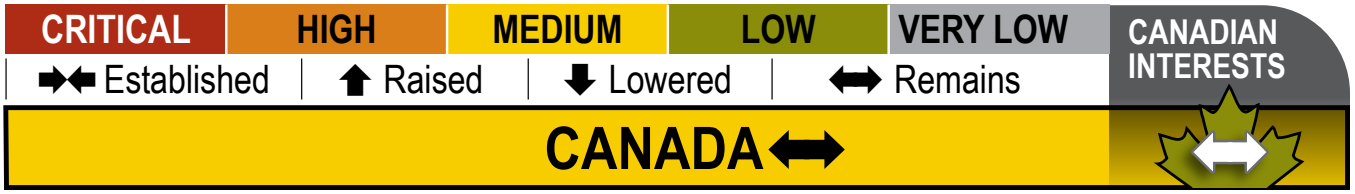
National Terrorism Threat Level

The National Terrorism Threat Level (NTTL) is an early warning tool to identify the likelihood of an act of serious politically, religiously, or ideologically motivated violence occurring. In 2025, violent extremist narratives and networks continued to inspire Canadians, notably youth, to engage in activities affecting the national security landscape. ITAC's comprehensive analysis of threats showed that despite continued police and security intelligence mitigation of threats the violent extremist threat in Canada has remained constant. Some threats have increased, such as youth mobilization, and some have fallen, largely as a result of law enforcement actions. Those that have increased are the most pressing concerns of threats of mobilization to violence. Following recommendations from ITAC based on available reporting and information, in 2025 the Director of CSIS maintained the NTTL at MEDIUM, meaning that a violent extremist attack is a realistic possibility in Canada.

Threats to public officials

Throughout 2025, Canadian public officials continued to face a complex threat environment. ITAC's Threats to Public Officials Program monitored national security threats to federal officials, including foreign interference, espionage, cyber threat activity, and violent extremism. ITAC collaborated with federal partners, including the SITE TF during GE45. While public awareness of threats from foreign states has increased, state actors continued to target officials, including using tactics such as cultivation, illicit financing, and foreign information manipulation and interference. Violent rhetoric and intimidation targeting public officials also continued, though the vast majority of these threats were of low credibility and while likely criminal, did not necessarily involve violent extremism. Threats and threatening behaviours nevertheless continued to hamper some public officials' abilities to conduct their duties and threaten democratic institutions more broadly.

ITAC considered Gender Based Analysis Plus identity factors in its methodology to prioritize production, identify trends from data, and tailor briefings and assessments for specific clients.



Deepening and expanding partnerships

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

CSIS' Academic Outreach team worked closely with operational units to support government priorities by bridging the worlds of academia, industry, and national security agencies through in-person expert briefings, roundtables, a commissioned study, and workshops. CSIS plays an active role in fostering a clearer understanding of security issues, a process that benefits CSIS' experts, as well as the researchers and specialists who collaborate with us.

In February 2025, CSIS partnered with the Centre for European and Eurasian Studies at the Munk School of Global Affairs and Public Policy to host a workshop on Russia and international conflict to address Russia's full-scale invasion of Ukraine to coincide with the third anniversary. This event brought together scholars, Canadian and foreign government representatives, students, and practitioners for a day of panels and discussions.

To support the development of the next generation of national security, intelligence, and foreign affairs scholars and leaders in Canada, CSIS sponsored the Ottawa Symposium of the Canadian Association of Security and Intelligence Studies (CASIS) and the CASIS Essay Contest for the third year.

CSIS also hosted two experts for workshops discussing the gamut of violent extremist threats and lessons learned by both national security practitioners and academic subject matter experts.

In addition, CSIS hosted roundtables to discuss research security, as well as neurotechnology, cognitive warfare, and strategies for countering disinformation. CSIS remains committed to being at the forefront of understanding, investigating, and mitigating security threat activity.

Stakeholder engagement

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 produces two newsletters: the monthly *Need to Know*, which is sent to a broad cross-section of partners and stakeholders across Canada, and *Research Security Quarterly*, which helps meet the growing demand for national security engagement and transparency within the country's research and innovation communities. These newsletters provide readers with information on relevant developments in national security matters and highlights related events and training opportunities. In 2025, CSIS co-published the editions of *Research Security Quarterly* with the University of Alberta and the University of Ottawa.

Throughout 2025, CSIS joined Public Safety, the Department of Justice, and the RCMP to deliver targeted resilience and awareness briefings to non-governmental organizations, civil society organizations, community associations, Canadians from diverse communities, as well as university administrators, faculty, students, and staff across Canada. This coordinated effort was led by Public Safety's Office of the National Countering Foreign Interference Coordinator. The goal was to combat foreign interference and transnational repression, and reduce these threats to strengthen societal resilience, and maintain the trust of Canadians in their democratic institutions.

In June 2025, a representative from CSIS' Stakeholder Engagement team was a panellist at the 2025 Research Security National Conference: Navigating New Domestic and Global Frontiers hosted by the University of British Columbia in Vancouver. CSIS provided an overview of its engagement work with the academic community and of national security threats targeting researchers and research institutions.

In the past year, CSIS also continued its long-standing support to Canadian universities by complementing and reinforcing efforts of their research security departments and expanding relationships across Canada's research ecosystem. CSIS also provided briefings to health science groups, which included timely insights into evolving risks to Canada's life sciences sectors, helping institutions better safeguard sensitive research, and ensuring that the Canadian-led world-class life sciences research and innovation remains open, secure, and trusted.

CSIS continued working with Canadian businesses and business associations to build resilience and mitigate threats to Canada's economic security. This work with groups like the Business Council of Canada (BCC) and the Canadian Chamber of Commerce (CCC) helps enhance communication between the public and private sectors. CSIS continues to engage with businesses and business associations to deliver threat briefings to support informed decision-making, including to the CCC and to the BCC's National Security Working Group and National Security Executive Network.

In support of the Government's Defence Industrial Strategy (DIS), CSIS provides support to the Department of National Defence by prioritizing threat briefings for DIS industry partners to raise awareness of evolving national security risks and disseminate critical information that enables industry to integrate security considerations from conceptual design through final delivery.

Trust is imperative and helps CSIS foster relationships needed to better protect non-Government of Canada sectors and entities most affected by threats to Canada's national security. As CSIS continues to grow and deepen these partnerships, the knowledge shared will help inform CSIS' operations and, in turn, help CSIS continue to earn the confidence and trust of Canadians, which should lead to increased contributions to conversations around national security.

Five Eyes Indigenous Network and Summit

This past year, CSIS chaired the Five Eyes Indigenous Network. As Chair, CSIS hosted the Network for an in-person annual summit in Ottawa. The Summit was a first of its kind, where foreign and Indigenous partners discussed key threats, priorities, and activities. This three-day Summit included classified and unclassified thematic panel discussions, case studies presented by Five Eyes and Indigenous partners, and cultural experiential learning with First Nations, Inuit, and Métis artists and performers. Key outcomes of CSIS' Chairpersonship of the Network included:

- **Strengthening collaboration across Five Eyes nations on Indigenous initiatives and priorities;**
- **Ensuring Indigenous partner participation in the broader national security discussion, and ensuring indigenous priorities and perspectives are shared and heard; and**
- **Identifying case studies and promising practices based on past experiences of CSIS' work with indigenous partners that can be applied moving forward.**

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.

CSIS is keenly aware of how much the threat environment has changed over the last 20 years. As the Government of Canada looks to release its first national security strategy since 2004—a time when our key focus was terrorism in the post-9/11 environment—CSIS will lend its full support to the implementation of this strategy as it continues to play a central role in keeping Canada safe, secure, and prosperous.

Modern threats call for modern authorities. Despite changes over time, the CSIS Act continues to reflect the era in which it was written: the 1980s. The current authorities set out for CSIS remain defined by that era, and changes to the legislation over the years have been outstripped by the speed of evolving national security threats. Compared to its allies, Canada faces considerable challenges in collecting the intelligence needed to protect Canadians, inform decision-making, and advance Canada's interests. CSIS collects information abroad on security threats, but is unable to collect abroad on wider strategic issues such as the diplomatic, military, and economic intentions and capabilities of foreign states. Currently, CSIS is only able to collect this information from inside Canada and in the context of assistance to the Minister of National Defence or the Minister of Foreign Affairs.

CSIS is aware that Canadians' expectations of CSIS are high, as they should be. Identifying threats to the security of Canada and to Canadian interests, advising decision-makers and stakeholders, and mitigating those threats must be done reasonably and in a measured way, but it must be modern and nimble to ensure that CSIS can continue to keep all Canadians safe and Canada resilient and strong in an increasingly dangerous world.

Oversight and review will continue to be critical to maintaining trust in our national security institutions, and can be strengthened by ensuring we balance safeguards and efficiency. Since 2017, we have seen the addition of the NSICOP, the replacement of CSIS' dedicated review body with NSIRA, and the expansion of the role of the Intelligence Commissioner (IC) to include some oversight for CSIS. These are important developments designed to enable the review of activities across organizations, improve parliamentarians' ability to engage in matters of national security, and expand Canadians' exposure to and understanding of Canada's national security and intelligence activities. CSIS will continue to examine whether these functions are working optimally and if there are opportunities to improve and streamline the functions to help ensure that CSIS decisions and activities are appropriate and reasonable.

Lawful access

Canada is the only Five Eyes country that does not regulate electronic service providers to enable better lawful access to information. The 2025 NSICOP report on lawful access elaborates on the challenges that CSIS and law enforcement face in this space and recommends the development of such legislation. The Government introduced lawful access legislation (*Strong Borders Act*, Bill C-2) in June 2025 aimed at addressing these challenges. The Bill sought to amend the CSIS Act to ensure parity with the *Criminal Code* and provide CSIS with the authority to require service providers, such as telecommunications companies, to provide a confirmation of service, which would allow CSIS to verify the initial building block information (i.e., whether an individual is a client of a service provider, the date range of service, and the province/territory of service) to advance the early stages of national security investigations.

The Bill also sought to require electronic service providers to have the capabilities to respond to legal requests from the Federal Court to access information and data, and lawfully intercept communications.

Potential benefits of lawful access legislation

Example 1:

Two CSIS subjects of investigation are at an advanced stage of planning a terrorist attack. CSIS is aware that they are finalizing their plans from a hotel room in a major Canadian city, and has an idea of the general location, but is unable to confirm the exact hotel in question. With the confirmation of service demand, CSIS would be able to request a confirmation of service from a small subset of hotel providers in the local vicinity—information that is no more than minimally intrusive. CSIS could use this collected information as part of an application for a warrant from the Federal Court to further the investigation and work with its partners to prevent an attack.

Example 2:

A CSIS subject of investigation is planning to travel to an ideologically motivated violent extremist paramilitary training event. CSIS is aware that the subject uses a social media account associated with a Canadian phone number to share the agenda and other information related to the event. CSIS plans to seek a warrant to lawfully access their communications and advance the investigation. However, the service provider does not have intercept capabilities and despite a warrant, CSIS is unable to get the investigative information required. This results in a significant delay in the investigation, CSIS having to deploy additional resources to monitor the threat, and a longer investigation during which Canadians are less safe. The new legislation would require service providers to maintain basic capabilities that are up to international standards and ensure they are "intercept-capable," which would provide better, more predictable investigative outcomes for CSIS and keep Canada and Canadians safer.

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.

Independent external reviews by NSICOP and NSIRA foster a culture of compliance, transparency, and continuous improvement at CSIS, while keeping Canadians informed of key national security issues.

In 2025, there were a total of 30 national security reviews involving CSIS by NSICOP and NSIRA. Of these reviews, 22 are ongoing. CSIS received 71 requests for information and briefings from review bodies. CSIS responds publicly to all recommendations as they help to ensure CSIS remains lawfully compliant and is continuously improving, leading to better national security outcomes for Canadians.

Under the NSIRA Act, anyone can submit a complaint to NSIRA about a CSIS activity or the denial of a security clearance required by the Government of Canada. In recent years,

there has been a significant increase in complaints against CSIS filed with NSIRA regarding process delays for security screening of immigration applications. CSIS has seen a 290% increase in NSIRA complaints between 2024 and 2025, over 91% of which are related to allegations of delays in CSIS' immigration security screening. In response, NSIRA held an *en banc* hearing. CSIS will examine NSIRA's findings and recommendations, and will implement appropriate changes.

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 Canada and all Canadians. CSIS does not expedite application processing in response to complaints.

The IC also 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 classes of acts and omissions that designated CSIS employees and directed persons can commit that would otherwise constitute offences while performing intelligence collection activities. With the goal of further increasing transparency, the Office of the IC and CSIS work together in a way that protects against disclosure of information that would be injurious to national security when publishing IC decisions on its website. In 2025, the IC rendered 5 decisions involving CSIS.

Protecting privacy and personal information

CSIS limits the collection, use, retention, and disclosure of personal information to what is necessary and proportional to meet its mandate. CSIS engages with the Office of the Privacy Commissioner and the Treasury Board Secretariat to identify and implement best practices in privacy protection, ensuring that CSIS programs are aligned with the principles of the *Privacy Act*. In the past calendar year, CSIS has completed its review of 13 privacy breaches (2 material, 3 founded but non-material, 1 unfounded, 7 underway) and 31 privacy breaches related to non-compliance (2 founded but non-material and 29 in progress). CSIS also conducted 24 privacy needs assessments (6 completed, 18 currently underway) and is currently drafting 4 new privacy impact assessments (14 currently underway).

Access to Information Act and *Privacy Act* requests

CSIS has faced a number of challenges and workload pressures related to *Access to Information Act* (ATIA) requests, which has resulted in a drop in compliance rates. There are a number of factors at play, however, this drop is largely attributable to the significant increase in the amount of *Privacy Act* (PA) requests from individuals seeking the status of immigration and citizenship applications. These immigration-related PA requests have resulted in a drop in overall on-time compliance under both the PA and the ATIA programs. ATIA requests decreased over the past year, although the volume of pages reviewed increased by 86%. CSIS is actively examining a variety of options to deal with the pressures such as the use of technology, to improve efficiency, undertaking various staffing strategies, and exploring innovative approaches to address client requirements.

Justification Framework

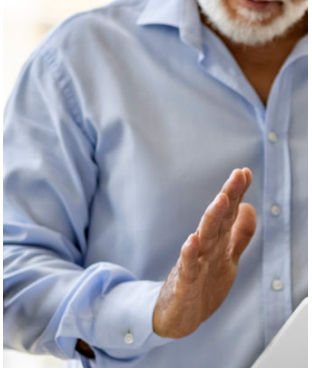
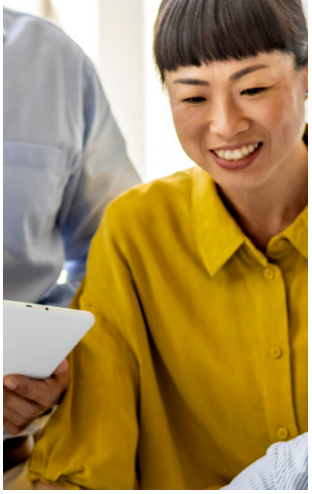
The Justification Framework provides legal authority for CSIS employees who are designated by the Minister of Public Safety and persons acting under their direction, such as human sources, to engage in activities that would otherwise constitute offences. This means, for example, a CSIS employee, or human

source acting at their direction, is protected from criminal liability when they engage in reasonable and proportional activities with a suspected terrorist in the hope of gaining their confidence.

As a first layer of accountability, the Justification 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 IC. 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, by fiscal year, provides the information required to fulfill these obligations:

Since the Justification Framework came into force in 2019, 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), and as such would otherwise constitute terrorism-related offences under the *Criminal Code*.

Justification Framework table	2021–2022	2022–2023	2023–2024	2024–2025
Number of emergency designations under s. 20.1(8)	0	0	0	0
Number of authorizations to direct the commission of acts or omissions under s. 20.1(12)	172	173	178	161
Number of directions under s. 20.1(15)(b)	0	0	0	0

Evolving how we work

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

Values and ethics

Building a respectful, inclusive, and equitable workplace culture starts as soon as new employees join the organization, and remains a priority throughout employees' careers, including at the executive level. The organization continues to prioritize training, awareness-building, and, in 2025, has added a more robust segment on values and ethics to the CSIS onboarding program to set the tone.

CSIS has its own Code of Conduct, and adherence to it is a condition of employment. As such, employees must familiarize themselves with and reaffirm their commitment to it on an annual basis. In 2025, CSIS also strengthened its internal conflict of interest declaration process to ensure that employees were better equipped to make informed decisions regarding their outside activities.

Addressing misconduct and wrongdoing at CSIS

In June 2025, CSIS publicly released its first annual Addressing Misconduct and Wrongdoing at CSIS report, following a commitment made by the former Director of CSIS, David Vigneault in 2023 in order to ensure transparency and hold the organization to account, as well as demonstrate that inappropriate behaviours are being addressed. These efforts also support the directive issued by the Clerk of the Privy Council to all deputy heads in 2025 that they produce annual reports on the disclosure of misconduct and wrongdoing.

To address the concerns raised by the 2023 and 2024 statistics included in this initial report, in 2025, CSIS continued to focus on providing training and awareness activities to educate employees and managers on acceptable workplace behaviours,

and to ensure that employees who experience or witness an act of misconduct or wrongdoing know what support resources and reporting mechanisms are in place.

The objective is to continue reinforcing the importance of a culture of integrity, respect, and accountability, and to provide a safe and supportive workplace for all employees.

The report also clearly demonstrates that where inappropriate behaviours took place, appropriate disciplinary measures were taken.

CSIS Ombuds Office

Part of the commitment made in 2023 included the creation of an ombuds office. CSIS was pleased to welcome its first Ombuds, Elianne Hall in May 2025, with her office officially launching in July 2025. This office further reinforces CSIS' efforts to support the development of a more people-focused organization by creating a safe space for employees. The Office of the Ombuds is also an independent option for employees at all levels to discuss workplace issues and concerns. This includes support for individuals navigating challenges related to harassment, discrimination, and other broad forms of wrongdoing and misconduct. The Office adheres to four key principles: informality, independence, impartiality, and confidentiality.

The Ombuds' mandate is to learn about systemic concerns within the organization, provide impartial advice to the Director, and inform decision-making in the organization to improve the workplace.

The Ombuds tabled her 100-day report in January 2026 in which she notes that CSIS is an organization with significant strengths—dedicated people, strong institutional knowledge, and a shared passion for its mandate. The report also points to a broader need for alignment—between values and behaviours, between policy and practice, and between leadership expectations and the supports provided to achieve them. Specifically, she noted concerns related to career development, competitive undercurrents, as well as gaps in management support and performance management practices. The report also underscored that addressing these systemic issues will take some time and likely require a multi-level approach that reinforces trust, strengthens managerial capacity, and promotes a culture of constructive communication and accountability. The Ombuds' first annual report will be released in the fall of 2026.

The Director of CSIS and the executive team are taking these observations seriously, and the results have been shared with employees to ensure transparency. They are factoring into the priorities the organization has set for the coming year, toward achieving tangible changes and improvements.

Diversity, Equity and Inclusion (DEI) Strategy

In 2025, CSIS continued the implementation of its 2022 DEI Strategy, and its most recent scorecard was published in spring 2025. A total of 45% of the 45 commitments adopted are completed, and the remainder have been initiated or are advancing.

Over the past year, the organization has made key advances with regard to representation in the organization. CSIS continues to see a rise in diverse hiring with 21.8% of the workforce identifying as members of a visible minority, 8.5% as persons with disabilities, 2.4% as Indigenous peoples, and 48% of CSIS intelligence officers being women. CSIS has also improved its recruiting and staffing processes following intersectional analysis to remove barriers and increase fairness and equity.

CSIS has also initiated work to address the findings of the Zellars Report on Black Executives in the Public Service as they relate to CSIS through

consultations with a working group of Black employees. This will in turn help guide the way forward for the organization's Black employees.

CSIS' employee-led Women in Technology Plus network has driven positive change by using data and employee feedback to promote diversity and inclusion in the organization's technology sector. This past year, CSIS saw a continued increase in representation with 19.8% of women in the science and technology sector.

CSIS 2026–2028 Accessibility Plan

CSIS is committed to ensuring that the organization is a place where all individuals, with diverse abilities, can thrive as they contribute to our mission.

CSIS has made significant progress with regard to accessibility and addressing barriers. The organization has progressed 95 of the 102 commitments in its 2023–2025 Accessibility Plan, with 42 of these commitments being completed.

Accomplishments include:

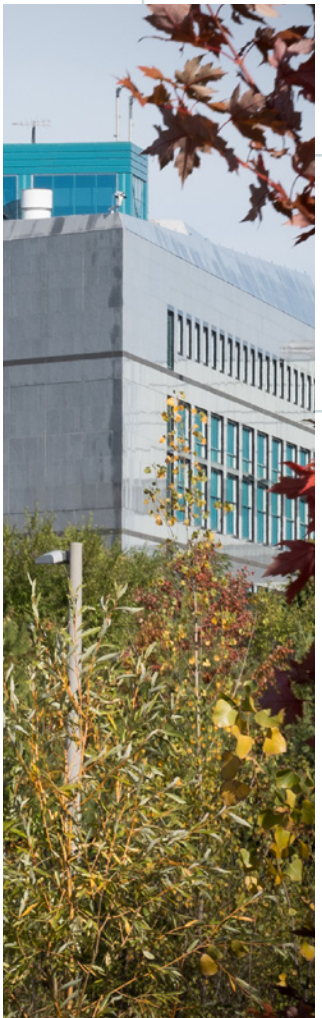
- Providing accessible transportation services to employees;
- Streamlining the process for requesting ergonomic equipment;
- Publishing products in accessible file formats;
- Offering mandatory training on accessibility, unconscious bias, and inclusion for all employees, including executives;
- Investing in accessible software that meets the organization's security requirements; and,
- Streamlining procedures and processes for routine requests for job supports for employees with disabilities.

Further, the organization also published its *CSIS Accessibility Plan 2026–2028*. This updated plan reflects an improved understanding of the work the organization must do, and CSIS is committed to continuing its efforts to remove barriers (be they physical, attitudinal or systemic) and increase accessibility for all employees. This was done through a collaborative and consultative process with employees with disabilities and key stakeholders, who together identified 32 barriers and the actions required to address them. The new accessibility plan focuses on 7 priority areas as identified in the *Accessible Canada Act.*

Areas of focus include:

- Improving accessibility in recruitment through increased training and implementation of more explicit offers of accommodations during the hiring process;
- Enhancing physical accessibility, including installing more automatic doors and conducting a thorough accessibility audit;
- Improving digital accessibility, such as through closed captioning and software evaluated for accessibility;
- Promoting accessible communications and further enhancing training and development through accessible learning resources and accommodations; and
- Increasing support and resources for all employees on how to access and apply workplace accommodations.




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

www.canada.ca/CSIS

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