Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

ISSN 2564-047X
CAT D95-11E-PDF

Communications Security Establishment Canada

Annual Report 2025–2026

Canada

Communications Security Establishment Canada
1929 Ogilvie Road,
Ottawa, ON K1J 8K6
cse-cst.gc.ca

ISSN 2564-047X
CAT D95-11E-PDF

Table of Contents

Introduction

For 80 years, the Communications Security Establishment Canada (CSE) has used its expertise in signals intelligence to keep Canada and Canadians safe. As technology has evolved, so has CSE's role. Through our Canadian Centre for Cyber Security (Cyber Centre), we now provide authoritative, practical advice and technical guidance to help Canadian individuals, businesses, various levels of government and critical infrastructure stay safe from cyber threats. Together, we are Canada's digital frontline of defence.

Canada is in a period of sustained geopolitical competition and rapid technological disruption. Cyber threats are growing in scale and complexity, and adversaries are increasingly targeting the systems and essential services Canadians rely on every day. In this environment, CSE plays a vital role in advancing Canada's strategic interests and protecting our security, sovereignty and prosperity.

In response, we have expanded how we work with partners in Canada and around the world. We work closely with our Five Eyes partners and other trusted allies to address shared security challenges and strengthen collective resilience and readiness.

By bringing together foreign intelligence insights with cyber security expertise, we are better positioned to identify threats quickly and proactively, and respond with speed and precision.

We are also growing our workforce and capabilities to meet rising demands. As the Government of Canada advances its defence, security and economic priorities, CSE is entering a period of sustained expansion and transformation. This growth reflects increased investment in digital infrastructure, cyber defence and emerging technologies, enabling us to scale our operations and deliver greater impact for Canadians.

This year marked a turning point for CSE. As the global security environment became more complex and contested, we enhanced our operations, partnerships and capabilities to better execute our mandate. Our throughline is greater integration – bringing together diverse perspectives, creativity, and focus to support Canada's security today and into the future.

This report provides an unclassified summary of CSE's activities from April 1, 2025, to March 31, 2026. Unless otherwise stated, "this year" refers to this reporting period.

FOREIGN SIGNALS INTELLIGENCE	TECHNICAL AND OPERATIONAL ASSISTANCE	ACTIVE CYBER OPERATIONS	DEFENSIVE CYBER OPERATIONS	CYBER SECURITY AND INFORMATION ASSURANCE
CSE's ability to collect foreign signals intelligence through the use of advanced techniques.	Assist federal law enforcement and security agencies, the Canadian Armed Forces and the Department of National Defence.	Interfere with foreign online efforts that threaten Canada.	Disrupt foreign cyber threats targeting important Canadian networks by taking online action.	Defend important Canadian networks.
Acquire information from or through the Global Information Infrastructure located outside Canada, including by engaging or interacting with foreign entities located outside Canada.	Use advanced techniques to support partners' activities, including cyber operations for government-authorized missions.	Online action to degrade, disrupt, influence, respond to, or interfere with foreign online efforts and capabilities as they relate to international affairs, defence or security.	Defend systems of importance to the Government of Canada.	Provide advice, guidance and services to protect important networks across the country, federal institutions, and electronic information and infrastructures of importance to the Government of Canada.

Minister's foreword

The threat landscape is changing rapidly. Alongside threats on land, at sea and in the air, today's foreign adversaries are increasingly operating in the cyber realm. As the world becomes more digitally connected, Canada must remain vigilant in defending the critical systems and services Canadians rely on every day.

For 80 years, the Communications Security Establishment Canada (CSE) has played a central role in keeping Canadians safe and secure. As the national cryptologic agency, CSE brings together foreign signals intelligence, cyber security, cyber operations, and technical and operational assistance to federal partners. This combination of expertise and capabilities is essential to protecting Canada's security, sovereignty, prosperity and resilience in a more complex and contested world.

This Annual Report shows the depth of CSE's contribution in support of government decision making and operations. CSE works closely with the Canadian Armed Forces, the Department of National Defence, the Canadian Coast Guard, and other federal departments and agencies to support Canada's defence and security efforts at home and abroad. Its support strengthens decision-making, enhances readiness, and helps partners carry out their mandates in an increasingly complex security environment.

In 2025, the Government of Canada made historic investments to strengthen national defence and security, and CSE is an important part of that effort. CSE's capabilities help advance Canada's defence objectives and contribute to Alliance commitments. These investments helped Canada achieve the North Atlantic Treaty Organization (NATO) 2% benchmark in 2025–2026 and support a path toward the Alliance's 5% Defence Investment Pledge by 2035.

CSE also brings capabilities that position Canada as a strong and reliable partner on the global stage. Its technical expertise, operational experience and trusted partnerships support international defence, intelligence and cyber security cooperation, including through the Five Eyes partnership. This role is also reflected in CSE's mandate through the Canadian Centre for Cyber Security, which provides vital guidance to government partners, small and medium enterprises, critical infrastructure sectors and Canadians. By strengthening awareness, resilience and readiness across the country, the Cyber Centre helps ensure that Canada operates from a position of strength.

Behind all this work are dedicated public servants whose expertise and commitment serve Canada every day. Their work is often done behind the scenes, but its impact is felt across governments and across the country. I am grateful for their continued service and for the important role they play in helping protect Canada now and into the future.

The Honourable David J. McGuinty (he/him)
Minister of National Defence

Message from the Chief

I am pleased to share this year's Annual Report with Canadians, which reflects a significant year for CSE during a period of considerable global change and instability.

The security environment facing Canada has become more complex. Cyber operations against critical infrastructure, disinformation campaigns aimed at democratic institutions, and increasingly sophisticated adversaries targeting Canada's interests underscore the need for sustained vigilance and action.

These threats do not sleep, nor do they retreat in bad weather, nor do they take breaks on statutory holidays. As interest in our digital assets grows, CSE's mandate forges ahead 24/7 across international time zones, 365 days a year to strengthen Canada's cyber posture and stay ahead of attacks on our country. Our motivation for this is singular: we are Canada's digital frontline of defence.

In Budget 2025, the Government of Canada made historic defence investments that reflect the trust placed in CSE's capabilities and the importance of our work to Canada's security. This report sets out how CSE is advancing Canada's security, strategic interests, and prosperity by putting that trust into action.

For CSE, 2025 was a year of significant progress. We advanced work that supports Canada's commitment to NATO defence-spending targets, translated major investments into concrete action, and strengthened the capabilities and partnerships that contribute to Canada's security. Across our mandate, we continued to link intelligence to operations – connecting insight to action through closer integration between foreign intelligence, cyber security and cyber operations. This integrated approach strengthens Canada's autonomy in the digital domain and underpins broader security efforts across North America, extending into Canada's North and Arctic systems while allowing us to strengthen relationships with Indigenous communities, as the original stewards of the land. Across all areas of progress, our focus now is to continue executing with discipline, ambition, and clear strategic intent in service of Canadians.

CSE's foreign signals intelligence operations continue to support our banner mission: to defend Canada's national security while keeping the Government of Canada's information secure. With that responsibility comes our commitment to support industry and academia here at home, and our allies around the world who all share our cyber and national security mandate. This year, we also advanced the use of artificial intelligence in a responsible manner to improve how we work across our mission – helping our people analyze complex data more efficiently, accelerate decision-making, and strengthen cyber defences against increasingly sophisticated threats.

At the same time, our researchers are contributing advances adopted by the international open-source community and academia, reinforcing CSE's role in cyber security innovation. Our momentum continues to grow as we expand partnerships across the private sector, Indigenous communities, and international organizations to strengthen Canada's long-term resilience and help build the foundation for future generations of cyber security talent.

While our mission requires speed and agility, it also demands trust. As such, CSE remains firmly committed to transparency and accountability. We are proud to operate under the scrutiny of independent oversight and external review bodies that hold us to the highest standards. We continue to enhance our compliance frameworks to reflect the evolving nature of our work and the technologies we use.

This year, CSE celebrates 80 years of service to Canada. Our core purpose has endured over the decades: analyzing threats, protecting digital infrastructure, supporting Canada's military and security partners, and most importantly, keeping Canadians safe.

Over those 80 years, it has always been our people who have made the difference, people from every background, discipline, and perspective, united by a shared mission. CSE is committed to removing barriers in the workplace and fostering an environment where all employees can contribute fully and thrive. Maintaining a diverse workforce is essential to operational excellence. Diversity in all its forms is a mission strength, and it amplifies our ability to anticipate threats, remove blind spots, solve complex problems, and deliver for Canadians.

As CSE looks to its next chapter, our focus is on strengthening the digital foundations that support Canada's security and resilience. Our work contributes to how the country functions, grows, and protects itself in an evolving digital world. As the global environment continues to change, CSE will continue to adapt so that Canada is prepared to meet emerging challenges with confidence. We will do it as One CSE.

Caroline Xavier (she/her)
Chief, CSE

2025-2026 highlights

Our workforce in 2025 to 2026

Total workforce	4,178[1]
Attrition rate	2.8%[2]
Workforce increase	337 (8.1%)
Workforce representation (by self-identification)	
↳ Women	33.9%
↳ Persons with disability	14.1%
↳ Racialized persons	17.9%
↳ Indigenous persons	2.6%
↳ 2SLGBTQIA+ persons	6.4%

Alerts and notifications issued to protect against malicious actions in 2025 to 2026

Cyber Centre general inquiries received	14,700 (9% increase)
Cyber Centre incidents responded to	
↳ Government of Canada	1,528
↳ Canadian entities	1,688
of these 3,216 incidents	
↳ the Cyber Centre identified the incident, notified the organization and provided support in response to	2,282 cases (1,094 affecting federal institutions) (1,188 affecting Canadian entities)
↳ the Cyber Centre received incident reports and provided response support to	934 cases (434 from federal institutions) (500 from Canadian entities)
Cyber Centre Alerts published	25
Cyber Centre Advisories published	995
Pre-ransomware notifications	67 notifications sent to 67 Canadian organizations
National Cyber Threat Notification System (NCTNS) alerts	Over 97,000 security alerts sent to 1,363 subscribed organizations
Supply chain risk assessments	1,772

Foreign signals intelligence in 2025 to 2026

Reports	3,976
Client departments	30
Individual clients	3,332
Requests for assistance	55

Reports, publications and guidance released in 2025 to 2026

Cyber security guidance publications	41
Joint endorsement publications	28
Unclassified threat assessments and bulletins	7

Engagement with other government departments and critical infrastructure industries in 2025 to 2026

Meetings held with Critical Infrastructure partners	522
Speaking engagements	120
Cyber Centre booths	5
Briefings on preparing for the quantum computing threat to cryptography	13
Tabletop exercises	4
Biweekly threat briefings for IT security professionals	23
"Walk-the-talk" sessions	8

Media and public engagement in 2025 to 2026

Media queries	169
Interviews	20
National news conferences	6
Parliamentary appearances	11
Order Paper Question (OPQ) responses	97
Enrollments in Learning Hub courses	6,585

1 Includes indeterminate, term and casual employees working full-time and part-time.
2 This figure excludes term employment and retirements.

Accountability, transparency and compliance in 2025 to 2026	
Ministerial authorizations	
↳ Via Intelligence Commissioner	9
↳ For conducting foreign cyber operations	4
Ministerial orders in effect	6
Ministerial directives	1
External Reviews	
↳ Reviews and reports contributed to	26
↳ Briefings to review bodies	24
↳ Questions answered	454
Operational compliance incidents	
↳ Involving information related to Canadians	186
↳ Not involving information related to Canadians	14
External complaints	
↳ Sent to the Chief	7
↳ Sent to NSIRA	Nil
Open Government portal uploads	
↳ Datasets	5
↳ Information assets	56
Access to Information Act requests	85
Proactive disclosures	4 committee binders
Tabled documents	3
Internal audits	
↳ Assurance audits	3
↳ Advisory audits	1

WE ARE CANADA'S DIGITAL FRONTLINE OF DEFENCE

The global security landscape is changing rapidly, shaped by geopolitical instability, new forms of conflict and accelerating technological change. These dynamics are redefining how states compete, collaborate, and protect their interests.

As these pressures intensify, CSE is scaling its operations to respond. Enabled by historic defence investments in 2025, we are strengthening Canada's digital frontline and strategic advantage through integrated intelligence and cyber operations, working closely with partners at home and abroad.

Within this context, CSE plays a critical role in protecting Canada's people, infrastructure, and sovereignty. Foreign signals intelligence is one of the country's key national security assets, providing timely insight and early warning to support decision-makers and enable effective action against emerging threats.

To deliver on our mandate, we work closely with partners across the Government of Canada and Five Eyes partners, and trusted international allies.

From protecting the Arctic to countering foreign interference and expanding cyber defence operations, we are focused on the priorities that matter most to Canada and our allies.

Together, we reduce risk, strengthen resilience, and help ensure Canadians can rely on secure and uninterrupted services in an increasingly digital world.

CSE is focused on building the capabilities that will define Canada's digital security in the years to come – from artificial intelligence and quantum-resistant cryptography to deeper partnerships across government and industry, including with a variety of international partners. This is our long-term vision of a more secure, resilient and sovereign digital Canada.

Detecting, defending, disrupting and deterring foreign threats

CSE's work does not occur in a vacuum. Our operations are explicitly authorized by the *CSE Act* and steered by Canada's Intelligence Priorities, which serve as the operational blueprint for the agency, ensuring that our work is tied directly to the interests of the nation.

Foreign signals intelligence (SIGINT) is a core part of CSE's mandate. It helps us understand foreign threats and provide strategic insights to support government decision-making, without targeting Canadians or people in Canada.

This intelligence directly informs Canada's security, defence and economic prosperity interests in a complex and rapidly evolving environment.

SIGINT has evolved significantly over the past 80 years. In the aftermath of World War II, SIGINT efforts were focused on intercepting radio signals and decrypting electromechanical devices. Today's powerful SIGINT capabilities are used to intercept, decrypt and analyse electronic communications and digital signals within the Global Information Infrastructure using sophisticated and classified techniques. CSE continues to invest in new capabilities, and we are increasingly incorporating Artificial Intelligence (AI), to transform how we identify and respond to foreign threats.

Foreign cyber operations

The *CSE Act* authorizes two types of foreign cyber operations: defensive and active. These operations, sometimes referred to as offensive cyber or cyber effects, may be used to counter foreign threats to Canada, advance Canadian interests related to international affairs, defence or security, the economy, or to help protect systems and electronic information, depending on the type and scope of the operation.

- **Defensive cyber operations** help protect systems designated as important to the Government of Canada during major cyber incidents, when other measures are not enough.
- **Active cyber operations** are used to disrupt foreign threats before they can cause harm to Canada's international affairs, defence or security interests.

These operations are strictly governed by law, as described in the *CSE Act*. They cannot target Canadians in Canada or around the world, nor anyone in Canada. In addition, active cyber operations must not interfere with the course of justice or democracy, or cause death or bodily harm to an individual, either deliberately or by criminal negligence. They may only be directed at foreign targets that relate to international affairs, defence or security, which includes economic interests.

Foreign cyber operations are approved under a "two-key" system. All cyber operations require approval by the Minister of National Defence. Active cyber operations also require consent of the Minister of Foreign Affairs, while defensive cyber operations require consultation with the Minister of Foreign Affairs. This includes working closely with Global Affairs Canada (GAC) to assess the foreign policy impacts and legal implications of proposed cyber operations, considering both Canadian law and international law applicable in cyberspace[1].

CSE's foreign cyber operations mission is carried out in close cooperation with the Canadian Armed Forces Cyber Command (CAFCYBERCOM). Through this valued partnership, many members are integrated into CSE operations to defend and advance Canadian interests, helping our country build an effective, agile capability for foreign cyber operations.

Enabled by new investments in cyber capabilities, CSE strengthened its ability to conduct both defensive and active cyber operations at scale to counter foreign threats.

Integrated mission: how our mandates work together

CSE's strength lies in how its foreign intelligence, cyber operations and cyber defence teams work together. This integrated approach allows us to move from insight to action more quickly and effectively. We also work closely with the Canadian Security Intelligence Service (CSIS), bringing together complementary authorities, expertise and insights to help identify threats earlier, strengthen situational awareness and support coordinated responses in defence of Canada's security interests. As stewards of our country's national security, we are driven by the trust that Canadians place in our work, and by the responsibility to uphold this as the security and intelligence environment continues to evolve.

- In 2025, the Cyber Centre identified a phishing campaign targeting Canadian federal institutions and designated systems of importance.
- SIGINT foreign intelligence teams analyzed the campaign and identified the tools being used.
- This intelligence enabled a defensive cyber operation that disrupted the threat actor's infrastructure and degraded their ability to continue to target Canadians.
- This year, CSE's SIGINT cybercrime team produced high-confidence reporting which identified sophisticated tactics, techniques and procedures used by a notorious Ransomware-as-a-Service (RaaS) cybercrime group responsible for over 25 incidents against transportation, healthcare, pharmaceutical and business sectors in Canada.
- Working with Five Eyes partners and law enforcement, CSE carried out an active cyber operation which rendered the group's infrastructure inoperable and deleted a large amount of stolen data that was being advertised for sale on the dark web.

Espionage, foreign interference and state cyber threats

State-sponsored actors are becoming more aggressive and are moving beyond traditional espionage to conduct more disruptive activities. In the current geopolitical environment, nation states are increasingly engaging in hybrid threat activity, integrating cyber operations, online influence and disinformation campaigns and the targeting of critical infrastructure to achieve their disruptive objectives.

CSE provides foreign intelligence to help Canada understand and respond to hostile state activity that undermines Canada's security, sovereignty and prosperity. Our intelligence underpins efforts to counter foreign interference, protect critical infrastructure, and safeguard Canada's economic and democratic interests, while also informing key priorities such as Canada's Arctic security and Canadian support for the sovereignty of Ukraine. It directly supports Cyber Centre activities – from threat bulletins and advisories to operational support for cyber defenders – and is strengthened through close collaboration with CSIS and other partners to enhance shared awareness and enable coordinated responses across Canada's security and intelligence community.

This year, our intelligence and timely reporting:

- supported Canadian and allied efforts to list and enforce sanctions against Russia, including identifying entities that the Russian government is using to circumvent international sanctions
- informed Canadian and allied efforts to confront and counter Russia's persistent disinformation efforts, including a campaign by Russia to promote its narrative on its war against Ukraine and sow discord and division
- identified cyber threats to Canada from Russia and pro-Russian affiliates
- supported Canadian and allied efforts to identify and counter People's Republic of China (PRC) state-sponsored cyber espionage

Arctic sovereignty and security partnerships

The Arctic is an established priority for Canada, especially with shifting geopolitical winds layered on top of climate change. As interest in the region grows, especially from foreign states such as Russia and the PRC, so do the risks to Canada's security, sovereignty and long-term prosperity. These challenges are increasingly complex, extending beyond traditional military and cyber threats to include economic and influence-related activities that seek to shape access, infrastructure, and decision-making in the region.

As one of Canada's leading security and intelligence agencies and Canada's digital frontline of defence, CSE plays a critical role in responding to these risks. Working closely with domestic and international partners, we provide foreign intelligence, cyber defence, and operational support that underpin Canadian and broader North American security efforts. This work reflects the integrated and interconnected nature of modern Arctic defence, including close collaboration with partners such as the Canadian Armed Forces (CAF) and the Canadian Coast Guard.

Supported by increased defence investments, CSE has strengthened its intelligence capabilities in the Arctic to help address priority intelligence gaps and provide insight into foreign states' strategic intentions, capabilities, and activities in the region in support of Canada's sovereignty and security priorities. These insights also inform cyber defence efforts delivered through the Cyber Centre, enabling more timely and coordinated responses to emerging threats. Through partnerships across government and with allies, we support cyber defence, economic security, and efforts to counter foreign interference.

This work enhances Canada's ability to anticipate risks in a strategically important region and supports informed national security decision-making.

This year, CSE shared classified intelligence reports on Arctic security with multiple Government of Canada departments and international allies. Compiled with the help of CSIS intelligence and support, these reports covered foreign states' political intentions, military capabilities, technological advancement, economic interests and research activities in the region. We also actively pursued intelligence on foreign cyber actors seeking to exploit and compromise Arctic-related systems.

Partnerships in the Arctic

As attention on Arctic sovereignty continues to grow, CSE has made significant progress in deepening partnerships to advance our mandate this year. This includes:

- continuing to co-chair, together with the Privy Council Office (PCO), the Arctic Intelligence Coordination Group, which coordinates Arctic security activities across the Government of Canada
- promoting engagement through a dedicated Indigenous Engagement Team that works directly with Indigenous partners in the Arctic to advance cyber resilience
- participating in round tables led by GAC to brief on cyber threats to Indigenous communities and organizations in Yukon, Northwest Territories, Labrador, and Nunavut
- delivering a cyber security panel in collaboration with Nunavut Tunngavik Incorporated at the Arctic Security Working Group
- providing classified cyber threat briefings to territorial partners
- continuing to host and lead international forums on signals intelligence concerning the polar regions

These partnerships are grounded in a shared, multilateral commitment to collaboration, respect, and inclusion. CSE works closely with territorial and Indigenous governments to strengthen collective awareness of threats and to support responses to cyber incidents affecting critical systems in northern communities. It is important to note that CSE's engagement with Indigenous communities extends well beyond Arctic security. Our broader partnership efforts, including nation-to-nation relationship building and tailored cyber security support, are described further in this report.

Over the course of its work, CSE relies on strong partnership with the CAF to identify and monitor threats posed by foreign adversaries in the Arctic. We support operations across the Canadian Army, Royal Canadian Navy, the Royal Canadian Air Force, Special Operations Forces Command, and the Canadian Coast Guard, contributing to situational awareness and operational effectiveness in the North.

In an increasingly congested Arctic operating environment, Canada's role in the North American Aerospace Defence Command (NORAD) continues to grow in importance. Within this framework, CSE provides indications and warnings of potential air and maritime threats.

Beyond policy and analytic work, the Cyber Centre is connecting directly with communities and stakeholders, including critical infrastructure organizations, across Canada's North. Through targeted engagements like conferences and expositions, it promotes cyber security awareness, shares advice and guidance, and delivers services that strengthen the resilience of critical infrastructure and government systems. In support of this effort, the Cyber Centre has also deployed advanced sensors on territorial government systems to detect and mitigate malicious cyber activity.

Border security and illicit synthetics

The trafficking of fentanyl and other illicit drugs is having a direct and devastating impact on Canadians. At CSE, our work to counter transnational crime is grounded in a clear purpose: helping to save lives and reduce harm.

CSE has responded directly to the Prime Minister's Directive on Transnational Crime and Border Security, by supporting Canada's efforts to collect intelligence and disrupt criminal networks. We provide foreign signals intelligence on the logistics and mechanics of the international drug trade, with a focus on illegal drug trafficking and supply chains.

Working with partners in Canada and abroad, we share intelligence and take action – where appropriate – including cyber operations that disrupt activities threatening Canadians and our allies.

We have strengthened our capacity to deliver timely, actionable intelligence on foreign criminal actors involved in the trafficking of fentanyl, other illicit drugs, and their precursors across North America. By uncovering how these networks operate and adapt, we help reduce their ability to evade detection and continue harming communities.

Joint Operational Intelligence Cell

Transnational organized crime, including the trafficking of fentanyl and its precursors, poses a growing threat to Canada's public safety, health, and security. Addressing these networks requires coordinated intelligence and operational action across government and with international partners.

Through the Joint Operational Intelligence Cell (JOIC), we work alongside the Royal Canadian Mounted Police (RCMP), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Canada Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS), and Public Safety Canada (PS). This collaboration brings together intelligence, financial analysis, and law enforcement capabilities to better understand and disrupt complex criminal networks.

This year, we strengthened this coordinated approach by supporting initiatives such as the Secure Intelligence Regional Forum (SIRF) with Government of Canada partners, which enhances the sharing of intelligence and operational insights across partners.

On July 10, 2025, we also hosted Fentanyl Awareness Day in a classified setting to support collaboration and information sharing. The event reinforced Canada's commitment to combat the illicit drug trade and protect public safety and brought together key federal partners, including Canada's Fentanyl Czar, JOIC stakeholders, and the Public Health Agency of Canada. CSE also facilitated a multidisciplinary forum, inviting experts from the international medical field and law enforcement to participate.

Together, this work helps Canada identify, disrupt and reduce the impact of transnational criminal activity – including fentanyl harm, contributing to safer communities and stronger national security.

Case Study How CSE intelligence and cyber operations worked together to disrupt fentanyl and its precursor drug supply to Canada

- In 2025, CSE discovered that key online cybercriminals based outside Canada were brokering the purchase and sale of precursor chemicals used to fabricate synthetic opioids like fentanyl.
- CSE collected foreign intelligence on the brokers to better understand the threat to Canada, and developed options to disrupt their activities.
- CSE conducted authorized active cyber operations against these brokers that disrupted and diminished their ability to operate.
- CSE leveraged its authorities to successfully mitigate complex transnational threats, and supported law enforcement in advancing our national security objectives while saving lives and safeguarding our public health.

Countering violent extremism

Violent extremism continues to evolve, requiring coordinated and proactive responses.

CSE works to identify and counter foreign-based violent extremist threats against Canadians. Our intelligence helps government and our security and intelligence partners act quickly by highlighting threats from violent extremist groups and ideologies, including religiously-motivated groups (such as al-Qaeda and Daesh affiliates), and ideologically-motivated violent extremism (such as xenophobic, anti-authority, gender identity-driven and grievance-driven tendencies). Globally there continues to be an increasing trend of all forms of violent extremism manifesting online and in the real world with the intent of causing threats to public safety and innocent victims. These transnational movements leverage online forums to share their ideology and generate manifestos with a view to recruit others and terrorize others. Although the motivations may vary, the threats continue to be very real and threat actors seek to seize any opportunity to create chaos.

Across North America and Europe, our efforts have helped expose and disrupt multiple extremist threats. We continue to work closely with various allied intelligence services and law enforcement while also leveraging our foreign cyber operations authorities to disrupt plots and preserve public safety. Our priority continues to be identifying and responding to any threat to life and using cyber operations to dismantle terrorist networks that seek to do harm. We have also supported Canada's response to terrorism-motivated hostage situations, and threats to public events and Canadian missions.

Recent examples include:

- working closely with domestic partners to provide crucial information on foreign extremists aiming to direct attacks in Canada
- supporting responses to kidnappings or potential hostage-taking incidents involving Canadians abroad
- identifying threat actors responsible for bomb threats against entities in Canada
- working with international partners, on multiple occasions, to support efforts to mitigate and disrupt extremist threats in their countries
- monitoring threats to international events
- working with multiple foreign partners to protect Canadian athletes, delegations and the broader public against threats to the 2026 Milano Cortina Winter Olympic Games

Cyber operations to disrupt violent extremist organizations

CSE also enables and conducts real-world cyber operations to disrupt the activities of violent foreign extremist organizations. By targeting their online presence and technical infrastructure, we reduce their ability to operate, recruit, and spread harmful content.

Case Study How CSE intelligence and cyber operations worked together to counter violent extremism

- CSE collected SIGINT on a foreign extremist group spreading violent ideology and seeking to recruit in Western countries, including Canada.
- Our SIGINT teams developed intelligence – analyzing the group's network, reach and vulnerabilities – to determine how to disrupt it.
- Based on appropriate authorizations, we conducted an active cyber operation which successfully undermined the group's credibility and limited their ability to radicalize and recruit new members.

Cybercrime

Cybercrime is a persistent threat to Canada. As we reported in our Ransomware Threat Outlook 2025-2027[2], ransomware continues to be the most disruptive form of cybercrime affecting Canadian organizations, including critical infrastructure. CSE plays a key role in helping the Government of Canada understand and respond to this threat by working with allies and partners to monitor foreign cybercriminal activity and assess its potential impact on Canadians.

CSE produces foreign intelligence on the tactics, techniques and procedures used by foreign cybercriminals and hostile states. This intelligence helps the Cyber Centre warn cyber defenders, strengthen protections and support action against malicious activity targeting Canadian systems and critical infrastructure. By combining intelligence insights with cyber security expertise, CSE helps turn threat awareness into practical defence and response.

This year, CSE took concurrent action against 10 of the most significant ransomware groups causing harm to Canada and its allies. We carried out authorized technical disruptions to make parts of their infrastructure unusable, and we worked with international law enforcement partners to help disrupt foreign cybercriminal networks and reduce cyber victimization.

Support to military operations

CSE's intelligence helps keep Canadian Armed Forces (CAF) personnel safe. By providing timely warnings and situational awareness, we support operations in Canada and abroad. Over the past year, we delivered actionable foreign intelligence in support of key operations, including UNIFIER, REASSURANCE, and HORIZON.

Our intelligence helped to:

- identify counter-intelligence threats to CAF personnel
- provide early warnings to deployed forces assess how foreign state-owned enterprises could affect Canadian operations and exercises
- analyze enemy electronic warfare capabilities to better inform CAF responses

We also track how foreign adversaries develop and use their capabilities, including command, control systems, communications, computers, intelligence, surveillance, reconnaissance and targeting tools. This insight helps protect Canadian and allied forces conducting operations. The CAF used the intelligence we produced this year to improve their operational security, shape their operations and brief allies on adversary intent and capabilities, enhancing collective awareness and protection.

Operation REASSURANCE

Canada continues to play a leading role defending NATO territory on land, at sea and in the air, in response to Russia's ongoing aggression against Ukraine and hybrid activities against Allies.

In August 2025, Canada renewed its leadership role in Operation REASSURANCE for three years, starting in 2026-2027. This commitment strengthens Canada's contribution to security and stability alongside our transatlantic partners in Latvia and across the Mediterranean, Black Sea, and North Atlantic regions.

CSE supports this mission through its Deployed Cyber Security Officer (DCSO) program. Over the past year, Cyber Centre analysts deployed to Latvia and Lithuania where they:

- conducted proactive threat-hunting activities
- provided on-the-ground advice and guidance
- supported cyber defence operations

These efforts help strengthen allied resilience and ensure Canadian forces can operate securely and effectively. While these activities help Canada understand and counter threats abroad, CSE also applies this integrated approach at home, working through the Cyber Centre to prevent, assess and respond to cyber incidents affecting the systems Canadians rely on every day.

Responding to and preventing cyber incidents

Canada's cyber threat environment continues to grow in scale and complexity. State-sponsored threat actors and cybercriminals are evolving quickly, using new tools and techniques to target systems of importance, democratic institutions and Canadians.

In 2025–2026, the Cyber Centre recorded more than **3,200 cyber incidents** affecting Government of Canada institutions and critical infrastructure sectors.

Working closely with partners, we provided technical assessments, incident triage, containment advice, and mitigation support. Drawing on intelligence insights, the Cyber Centre was able to identify, assess and respond to cyber incidents more quickly and effectively.

This work helped reduce disruptions to essential services, limit the impact of cyber incidents on critical infrastructure, and protect the systems Canadians rely on every day.

Communications Operational Production and Coordination Centre (COPCC): CSE's 24/7 operational nucleus

CSE maintains a continuous operational posture in support of Canada's national security. At the centre of this effort is the COPCC, which provides round-the-clock situational awareness and operational coordination for CSE and Government of Canada partners.

COPCC monitors global developments and coordinates responses to events that may affect Canada and Canadians, including cyber incidents, national security threats, and major domestic and international events. These ongoing operations ensure timely, coordinated action across the federal security community.

Its effectiveness is grounded in close collaboration with federal partners and Five Eyes Security Operations Centres (SOCs), enabling shared situational awareness, joint planning, and aligned responses.

Holding the digital frontline

Outside regular business hours and through the night, COPCC serves as CSE's first line of response on the digital frontline. It issues alerts and notifications, and coordinates response activities to address cyber incidents without delay. This year, COPCC alerted the Canadian Centre for Cyber Security to **121 cyber security incidents after hours**, helping strengthen the resilience of Canada's digital infrastructure.

Supporting global events and emerging crises

In a period of heightened global instability, COPCC coordinated CSE's response to international developments and notified CSE stakeholders of **220 significant terrorist or global incidents** this year.

COPCC also worked closely with partners across the Government of Canada to share information and coordinate responses to emerging situations, including developments in Mexico, Cuba, Venezuela, Iran, and the broader Middle East.

Enabling secure delivery of planned events

This year, COPCC coordinated CSE's cyber security and foreign intelligence efforts in support of major planned events, including:

- the 45th General Election
- the G7 Leaders' Summit in Kananaskis, Alberta
- the Milano Cortina 2026 Winter Olympics and 2026 Winter Paralympics

COPCC also supported preparations for Canada's participation in, and hosting of the Fédération Internationale de Football Association (FIFA) World Cup 2026™.

Building on COPCC's coordinating role, the Cyber Centre provided more direct operational support to event partners, helping translate threat awareness into practical cyber defence measures before and during major events.

Cyber security support for major events

Major events present unique cyber security challenges that require coordinated planning and response.

CSE played a key role in coordinating cyber security support for major events this year, including the 2026 Milano Cortina Winter Olympic Games, the G7 Summit, and preparing for the FIFA World Cup 2026™. This work was strengthened by our integrated mission, which combined foreign intelligence, cyber security advice and operational coordination to help event partners prepare for and respond to evolving threats.

As a key member and leader of the Federal Cyber Security Working Group, we:

- worked with Government of Canada partners to strengthen the cyber security posture across host organizations and critical infrastructure
- provided strategic advice, technical guidance and threat assessments
- supported onboarding of involved critical infrastructure organizations to Cyber Centre services
- delivered targeted cyber security briefings to stakeholders

We also took part in several tabletop and functional exercises designed to test readiness and enhance coordination across partners. During events, CSE maintained an on-site presence at event command centres, ensuring direct operational engagement and real-time support.

Safeguarding the 2026 Olympic Games

CSE supported a coordinated intelligence effort to enhance the security of the 2026 Milano Cortina Winter Olympic Games. Working with event partners, we established and maintained strong information-sharing processes to monitor threats and support safe event delivery. We also prioritized our intelligence collection efforts to identify any potential threats to the Games or to Canadian attendees.

This work contributed to the smooth operation of the Games, the protection of athletes, officials and spectators, and reinforced Canada's role as a trusted security partner on the international stage.

G7 Summit

In June 2025, Canada hosted the 51st G7 Summit in Kananaskis, Alberta. The Cyber Centre supported the event by deploying experts, delivering cyber defence services, and providing advice to federal, provincial and municipal partners.

CSE maintained a heightened state of readiness to detect, mitigate and respond to any cyber incidents that could have impacted the summit.

Fédération Internationale de Football Association (FIFA) World Cup 2026™

CSE is supporting preparations for the FIFA World Cup 2026™, which will take place across North America.

CSE's Cyber Centre is part of a working group convened by CSIRTAmericas, alongside its American and Mexican counterparts, to strengthen operational, strategic and technical coordination and information sharing. This includes joint efforts to prevent, detect, and respond to cyber incidents.

During the planning phase, the Cyber Centre delivered briefings outlining the national cyber security posture for Canada, Mexico and the United States.

Preparation activities included:

- sharing threat intelligence, enhanced monitoring and awareness briefings
- participating in working groups and tabletop exercises
- supporting government coordination efforts

During the tournament, the Cyber Centre will maintain a heightened operational posture, with personnel deployed to the FIFA World Cup 2026™ Technology Command Center in Miami and to domestic security operations centers.

To maintain situational awareness and sustain operational readiness, COPCC also oversaw CSE's participation in several national security exercises with domestic and international partners throughout the year.

Ever Vigilant

Should crisis situations arise that pose a threat to Canada or Canadians abroad, COPCC is already in place, monitoring events, coordinating responses and ensuring decision-makers have the information they need, when it matters most.

Alerts and advisories

The Cyber Centre observed an increase in the number of vulnerabilities and their severity this year, leading to the publication of a high number of alerts (25) and advisories (995). Informed by foreign intelligence insights, technical analysis and operational reporting, these products helped partners better understand emerging risks and act quickly. This is a 25% increase in alerts and a 28% increase in advisories compared with in 2023–2024.

Notable alerts included:

- the Cisco Software-Defined Wide Area Networks (SD-WAN) network's critical vulnerability, which was accompanied by joint guidance on malicious cyber threats to SD-WAN networks released with Five Eyes partners[3]
- an alert warning about hacktivists abusing Internet-accessible industrial control systems in Canadian critical infrastructure[4]
- the SharePoint zero-day vulnerability

SharePoint zero-day vulnerability

In July 2025, Microsoft disclosed a set of zero-day vulnerabilities affecting on-premises SharePoint servers. Given the extensive threat surface across Canada and the potential for widespread compromise, the Cyber Centre coordinated the Government of Canada's response in collaboration with federal partners.

As part of this effort, the Cyber Centre issued alerts, provided sensor monitoring support, conducted forensic analysis, and published a detailed technical assessment. Through its investigations, the Cyber Centre observed sophisticated exploitation, including the early use of novel techniques and custom in memory payloads to gain persistent access, move laterally within networks, and exfiltrate sensitive data – at times beginning weeks before public disclosure.

The Cyber Centre publication Threat detection for SharePoint vulnerabilities documented how the vulnerabilities were exploited in practice, highlighted the limitations of traditional indicators of compromise, emphasized the importance of patching combined with key and credential rotation, and shared detection and mitigation guidance to help organizations identify and respond to similar activity.

In parallel, the Cyber Centre worked closely with the broader cyber security community to exchange timely information and rapidly notified Canadian critical infrastructure operators about vulnerable systems using our National Cyber Threat Notification System (NCTNS).

National Cyber Threat Notification System

The National Cyber Threat Notification System (NCTNS) is Canada's early warning service for cyber threats, delivered by the Cyber Centre. It monitors cyber threat activity and sends timely notifications to subscribers when cyber incidents, vulnerabilities or other risks are detected.

This year, more than **97,000 notifications** were sent – reaching organizations across the country and providing early warning of potential threats. On average, nearly **450 organizations** were notified each week. As of this reporting period, **1,363 organizations** are subscribed to the service, including **97 newly subscribed organizations**.

These alerts help enable organizations to act early – reducing the likelihood of successful cyber incidents and strengthening Canada's overall resilience.

Pre-ransomware notifications

The Cyber Centre's pre-ransomware notifications help organizations stop cyber incidents before they escalate into data theft or system disruption.

This year, we issued **67 notifications** to Canadian organizations identified as potential targets. Our intelligence partnerships are constantly evolving, and therefore the scope of our notifications to organizations may fluctuate according to the dynamic cyber threat landscape. These included partners across all levels of government and key sectors such as health care, energy, manufacturing, finance and education. By enabling early action, these notifications helped reduce potential operational and financial impacts.

The Cyber Centre's pre ransomware notifications can deliver tangible financial benefits by helping organizations act before incidents escalate. By identifying and alerting potential victims early in the attack lifecycle, these notifications enable organizations to contain threats before encryption or data theft occurs, avoiding costly downtime, recovery efforts and potential ransom payments. In the previous reporting period, this approach contributed to estimated economic savings of up to $18 million across notified organizations, demonstrating the significant value of early intervention.

Protecting Canada's democracy and most critical systems

As cyber threats increasingly target democratic systems and essential services, CSE continues to work with key stakeholders to support the protection of Canada's democratic institutions.

Through proactive outreach, collaboration with specialized intelligence teams, and advanced threat detection tools, we are strengthening critical systems across provinces and territories. This work supports the security and integrity of elections, the resilience of critical infrastructure and the protection of Canadians' daily lives, online and offline.

Supporting federal institutions

CSE and the Cyber Centre work closely with federal institutions to help them prevent, respond to and recover from cyber incidents.

Over the last year, we:

- provided direct assistance during cyber incidents
- produced targeted advice and guidance to reduce cyber risk
- offered tailored briefings to departments affected by malicious activity

Together, these efforts strengthened the collective resilience of federal government and Crown corporations.

Cyber Centre Service Briefings

The Cyber Centre continues to deliver regular service briefings for federal institutions. These interactive sessions help Government of Canada cyber-security teams understand and access available tools and services from the Cyber Centre.

In 2025–2026, **1,330 participants** from **153 departments** took part in these briefings, strengthening awareness and uptake across government.

Quick Connect series

This year, the Cyber Centre launched a Quick Connect series, an online forum for IT and cyber security professionals to share insights and address emerging challenges.

The series brought together approximately **2,300 participants** from **91 Government of Canada (GC) departments and agencies**. It responded directly to demand for a federal collaborative space to discuss technical, operational and policy issues.

Engagements with Crown corporations and Government of Canada departments

The Cyber Centre continues to deepen its engagement with Crown corporations and federal departments to strengthen cyber security across government.

This includes:

- promoting the consistent application of Treasury Board of Canada Secretariat (TBS) cyber security direction
- supporting onboarding to key services, including the Sensors program, which remains one of the Cyber Centre's most effective tools for detecting and blocking malicious cyber activity across systems of importance

These engagements have provided valuable insight into departmental gaps, needs, and operational challenges. They help refine the Cyber Centre's services and ensure support is targeted where it is most needed.

Communications Security: protecting sensitive information

As Canada's communications security (COMSEC) authority, we deliver a comprehensive suite of capabilities to protect the Government of Canada's most sensitive information.

Through our information assurance mandate, we continue to evolve our COMSEC program both technically and strategically to keep pace with sophisticated threats and the demands of an interconnected environment.

This work underpins secure communications across government and with our partners. It includes:

- cryptographic key management
- policy development and compliance
- asset management for cryptographic systems
- the design and delivery of innovative telecommunications solutions grounded in robust research and development

Over the past year, we strengthened our close partnerships with the United States and the United Kingdom, while also building new collaborations on secure communications and mobile solutions. These efforts support how the federal government operates, both at home and with international partners, while improving the tools available to decision-makers to protect government systems and information. Through foresight comes CSE's posture of readiness and resilience, and this is demonstrated through the valuable work done by CSE alongside our allies.

Protecting democratic institutions

As cyber threats to elections and democratic processes continue to grow in scale and sophistication, protecting Canada's democratic institutions remains a priority for CSE.

Over the past year, the Cyber Centre worked closely with federal partners and democratic institutions to help protect the integrity of Canada's elections. We delivered briefings to raise awareness of evolving threats and provided targeted support to strengthen the resilience of operational systems. This work was underpinned by foreign intelligence generated through CSE's SIGINT activities. These insights helped inform efforts to identify and counter PRC state sponsored threats and support the protection of Canada's democratic processes at both the federal and provincial levels, and supporting secure, trusted elections.

Security and Intelligence Threats to Elections Task Force

CSE is a core member of the Security and Intelligence Threats to Elections (SITE) Task Force alongside the Canadian Security Intelligence Service (CSIS), Global Affairs Canada (GAC) and the Royal Canadian Mounted Police (RCMP).

Established in 2019, the SITE Task Force (SITE TF) coordinates government-wide efforts to monitor and respond to threats to federal elections.

Through SITE, CSE shared foreign intelligence on threats to Canada's electoral processes this year, including Canada's 45th General Election in 2025 and the Battle River-Crowfoot by-election. This work, carried out in close coordination with other SITE partners, helped strengthen the Government of Canada's ability to detect, assess and respond to threats targeting democratic institutions.

Working with partners, CSE also supported public attribution of two instances of foreign state-directed information operations on social media platforms aimed at influencing public opinion. This collaboration highlights the effectiveness of the Government of Canada's work in protecting its democratic processes and increasing transparency and public awareness of the threats targeting Canadians online.

CSE continues to monitor for threats to our democratic processes and critical infrastructure year-round to ensure Canadians can have confidence in the institutions that govern on their behalf.

Supporting provinces and territories

Cyber threat actors, including nation-state threat actors, increasingly target all levels of government. Provincial, territorial, Indigenous and municipal governments are most likely viewed as valuable targets for cyberespionage as they hold sensitive information and are key partners in Canada's cyber security ecosystem.

CSE is strengthening collaboration across jurisdictions to improve collective awareness and response.

Following a series of cyber incidents targeting northern institutions, and with the Minister of Defence's authorization, the Cyber Centre began proactively deploying sensors to territorial government IT assets in Yukon, the Northwest Territories and Nunavut in 2024–2025. These sophisticated sensors help detect malicious cyber activity in devices at the network perimeter and in the cloud. They are one of the Cyber Centre's most important tools for defending systems of importance to the Government of Canada.

Through the Provincial-Territorial (PT) Sensor Expansion Strategy, the Cyber Centre is extending sensor services beyond the federal government and territories to protect Canada's critically important systems. Sensors are now deployed across several provinces and all three territories, representing approximately **5%** of the overall sensor fleet. In 2025, these deployments led to roughly **150 prevention and detection reports** shared with PT partners, supporting earlier detection and faster responses to threats.

This year, provinces and territories with access to our sensor services were also granted access to ObservationDeck, an interactive web application that brings together data from Cyber Centre security services to provide a clearer view of their cyber security posture. ObservationDeck reporting is enriched with commercial, open-source and in-house analytics that summarize departmental IT assets and their vulnerabilities.

Federal-Provincial-Territorial cyber security agreement

In fall 2025, provincial, territorial and federal governments reached an important milestone to defend Canadians against cyber threats. The signing of the **Canadian Cybersecurity Collaboration Agreement** strengthens pan-Canadian coordination by enabling more efficient sharing of cyber security information, expertise, and tools across jurisdictions. Through the Cyber Centre, CSE is supporting its implementation by building information-sharing channels, advancing common tools and processes, and working with partners to improve collective readiness for cyber threats. Together, these efforts strengthen Canada's ability to respond to cyber incidents and protect Canadians in an increasingly complex threat environment.

Federal, Provincial, and Territorial Heads of Cyber Roundtable

In April 2025, the Cyber Centre hosted the third-annual Federal, Provincial, Territorial Heads of Cyber Roundtable. Representatives from across Canada met to share insights, strengthen coordination across jurisdictions and discuss priorities such as incident response, supply chain security and regulatory frameworks for critical infrastructure.

This collaboration helps ensure a coordinated, national approach to cyber threats.

Supporting critical infrastructure

Canada's critical infrastructure underpins the safety, well-being and economic security of Canadians. It is also a growing target for cyber threats, from financially motivated criminal activity to state-sponsored attacks. These threats can disrupt essential services that Canadians rely on every day.

> *"Malicious cyber activity targeting Canada's critical infrastructure […] are on the rise and are a real and urgent threat. […] Any disruption to critical infrastructure is not only a threat to public health and safety, but also a threat to public confidence, the environment and the economy."*
>
> *Joint statement on malicious cyber activity targeting Canadian critical infrastructure*[5]

In response, CSE works to protect and defend critical infrastructure, strengthen cyber resilience and reduce risk. Through the Cyber Centre, we partner with organizations across key sectors, including telecommunications, energy, finance, transportation, water, and health. Intelligence collected by CSE helps identify emerging threats to these sectors, allowing the Cyber Centre to deliver more targeted advice, alerts and operational support.

Over the past year, we:

- delivered sector-specific briefings
- participated in tabletop and functional exercises
- provided technical guidance on risks, including signaling vulnerabilities, mobile network security, and supply-chain integrity
- convened national-level forums and communities of practice to help organizations turn guidance into action

Highlights for 2025–2026 include:

- 522 engagements with organizations across key sectors and levels of government
- bi-weekly cyber threat briefings reaching over 1,000 IT security professionals in Canada's critical infrastructure sectors per session
- 8 "Walk-the-Talk" sessions, with an average of 810 participants

Telecommunications sector

Telecommunications networks form the backbone of Canada's internet and remain a top target for foreign espionage. State-sponsored cyber actors continue to exploit these systems to gain access to sensitive information.

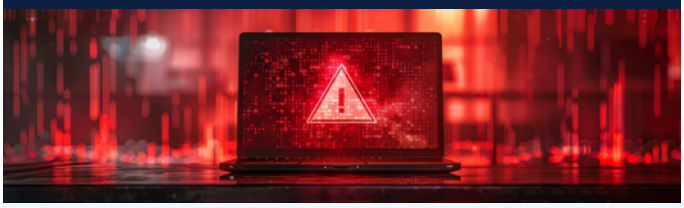
Through the Cyber Centre's Telecommunications Cyber Resilience Program (TCRP), CSE works with Canadian mobile network operators to strengthen the security and resilience of Canada's 3G, 4G, and 5G networks.

In 2025–2026, key efforts included:

- advancing threat hunting activities with Canadian Telecommunications Cyber Protection partners to detect and remove threat actors who are pre-positioned for disruption in Canadian networks
- identifying risks in legacy mobile technologies and promoting mitigation measures to reduce the threat surface across Government of Canada mobile devices

- providing guidance on best practices for embedded subscriber identity module (eSIMs) and embedded universal integrated circuit cards (eUICC), supply chain integrity in mobility and private 5G networks
- conducting targeted testing and sharing mitigation guidance in support for new industry-led efforts to address global signaling threats, and strengthen subscriber-data

Salt Typhoon



In winter 2025, Salt Typhoon emerged as a significant threat to networks worldwide. When these cyber incidents were discovered, the Cyber Centre worked with CSIS alongside international partners to better understand and respond to the threat. This collaboration led to the release of a joint cyber security advisory[6] with the National Security Agency (NSA) and a joint cyber threat bulletin[7] with the Federal Bureau of Investigation (FBI), outlining the threat and the recommended mitigations measures.

The Cyber Centre continues to closely monitor this threat. We are working closely with Canadian telecommunications providers and critical infrastructure operators and publishing cyber threat guidance[8] to help them stay informed and prepared.

Marine transportation

Strengthening the cyber resilience of Canada's marine transportation sector was a key focus this year. Marine transportation is deeply interconnected with Canada's supply chains, and any disruptions – whether to port operations, vessel navigation systems, or cargo handling – can have significant economic and security impacts.

To support this sector, the Cyber Centre published an assessment of cyber threats to marine transportation[9], including ports and connected industries. The assessment identified ransomware and financially-motivated cybercriminal activity as the most significant risks. It also provided practical guidance to help operators strengthen their defences and reduce their exposure to vulnerabilities.

Water sector

Canada's water supply and wastewater systems are essential to public health and safety. While these systems often operate out of sight, they increasingly rely on digital technologies that expose them to cyber threats.

In this evolving threat landscape, water infrastructure now faces risks it was not originally designed to withstand. Recognizing that disruptions can have cascading effects across other critical infrastructure sectors, CSE helps safeguard these essential systems and provides support to enhance their cyber defence.

To raise awareness and promote better protection, the Cyber Centre published an assessment of cyber threats to Canada's water systems[10], with clear guidance and mitigation measures to help water-system operators prevent cyber threat actors from compromising their systems, disrupting their services or stealing sensitive data.

Unauthorized access to a Quebec water treatment plant

On October 7, 2025, CSIRTAmericas relayed NoName's claim of unauthorized access to a Quebec municipality's water treatment plant, including the ability to covertly control pumps, chlorine dosing, pressure settings and monitoring/alerts systems. This timely intelligence allowed the Cyber Centre to rapidly assess the threat and work with partners to coordinate mitigation efforts, helping to reduce the risk to public safety.

Supporting critical infrastructure also depends on helping partners understand the threat environment. To complement direct support and operational engagement, CSE translates intelligence and frontline observations into threat reporting that organizations can act on.

Assessing and reporting on cyber threats

Providing timely and practical threat information is a core part of how CSE supports partners.

Throughout the year, the Cyber Centre delivered unclassified assessments, technical reports, and threat bulletins to help organizations understand emerging risks and take action. Many of these products drew on a combination of foreign intelligence, technical analysis and operational insights, reflecting CSE's integrated approach to threat awareness and cyber defence. This included the publication of the Ransomware Threat Outlook 2025-2027[11], as well as six unclassified threat assessments and bulletins:

- Cyber threat bulletin: People's Republic of China (PRC) cyber actors target telecommunications companies as part of a global cyberespionage campaign[12]
- Cyber threat bulletin: Iranian cyber threat to Canada from Israel-Iran conflict[13]
- The cyber threat to Canada's water systems: Assessment and mitigation[14]
- The cyber threat to marine transportation[15]
- Cyber threat bulletin: Iranian Cyber Threat Response to US/Israel strikes[16]
- Cyber threat bulletin: People's Republic of China-sponsored cyber activity against Canadian provincial, territorial, Indigenous, and municipal governments[17]

Ransomware Threat Outlook 2025 to 2027

The Ransomware Threat Outlook (RTO) 2025-2027[18] provides a clear picture of how the ransomware threat is evolving in Canada. It helps Canadian organizations understand how the threat is evolving, while also offering practical advice and guidance from the Cyber Centre to strengthen cyber resilience and prepare for cyber incidents.

The report also explains the early history of ransomware, outlines emerging and projected trends, and debunks common myths and misconceptions about cyber hygiene and incident response. The RTO highlights four key findings:

- **Ransomware is a growing threat:** Threat actors are using more advanced tools and techniques, increasing the scale and impact of attacks.
- **Threat actors are evolving:** They are leveraging new technologies – like artificial intelligence and cryptocurrency – and developing new extortion tactics to increase their financial reward.

- **Basic cyber hygiene works:** Regular software updates, multi-factor authentication (MFA), and vigilance against suspicious activity remain the most effective defences.
- **Collaboration is essential:** Governments, industry, law enforcement and individuals all have a role to play in reducing risk.

The RTO generated strong media interest and widespread coverage following its release in January 2026, helping raise awareness of the ransomware threat across Canada.

Understanding threats is only part of the response. CSE also turns this knowledge into practical guidance, tools and technical analysis to help defenders strengthen resilience and reduce cyber risk across Canada. Together, CSE leverages the full breadth of its authorities to keep Canadians safe from cyber threats.

Strengthening Canada's cyber resilience and defence

Cyber threats continue to grow in scale and sophistication. Threat actors are constantly adapting, finding new ways to target organizations and individuals. As cyber threats continue to evolve, so does the guidance available to Canadians.

The Cyber Centre provides practical, accessible guidance to help Canadians stay ahead of these threats. Whether supporting government, critical infrastructure or individuals, this guidance helps strengthen defences and improve readiness across the country.

Cyber guidance publications

This year, the Cyber Centre published a wide range of guidance to support organizations and individuals, from technical practitioners to senior leaders in government and the private sector.

Topics included artificial intelligence, cloud security, drone use and emergency preparedness. This work also advanced secure-by-design practices across government, including through enterprise security architecture guidance for departments.

We also improved how guidance is developed and released, enabling faster and more coordinated delivery.

In total, we published:

- 41 cyber security guidance publications
- 28 joint publications with our Five Eyes and other international partners

Top 10 artificial intelligence security actions: A primer

In March 2026, the Cyber Centre released timely guidance for Canadians to adopt security actions specific to threats linked to AI[19]. As individuals and as a society, these actions matter so that confidential information remains in the rightful owner's hands, and so that hard-earned money isn't stolen from victims because of AI-enabled theft. As AI models evolve over time, this calls for continuous monitoring and human oversight for critical decisions to ensure AI systems remain within acceptable risk boundaries.Organizations are encouraged to implement these Top 10 IT security actions[20] to protect their Internet connected networks and information from cyber security threats.

Tools to help defenders stay ahead of threats

The Cyber Centre continues to expand its suite of open-source tools, to support cyber defenders and promote secure-by-design practices.

In October 2025, we released **Clue**, an enrichment framework that helps analysts discover, investigate, triage and report cyber security incidents more quickly. Clue integrates with other Cyber Centre open-source tools and is available on GitHub.

At the same time, our malware analysis system, **Assemblyline**, processed record-high volumes this year, enabling faster analysis for the Government of Canada and its partners.

By accelerating how quickly threats are identified and understood, these tools help defenders respond sooner – reducing the risk of disruption to critical systems and services Canadians rely on every day. As the pace of cyber threats increases, our innovative work with tools like Clue and Assemblyline helps ensure Canada stays ahead of threats and strengthens its digital frontline.

Technical analyses

The Cyber Centre also published several high-impact technical analysis reports to help Canadian organizations understand emerging threats.

These reports draw on real-world investigations and large-scale observations, providing insight into how modern attacks are carried out by both criminal and state-aligned actors and how to defend against them.

This year, we published three technical analyses on:

- adversary in-the-middle threats with phishing-resistant multi-factor authentication[21] targeting Entra ID (formerly Azure AD)
- threat techniques used to exploit on premises SharePoint[22]
- EtherHiding[23] – an attack involving malicious code hidden in developer tools

By sharing detailed findings, indicators and defensive recommendations, the Cyber Centre helped cyber defenders strengthen detection and improve their organization's overall cyber resilience.

Strategic defence and security enhancements

As global security challenges continue to evolve, Canada must be ready to defend its territory and values, secure its sovereignty and support its commitments to allies.

The nature of conflict has evolved beyond physical battlefields to include cyberspace, and digital domains. Advances in AI, quantum computing, and autonomous systems are redefining how countries protect their interests and advance their security goals.

Over the past year, CSE has laid the groundwork to advance key national security, defence and resilience priorities. These upgrades reflect a shared commitment across CSE, the Canadian Armed Forces, and the broader security and intelligence community to defend Canada and protect Canadians. Together, we are working toward a common goal: strengthening the country's national security in an increasingly complex threat environment. This includes:

- advancing **modern, secure digital infrastructure and tools** for the Canadian Armed Forces and the security and intelligence community
- scaling up our cyber defence capabilities to **assist today's military operations**
- working with government, academia and industry to develop **made-in-Canada AI solutions**

CSE continues to drive innovation and resilience, reinforcing Canada's ability to operate securely, decisively and confidently in an increasingly complex security environment.

Contributing to a sovereign and secure digital Canada

As CSE continues to drive innovation and resilience, Budget 2025 recognized the organization's critical role in reinforcing Canada's ability to operate securely, decisively and confidently in an increasingly complex security environment. This significant investment in CSE will enable a multi-year transformation that will bolster national security, economic competitiveness and digital sovereignty, while enhancing the interoperability of systems across Canada and with international partners.

Driving digital transformation and resilience

Working with partners across the defence, security and intelligence community, CSE will improve how information is analyzed and securely shared, especially during crisis and conflict. Generational investments will strengthen Canada's ability to:

- safeguard sensitive information, communications and operations
- deliver modern and high-performance capabilities
- integrate emerging technologies like artificial intelligence to support more informed decision-making
- collaborate securely with trusted allies

Delivering these capabilities requires resilient, high-performance computing infrastructure and a highly skilled workforce. To that end, CSE has begun planning its data centre and real property requirements, prioritizing investment in Canadian communities and industries. These foundational investments will support the growth of CSE's national footprint, allowing the organization to scale as its needs evolve.

Expansion of CTSN footprint

CSE continues to expand and modernize its secure communications infrastructure to support operations across government and meet the growing need for access to intelligence. This includes the rollout of a more resilient and unified Canada's Top Secret Network (CTSN), enabling secure access to intelligence for more departments and agencies.

This year, CTSN grew to eight federal members and continued to support operations abroad through portable secure workstations. Together, these capabilities provide flexible, secure connectivity for users across Canada and internationally.

Cloud computing solutions

CSE continues to advance cloud computing solutions that support the Government of Canada's classified cloud strategy, in partnership with the Department of National Defence and Shared Services Canada. High-security organizations like CSE and DND work every day with classified information that requires enhanced protection and secure digital infrastructure. CSE and our government partners are aware of the critical place of cloud computing within a broader set of technical capabilities for future-proofing Canada's national security and communications infrastructure. Through its reach into cyber security, quantum, artificial intelligence, and cryptography, this further solidifies Canada's control over sensitive data.

Canadian cryptography and the transition to post-quantum

As Canada's national authority for foreign signals intelligence, cyber security and information assurance, we play a key role in anticipating emerging cryptographic threats, including those linked to advancements in quantum technologies.

CSE is leading efforts across government to prepare for a secure transition to post-quantum cryptography (PQC), strengthening our COMSEC program, and working with partners and Canadian industry to develop secure, flexible solutions that can adapt to evolving threats and meet future demands. This year, in close collaboration with our trusted allies, CSE also worked to improve the private sector's understanding of the Government of Canada's cryptographic security needs, enabling greater participation and supporting the growth of a domestic industry.

This year, CSE published the Roadmap for migration to post-quantum cryptography for the Government of Canada[24]. It provides departments with a clear, phased approach to support planning and implementation. To support adoption, the Cyber Centre also delivered a learning series to help government employees build awareness and readiness. In parallel, we advanced quantum-safe procurement by working closely with Public Services and Procurement Canada (PSPC) and Shared Services Canada (SSC) to integrate PQC requirements into federal contracting.

CSE also strengthened coordination and international engagement by:

- chairing an interdepartmental PQC migration working group
- leading the G7 Cybersecurity Working Group on post-quantum readiness
- contributing to standards development

The concepts of defending Canada and building Canada are not mutually exclusive. Under the Defence Industrial Strategy, enhancing our cryptographic security today will ensure Canada retains its sovereignty for future generations.

Supporting Canada's Defence Industrial Strategy

Canada has entered a new era of national defence investment, and CSE is directly supporting the Defence Industrial Strategy (DIS)[25]. The strategy mobilizes resources across the country to strengthen Canada's technological capacity, build domestic expertise and reinforce Canadian sovereignty.

As defence operations increasingly depend on digital systems, CSE is supporting Canada's ability to keep pace, by advancing research and innovation, supporting resilient supply chains and working with industry to enable modern capabilities.

> *"The changing nature of war is reshaping global security. Conflict now extends beyond traditional battlefields into cyberspace, space, and the digital domain, driven by technologies such as AI, quantum, autonomous systems, robotics, and advanced cyber and space capabilities. Countries are racing to harness commercial innovations not only to safeguard sovereignty, but also to capture the economic advantages they bring."*
>
> *Canada's Defence Industrial Strategy*[26]

Bureau of Research, Engineering and Advanced Leadership in Innovation and Science (BOREALIS)

A key initiative supporting the DIS is the Bureau of Research, Engineering and Advanced Leadership in Innovation and Science (BOREALIS).

By bringing together government, academia, and industry, BOREALIS provides a central hub to advance defence and national security innovation. It focuses on accelerating the development of cutting-edge capabilities in defence and security technologies such as AI and quantum computing.

As a member of the BOREALIS Joint Program Office (JPO), CSE is helping to advance this initiative and shape its direction.

This year, CSE helped define priorities for BOREALIS, supported policy development and worked with industry and academia in order to advance a new approach to partnerships between government, academia and industry on defence technologies.

Artificial intelligence

Over the past year, CSE continued to advance its Artificial Intelligence Strategy[27], expanding our ability to use AI tools while embedding strong governance, risk-management and ethical safeguards.

AI is not new to CSE. For years, we have developed, adapted and applied AI, automation, machine learning and data science tools to help our people work more efficiently, generate faster insights and strengthen our operational capabilities.

Investments in advanced technologies are enabling CSE to scale the use of AI across its mission. This includes improving efficiency across the organization by automating routine tasks, supporting faster analysis and helping employees focus on higher-value work. At the same time, these technologies are strengthening threat analysis, cyber defence and cyber security in a threat environment that is evolving faster and becoming more complex.

CSE actively engages with government partners, academia and industry to share insights, align on best practices, and advance shared priorities in responsible AI. These partnerships are helping equip our workforce with cutting-edge tools and expertise while enabling secure and tailored solutions that improve operational effectiveness and help defend Canada against AI-enabled cyber threats.

As AI capabilities evolve rapidly, including increasingly capable frontier models, CSE continues to track these developments closely and adapt at pace. We are actively monitoring and countering the misuse of AI by malicious actors, as these tools can enable more sophisticated, scalable and persistent cyber threats while shortening the time between vulnerability discovery and exploitation.

Our leadership and technical expertise in the understanding of frontier AI is helping to ensure these technologies are adopted securely and responsibly across Canada. This includes working closely with partners, particularly in critical infrastructure sectors, to strengthen resilience and prepare for more advanced threats. We continue to share intelligence with allies and advance research to help Canada stay ahead of evolving AI-enabled threats.

By combining long-standing expertise, responsible innovation and strategic partnerships, CSE remains well positioned to apply AI in ways that support Canada's national security, economic prosperity and democratic values.

Using AI to strengthen foreign intelligence analysis

CSE is integrating AI solutions to strengthen signals intelligence analysis by improving how analysts work with large and complex data. By applying these technologies within clear risk frameworks and guardrails, Canada can improve operational effectiveness while maintaining the trust, accountability and human oversight needed for responsible use.

We are currently testing new approaches that:

- automate repetitive, data-intensive tasks
- help analysts focus on higher-value analysis and decision-making
- improve how information is searched, understood and used

As an example, CSE is developing an AI-enabled tool that can:

- translate data from over 200 languages into English and French using Large Language Models (LLMs)
- extract relevant information from large datasets
- support conversational queries through chat-based interaction, enabling analysts to ask natural, conversational questions
- improve search accuracy using semantic analysis, allowing analysts to query data by taking the intent of the text into considerations, beyond simply matching keywords
- organize and analyze data using topic modeling, which lets analysts visualize the data by theme or topic

MOBILIZING RESEARCH AND PARTNERSHIPS TO SAFEGUARD OUR FUTURE

Safeguarding Canada's future and staying ahead of evolving threats requires more than technology – it requires collaboration.

Through research and partnerships, CSE develops the tools and capabilities needed to meet today's cyber challenges and prepare for those ahead. Because no single organization can meet these challenges alone, we partner with all levels of government, critical infrastructure operators, academia, and international allies. Together, we address complex cyber challenges collectively, strengthening Canada's digital sovereignty and building a more resilient cyber ecosystem.

Advancing mission-critical capabilities through research

CSE turns innovative ideas into operational solutions. Working with partners across government, academia and industry, our Research Directorate explores ways to address complex and persistent challenges as part of CSE's mission.

Artificial intelligence and machine learning research

This year, our AI and machine learning (ML) researchers focused on the development and responsible application of AI/ML in secure environments. They developed and tested custom models for CSE to use in high-priority cases, like the need to analyze a high-volume of multimedia data. They also created evaluation datasets to ensure that CSE and its partners can properly assess ML model behaviour before integrating them into operations.

Outside the lab environment, our AI/ML researchers provided expertise and support across CSE and to partners by:

- organizing sessions with Five Eyes partners and other Government of Canada departments
- participating in CSE's flagship innovation and collaboration workshops, such as BIG DIG, Kickstart and Geek Week
- scheduling monthly ML office hours sessions
- delivering practical training, including data science modules

This work ensures AI is applied responsibly, effectively and in ways that support operations.

Vulnerability research

Through our Vulnerability Research Centre (VRC)[28], we are conducting applied research to identify and address cyber vulnerabilities, in support of our mandate.

Over the last year, work with the Royal Military College of Canada's Computer Security Lab led to new detection techniques and the responsible disclosure of three vulnerabilities to industry partners, such as Microsoft and Netgear.

These efforts help reduce risk across the broader cyber ecosystem.

Tutte Institute for Mathematics and Computing

Over the past year, the Tutte Institute for Mathematics and Computing (TIMC) continued to develop foundational theory, innovative techniques and effective tooling in two focus areas: mathematical foundations of cryptography and foundations of AI/ML. Engagement and collaboration with vibrant research communities in the classified and unclassified spheres have enabled TIMC to deliver impactful research results across both areas.

Contributing to scientific advancement

TIMC strives to share its activities and tools regularly with the public and academic community.

This year, TIMC's contributions included:

- publishing 10 journal articles and 1 book
- producing 16 software releases of new or significantly updated code
- organizing 3 conferences
- editing 1 conference proceedings
- giving 6 invited talks and 3 presentations at external conferences
- holding positions on the Canadian Mathematical Society Board and committees

In addition, software libraries from TIMC reached a wide audience, with over 6.5 million downloads each month, extending Canada's influence in cyber and mathematical research.

Engaging with universities in the National Capital Region

Locally in Ottawa and Gatineau, TIMC works with universities to develop highly qualified personnel by sponsoring university-led events and collaborating on academic research.

Supporting mathematics and computer science conferences

TIMC is committed to fostering strong partnerships and providing broad support to the Canadian scientific community. In 2025-2026, TIMC sponsored eight mathematics and computer science conferences that align with its research interests.

NSERC-CSE research communities

Through our partnership with the Natural Sciences and Engineering Research Council of Canada (NSERC), we support research communities conducting unclassified research on cutting-edge technologies of strategic importance to CSE and the Government of Canada.

This year, we were pleased to announce the creation of the NSERC-CSE Research Community on Exploratory Analysis of Unstructured Data for the project "ZenithVector: Advanced Vectorization, Embedding, and Cybersecurity Analytics Toolkit for Scalable Intelligence"[29]. Led by McGill University, this community brings together researchers from 10 Canadian universities to study large-scale data analysis.

The goal is to develop a comprehensive, multimodal solution for the exploratory analysis of large collections of unstructured data (like text, code, and images). The project integrates advanced techniques to develop the building blocks necessary to understand, explore, and visualize collections of unstructured data in a way that makes sense to the human brain.

This is the second of four communities created as part of the NSERC-CSE Research Communities grants[30].

New research engagement space in Toronto

CSE regularly seeks opportunities to strengthen collaboration with Canadian researchers. Through a new partnership with the National Research Council of Canada (NRC), we are working to expand our presence and establish a new engagement space in downtown Toronto. Located in the city's academic core, the space will support in-person engagement, knowledge sharing, and research partnerships. The proximity to the Fields-NRC Mathematical Collaboration Centre will help deepen links between government research and Canada's academic mathematics community.

Protecting Canada through a whole-of-society approach

Cyber security is a shared responsibility.

The complexity of today's threats means no single organization, public or private, can address them alone. At CSE, we seek out diverse perspectives within government and beyond to strengthen our collective knowledge and capabilities, enhancing our ability to carry out our mission.

The Canadian Cyber Defence Collective

Under the National Cyber Security Strategy (NCSS), the Government of Canada established the Canadian Cyber Defence Collective (CCDC) this year. Its mission is to advance and strengthen Canada's cyber resilience through direct public-private responses to national-level cyber security challenges, policy priorities, and operations.

The CCDC ensures that critical infrastructure operators, businesses, provincial and territorial governments, municipal governments, Indigenous governments, and everyday Canadians benefit from shared intelligence, innovations, and best practices. This initiative strengthens Canada's ability to detect, prevent and respond to malicious cyber activity, creating a safer digital landscape for Canadians.

The CCDC includes two separate forums: the Canadian Cyber Defence Collective Operations (CCDC-O) and the Canadian Cyber Defence Collective Strategic Forum (CCDC-SF).

The CCDC-O is chaired by the Cyber Centre and is responsible for:

- leveraging partnerships to coordinate national responses to cyber threats
- contributing to the development of cyber threat intelligence
- strengthening information sharing
- developing technical mitigation strategies for cyber security challenges
- co-developing cyber defence solutions, including establishing a tiered engagement strategy to work in partnership with cyber defender communities

The CCDC-O includes a select group of trusted national and international cyber defender partners from both the public and private sectors. Initial bilateral meetings and multilateral group meetings were initiated and operationalized in 2025, which led to the start of operational and analytical collaboration.

The group focused on putting in place the initial partnerships, processes and technology needed to support coordinated work with industry partners.

The CCDC-SF, co-chaired by Public Safety Canada (PS) and the Cyber Centre, is the national advisory committee on cyber security matters. Members include public and private sector stakeholders who participate in macro-level discussions, inform national-level priorities, and advance a unified voice for Canadian cyber security solutions.

Regional presence in Montreal

To better engage with industry and critical infrastructure partners across Canada, the Cyber Centre recently established a regional office in Montreal.

This local presence makes services more accessible, deepens relationships with key partners in all levels of government and beyond, and enables two-way information sharing.

In 2025, the Montreal team led more than 100 outreach and engagement activities throughout the cyber security and intelligence field. These included:

- speaking engagements
- panel discussions
- service briefing
- collaboration with recruitment teams at job fairs
- joint presentations with other Montreal based security and intelligence organizations
- classified cyber threat briefings for cleared partners

Early feedback from local stakeholders has been positive.

Chief's advisory breakfast series

CSE continues to deepen partnerships with industry.

Through initiatives such as the Chief's Advisory Breakfast series, we are connecting with leaders across sectors to discuss shared challenges and opportunities.

This year, these sessions aimed to facilitate conversations on key CSE priorities, such as:

- attracting, developing, and retaining talent in Canada's IT, defence, and security and intelligence fields
- the dynamics and opportunities for greater collaboration and partnership between CSE, the Government of Canada, industry and academia

The Advisory Breakfast series supported CSE's efforts to deepen our engagement with industry partners. This dialogue helps shape our work and ensures we remain responsive to Canada's evolving needs.

Testing and evaluating industry solutions

To accelerate innovation, CSE is improving how it tests and adopts new technologies.

We recognize the importance of industry contributions to innovation and its potential to support our national security mandate; however, there are challenges to advancing pilot projects within our secure environment.

This year, we partnered with an external facilitator to speed up our ability to test and evaluate unclassified industry solutions. The first task authorization enabled operational teams to assess multiple industry solutions at once, accelerating the transition from pilot project to scalable capability and helping inform future procurement decisions. Additional tasks are still under development.

Partnerships with Indigenous communities

The Cyber Centre works in partnership with Indigenous communities to strengthen cyber resilience and support shared security priorities.

Our dedicated Indigenous Engagement team builds nation-to-nation relationships grounded in respect, recognition of rights, and collaboration. We follow the principle of "Nothing about them without them", ensuring that initiatives and projects are co-developed and reflect the unique needs and priorities of communities.

This year, the team:

- contributed to the Arctic Security Working Group, bringing together federal, territorial and Indigenous governments
- participated in the National Indigenous Information Technology Alliance Conference
- provided cyber security advice, services and guidance to Indigenous organizations
- strengthened relationships with Indigenous organizations to support cyber incident response and coordination
- shared a cyber threat bulletin on PRC-sponsored cyber activity against all levels of government with Indigenous governments
- worked with partners to integrate cyber incident communications and threat briefings into trusted federal-Indigenous channels
- supported leadership engagement, including Inuit-led discussions, which led to increased collaboration and proactive incident outreach

From January to March 2026, the Cyber Centre joined federal partners from Global Affairs Canada (GAC), the Department of National Defence (DND), the Canadian Security Intelligence Service (CSIS) and Innovation, Science and Economic Development (ISED) to deliver tailored briefings to Indigenous communities on the threat landscape in the North. These efforts led to strengthened relationships between Indigenous communities and the Cyber Centre, allowing us to provide customized advice and services to increase their cyber resilience.

In February 2026, Cyber Centre executives held active roles at the Arctic Security Summit, where they delivered a keynote and participated in a panel discussion. Held in Whitehorse, the event brought together Indigenous communities, Arctic partners and decision makers to strengthen relationships with one another on the topics of cyber threats, cyber resilience, and best practices in Northern and remote communities.

Contributions to ShadowServer

This year, the Cyber Centre worked with the nonprofit organization ShadowServer to exchange security alerts. Working under a shared goal to collect and analyze global threat data, ShadowServer shared vital insights that fed into the Cyber Centre's National Cyber Threat Notification System. In turn, the Cyber Centre contributed expertise and advice to the ShadowServer community to improve the detection and reporting of critical vulnerabilities and compromised devices.

International partnerships

Cyber threats are global – they ignore borders and move fast. International collaboration is essential to Canada's whole-of-society approach to cyber security.

By working with allies, including Five Eyes partners, CSE advances shared priorities and supports collective efforts to promote cyber resilience, stability and responsible behaviours in cyberspace.

United Nations Open-Ended Working Group (OEWG) on Information and Communications Technology (ICT)

CSE supports Global Affairs Canada in advancing Canada's role in the UN Open-Ended Working Group (OEWG) on Information and Communications Technology (ICT).

Through this work, CSE contributed to the development of rules, norms, and principles for responsible State behaviour in cyberspace. Following the conclusion of the OEWG's four-year mandate in July 2025, member states agreed to establish a permanent mechanism to carry forward and deepen discussions on ICTs in the context of international security. CSE will continue to support Canada's participation.

G7 Cybersecurity Working Group

During Canada's 2025 G7 presidency, CSE and Public Safety Canada co-chaired the G7 Cybersecurity Working Group, advancing international cooperation among G7 national cyber security authorities. Under Canadian leadership, CSE co-developed technical guidance on AI, post-quantum cryptography, and other key topics. The group also supported a shared understanding of operational and policy approaches that promote cyber security culture and issued a joint statement on improving the security of Internet of Things (IoT) products.

Integrating closer relationships with NATO

The Cyber Centre is strengthening collaboration with NATO partners on cyber defence.

An important visit in early 2026 to the NATO National Cyber Security Centre (NCSC) and the NATO Communications and Information Agency (NCIA) advanced discussions on shared capabilities, tool sharing, and opportunities for Canada to support emerging NATO initiatives. These engagements reflect strong mutual interest in deeper collaboration. The option of deploying a Canadian integree to support this work is under consideration.

Strengthened relationships between Cyber Security Incident Response Teams (CSIRT)

Over the past year, the Cyber Centre strengthened relationships with allied CSIRTs across several NATO countries through bilateral engagements and technical exchanges. It also worked closely with U.S. partners to support cyber preparedness for the FIFA World Cup 2026™.

These efforts enhanced trusted partnerships and enabled the exchange of operational knowledge, best practices, and threat information.

Pacific Cyber Security Operational Network

The Cyber Centre stands ready to support like-minded partners and technical experts from around the world, including in countries in Australasia and the Pacific Islands through the Pacific Cyber Security Operational Network (PaCSON).

This year, the Cyber Centre:

- delivered training and briefings on Assemblyline and the use of AI to enhance threat intelligence analysis and how to communicate with diverse audiences
- strengthened the security posture of members through rapid, bi-directional threat intelligence sharing
- helped them build their information sharing infrastructure and processes
- sponsored their participation at GeekWeek

Building national resilience through education and outreach

CSE builds national resilience by strengthening digital literacy, awareness, and preparedness. Through education and outreach initiatives, we equip Canadians and organizations with the knowledge and confidence they need to navigate the digital environment securely.

Learning Hub courses and resources

As the cyber threat environment evolves, training and upskilling today's workforce is essential.

The Cyber Centre's Learning Hub provides trusted cyber security training for those working within the Government of Canada, other levels of government, critical infrastructure, small and medium-size organizations, and educators.

This year, **6,585 participants** completed training offered through the Cyber Centre Learning Hub. Courses are regularly updated and cover topics such as post-quantum cryptography, generative AI and cyber incident management.

Demand for cyber security professionals continues to grow across Canada. In response, many academic institutions have introduced dedicated cyber security programs. To support Canada's future workforce, the Learning Hub maintains a searchable database of programs across Canadian post-secondary institutions[31]. With over 30,000 views, this resource helps students and professionals explore career pathways and supports the growth of Canada's cyber talent pipeline.

Telfer Cyber Range Program

Strong leadership is critical to managing cyber risks.

This year, the Cyber Centre partnered with the University of Ottawa's Telfer School of Management to expand professional development through the uOttawa-IBM Cyber Range. Building on Telfer's Leadership Crisis Simulation, this immersive environment allows leaders to practice responding to real-world cyber incidents.

Through this partnership, the Cyber Centre expanded the Cyber Range's offerings with new crisis simulations, scenario catalogues and professional development programs grounded in real threats. By combining expertise in threat intelligence, cyber defence and critical infrastructure protection, the program prepares executives and frontline experts to prevent, respond to and recover from cyber incidents.

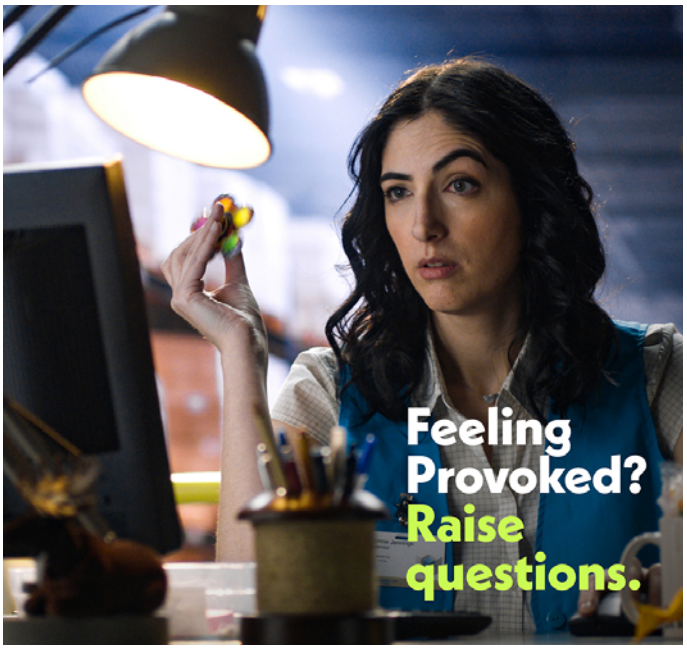
Together, the Telfer program and the Cyber Centre aim to equip leaders with the strategic skills needed to safeguard Canadians and the systems they rely on.

Online disinformation campaign

Concerns about online disinformation and its impact on society have increased in recent years. Foreign state actors use digital platforms, social media and emerging technologies such as artificial intelligence to spread false or misleading information, undermine trust and amplify social divisions. Online disinformation can also pose a serious threat to democratic processes, including by attempting to undermine confidence in elections, discredit people and news sources, and polarize public debate.

In early 2024, CSE launched a national awareness campaign[32] to encourage Canadians to think more critically about the information they encounter online. The campaign, which continued during the 2025 federal election period, featured the message "*If it raises your eyebrow, it should raise questions*" and encouraged Canadians to pause, verify information, and think before sharing content.

The campaign reached Canadians on platforms where disinformation most often spread, including social media and other digital channels. The ads were displayed over 44 million times and generated over 250,000 visits to the online disinformation webpage[33].



Community outreach

Community is at the heart of the CSE's work in keeping Canadians safe, and our programming tailored to different demographics.

Through our community outreach program, we help build pathways into Science, Technology, Engineering and Mathematics (STEM) and cyber careers, especially for groups that may face participation barriers and are underrepresented in the field. This includes partnerships with not-for-profit organizations, schools and community groups.

In 2025-2026, our support to the CyberSci[34] cyber security challenge led to top awards:

- Team Canada earned second place in the guest category at the European Cybersecurity Challenge. This marked CSE's fourth-consecutive year sponsoring and coaching the team.
- Team Canada placed fifth overall at the International Cybersecurity Challenge. This marked CSE's first year sponsoring the team.

We also supported organizations and initiatives such as:

- Hackergal
- Colourfully Digital
- Conseil des écoles catholiques du Centre-Est
- Raspberry Pi

Beyond youth programs, the Cyber Centre provides practical guidance, threat information, and tools to help organizations and communities understand emerging risks and improve their cyber readiness.

Get Cyber Safe campaign

Through our Get Cyber Safe national public awareness campaign, CSE provides cyber security advice to help Canadians protect themselves online.

This year, the campaign continued to expand its reach beyond both official languages by offering select resources in Ojibwe, Cree, Inuktitut, and Mi'kmaq – making cyber security information more accessible to Indigenous communities across the country.

Throughout the year, we delivered regular content, promoted our most popular resources, and supported nation-wide engagement through our digital channels.

New and updated resources released this year included:

- How to spot romance red flags[35]
- Phishing scams you're more likely to encounter when travelling[36]
- Social media habits that could hurt you (and how to strengthen your cyber security)[37]
- How to talk to your loved ones about cyber security[38]
- new videos on Backups[39] and Password Managers[40]
- a new quiz called How Hackable are you?[41]

Get Cyber Safe continues to show how CSE connects with Canadians, protecting not only national infrastructure, but also the everyday digital lives of millions.

Cyber Security Awareness Month

Each year, countries around the world take part in Cyber Security Awareness Month (Cyber Month) to encourage everyone to protect their online activities and personal data.

Here in Canada, the Get Cyber Safe campaign[42] is led by CSE and is supported by helpful advice and guidance from the Cyber Centre.

This year's theme **"Get cyber safe – for future you"** encouraged Canadians to take simple steps today to protect themselves tomorrow.

Over five weeks in October, Canadians heeded the call to become more cyber aware by sharing their success stories, adding campaign hashtags to their social-media posts in both languages, and by simply talking about the importance of Cyber Month with their colleagues, their friends and their family. From likable videos to a catchy unique full length country pop song[43] and cross-platform content, the campaign was a national conversation-starter and it was delivered with a tone that was equal parts informative, inclusive, and practical.

National partners from both private and public sectors supported the campaign by co-creating and sharing content. More than 310 organizations used our Cyber Month resources to connect with their audiences.

Over the course of Cyber Month, the campaign's content:

- was seen over 356,000 times, up from 293,000 in the previous year
- was shared by 253 unique social media accounts
- had 210,081 impressions and a reach of 2.6-million users
- generated 82,709 website visits, up from 73,081

Community outreach

Get Cyber Safe ambassadors engaged directly with Canadians through in-person outreach at the Markham Fall Fair and at Carrefour Laval. Visitors took part in an interactive quiz about cyber habits and a multifactor authentication (MFA) challenge that demonstrated biometric verification methods. Participants received prizes and take-home resources to reinforce cyber-safe behaviours throughout the year.

Around 136,000 people engaged with the outreach elements, with 32,483 confirmed impressions. Average booth visits exceeded eight minutes, compared to the industry average of three to five minutes. This shows that Canadians are taking an active interest in protecting their online activity while engaging with CSE and Cyber Centre guidance along the way.

Cyber security workshops

In alignment with Cyber Security Awareness Month, CSE supported the delivery and promotion of three free online cyber security workshops[44], in partnership with MediaSmarts, designed specifically for older adults. The sessions focused on practical digital safety skills, including creating strong passwords, recognizing and avoiding online scams, securing personal devices, and identifying misinformation.

CTV Deception Decoded segment

As interest in cyber security grows across all demographics, CSE continued to work with national media to raise awareness of cyber threats and practical advice Canadians can take to protect their online footprint.

On February 25, 2026, Rajiv Gupta, the Head of the Cyber Centre, participated in CSE's first live appearance in the CTV News series: Deception Decoded. The segment, "Canada's critical infrastructure is being targeted in cyber attacks[45]," highlighted the growing threat to critical infrastructure and reinforced the importance of basic cyber hygiene, such as strong passwords and multi-factor authentication to make it more difficult for threat actors to access valuable information stored online.

CSE will continue to take part in the series alongside national security partners to support public understanding of evolving cyber threats.


WE BUILD TRUST
THROUGH ACCOUNTABILITY
AND TRANSPARENCY

CSE's ability to deliver on its mandate depends on the trust of Canadians and our partners. We build and maintain that trust by being as open and transparent as possible about how we operate and how we are held accountable. While much of our work must remain classified to protect national security, we are committed to sharing meaningful information about our activities.

Our Annual Report is one way we support this commitment, alongside responding to access to information requests, appearing before Parliamentary Committees, and conducting audits. We ensure all actions are lawful, responsible and aligned with Canadians' expectations. Independent oversight, strong governance, ongoing monitoring, and rigorous compliance practices – including measuring internal compliance – help hold us to account and reinforce public confidence.

Evolving our operational policy framework

CSE has a robust policy suite that is responsive to operational needs and supports teams in conducting their activities in line with the Government of Canada's legal and policy requirements. CSE's operational policy framework guides all operational activities. It sets out clear rules and responsibilities to ensure we operate within the law and meet Government of Canada requirements as we deliver on our mandate.

In 2025–2026, we updated key parts of this framework to reflect today's complex world and rapidly evolving technologies. These updates help us meet Canada's intelligence priorities and protect critical systems from cyber threats.

We regularly review and update our policies and framework to keep pace with change. This includes:

- changes to Ministerial Authorizations (MAs)
- new operational activities and technologies
- feedback from independent review and oversight bodies
- addressing gaps, inconsistencies or areas requiring clarification

Ministerial orders

Ministerial Orders (MOs), issued by the Minister of National Defence, set out who CSE can support and what systems are considered important to the Government of Canada.

As of March 31, 2026, six Ministerial Orders were in effect for CSE. These orders designate:

- recipients of Canadian identifying information (CII) under the foreign intelligence aspect of CSE's mandate
- recipients of information relating to a Canadian or a person in Canada under the cyber security aspect of CSE's mandate
- electronic information and information infrastructures of importance to the Government of Canada
- electronic information and information infrastructures of the Government of Latvia as being of importance to the Government of Canada
- electronic information and information infrastructures of the Government of Ukraine as being of importance to the Government of Canada
- electronic information and information infrastructures of the Government of Lithuania as being of importance to the Government of Canada

Ministerial authorizations

Under the *CSE Act*, certain activities require ministerial authorization from the Minister of National Defence. There are different authorizations for the different aspects of CSE's mandate. Authorizations are valid for one year, and the following are subject to independent approval by the Intelligence Commissioner[46] before any activities can begin.

This year, CSE submitted **nine** authorizations to the Intelligence Commissioner, all of which were approved. These included:

- **1** cyber security authorization to help protect federal institutions
- **5** cyber security authorizations to help protect non-federal institutions
- **3** foreign intelligence authorizations

Additionally, authorizations for foreign cyber operations remained consistent with last year. These authorizations are also valid for one year and are issued for specific objectives which may also support multiple operations.

- **3** active cyber operations
- **1** defensive cyber operation

Disclosures of Canadian identifying information

CSE does not conduct activities that target Canadians at home or around the world, or individuals located in Canada. However, while conducting foreign intelligence activities, we may incidentally acquire information related to Canadians. When this happens, any Canadian identifying information (CII) is removed or masked before intelligence is shared.

In limited circumstances, government departments and agencies designated by the Minister of National Defence may request access to this information. Each request is carefully reviewed in line with the *CSE Act* before any disclosure is made.

Disclosures of Canadian Identifying Information in 2025	
Received (domestic)	1,032
Received (international)	75
Disclosed	930
Denied/cancelled	177

Internal compliance

CSE's compliance team monitors activities across the organization to ensure they align with internal policies and legal requirements. Findings and assessments are made available to external review bodies.

In 2025–2026, CSE's compliance team identified:

- **14** operational compliance incidents that did not involve information related to Canadians
- **186** operational compliance incidents that involved information related to Canadians

All incidents are reviewed and assessed. The compliance team identifies appropriate corrective actions and trends to strengthen practices and inform training and outreach.

This year, CSE also established a dedicated compliance education team to promote consistent practices across the organization.

External reviews

As part of Canada's national security and intelligence community, CSE is subject to external review by the National Security and Intelligence Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP).

These external review bodies verify, on behalf of Canadians, that CSE's activities comply with the law. Their work is an important part of maintaining transparency, accountability and public trust. We welcome independent review and insights to improve our processes.

This year, CSE supported **26 external reviews**, many of which were broader and more complex than in previous years. For example, CSE participated in NSIRA's pilot of a Technical Assurance Review (TAR), which applied new methods to examine CSE technical information and systems over a short, focused period.

CSE continued to provide quality and timely responses to all requests from review bodies and, once again, met all agreed upon timelines. We also continued to publish our management responses to external reviews[47] and report on progress in implementing agreed-upon recommendations. This year, we published responses to recommendations from two NSIRA review reports.

External review statistics in 2025–2026	
Reviews and reports contributed to	26
Briefings to review bodies	24
Questions answered	454

External complaints

This year, CSE received seven external complaints directed to the Chief. There were no complaints regarding CSE activities directed to NSIRA. We remain committed to continuous improvement and maintain a structured process to track complaints and report on the implementation of any related recommendations.

Audit and evaluation

CSE's Audit and Evaluation teams provide impartial, evidence-based advice and services to senior leadership. Their work supports sound decision-making and helps ensure we achieve our strategic objectives. Both teams receive quality assurance support from the CSE Professional Practices and Accountability Office.

This year, the teams completed:

- **3** assurance audits
- **1** advisory audit
- **3** performance evaluations
- **1** comparative analysis

They also:

- supported internal audit working groups
- provided guest audit support to an external federal partner
- helped develop a performance measurement framework for an internal program

This year, Canada's Auditor General conducted an audit to evaluate the cyber security of federal networks, including the role of CSE. The audit concluded that the government has tools in place to protect and defend systems, and that its overall cyber security plan is sound.

Cyber security audit program

Since 2018, CSE has offered a collection of free tools[48] to help auditors assess cyber security practices in their organizations. To date, we have received over 250 requests for these tools from across the Government of Canada and the private sector.

Access to Information and Privacy (ATIPs)

CSE is committed to transparency and disclosure while protecting our most sensitive information.

This year, CSE's Access to Information team processed:

- **85** ATIP requests
- **129** ATIP consultations
- **78** requests for information under the *Privacy Act*

To meet our legislative obligations under both the *Privacy Act* and the *Access to Information Act*, we continue to work with national security and intelligence partners to improve consultation processes and respond more quickly to requests for historical records. This work is ongoing, and we are focused on improving transparency while protecting sensitive information entrusted to us to protect Canada's national security, defence, foreign relations, and interests.

Strengthening transparency through public engagement

Building trust also requires consistent, visible engagement with Canadians. In a complex security environment, proactive communication helps demystify our work, reinforce confidence in our mandate, and translate technical insights into practical advice that Canadians can act on. It also helps tell the story of CSE – an organization whose work is often unseen but essential to Canada's security.

Over the past year, CSE strengthened its presence in the public domain through more active media engagement, participation in national and international forums, and increased visibility of its leadership.

CSE responded to **169 media queries**, conducted **20 interviews**, and participated in **6 national news conferences**, providing timely, factual information on emerging threats and cyber security issues.

At the same time, we expanded direct engagement with partners, stakeholders and the public through speeches, panel discussions and participation at key events and public discussions.

Through these engagements, we reinforced Canada's priorities in cyber security, intelligence and emerging technologies, while helping shape future directions, strengthening partnerships and advancing collective action. These forums also supported two-way dialogue, allowing us to share insights, promote practical cyber defence measures, and better understand evolving risks across sectors.

This helps humanize our work, reinforce accountability, and demonstrate how CSE contributes to broader government priorities and international cooperation.

This outreach also plays an important role in inspiring the next generation. By engaging students, researchers and early-career professionals, we help spark interest in careers as foreign intelligence analysts and cyber defenders, strengthen Canada's talent pipeline, and build a more resilient future workforce.

Together, these efforts strengthen transparency, improve awareness of cyber threats, and reinforce confidence in CSE as a trusted, authoritative voice. They complement formal accountability mechanisms and contribute to a more informed, resilient and secure Canada.

Values and ethics

We continue to strengthen our culture of ethics and accountability.

This year, CSE introduced an annual conflict of interest affirmation process for all employees to support transparency and maintain high ethical standards.

The Ethics team delivered over a dozen in-person, scenario-based ethics training sessions, including an interactive session with CSE's executives. They also developed practical "what-if" guidance on topics such as conflict of interest, personal social media use, non-partisanship and the use of AI.

During Ethics Week in January 2026, we welcomed a guest speaker from a Five Eyes partner organization. The session highlighted the importance of ethics in the workplace and the value that strong ethical practices bring to both individuals and organizations. It also explored emerging challenges for modern intelligence professionals, including the ethical use of artificial intelligence.

WE ARE ONE CSE AND WE ALL DELIVER THE MISSION

Our people are at the heart of everything we do. Our diverse and inclusive workforce is our greatest strength. United by a shared purpose and a passion for the mission, CSE employees bring agility, specialized skills and expertise to our country's most complex challenges, empowered by innovation and a relentless problem-solving mindset.

As Canada strengthens its defence posture, including its commitment to NATO, building and sustaining a healthy, skilled, and resilient workforce is essential. Equity, diversity, inclusion and accessibility (EDIA) guide how we recruit, develop and promote talent, communicate our achievements and collaborate with our partners. By investing in our workforce, we ensure CSE remains ready to deliver on its mission, now and into the future.

Top employer recognition

CSE continues to be recognized as an employer of choice.

This year, we were once again named a **Top Employer in the National Capital Region** and, for the first time, **one of Canada's Best Diversity Employers**.

Growing and supporting our workforce

To meet growing demands in an increasingly complex threat environment, CSE continues to expand its workforce.

This year, CSE's workforce reached **4,178 employees**, an **8.1% increase** from last year. This growth reflects sustained efforts to attract and retain top talent. It also reflects increased demand driven by defence and security investments, enabling CSE to expand its operational capacity and deliver on its evolving mandate.

Our workforce also increasingly reflects the diversity of the country we serve. As of March 2026, employees span all four employment equity groups as well as 2SLGBTQIA+ and intersectional identities. Representation among Indigenous people and people with disabilities is particularly well-represented at CSE, exceeding workforce availability in Canada.

Our workforce in 2025 to 2026	
Workforce representation (by self-identification)	
↳ Women	33.9%
↳ Persons with disability	14.1%
↳ Racialized persons	17.9%
↳ Indigenous persons	2.6%
↳ 2SLGBTQIA+ persons	6.4%

As we grow, we are also strengthening the employee experience. We continue to prioritize wellness and wellbeing, creating the conditions for employees to thrive. Through our efforts, we are building the future of CSE and empowering our people to deliver trailblazing outcomes for Canada while fostering an inclusive and dynamic workplace culture that has garnered recognition year after year.

Candidate outreach

CSE continues to broaden its reach to attract diverse talent.

We use targeted hiring platforms such as Obsidi and Indigenous Link, along with outreach events focused on equity-seeking groups. Our goal is to attract **three out of every four hires** from these groups.

This year, we:

- participated in **139 recruitment events** across 8 provinces
- held **26 virtual information sessions**
- hired graduates from across Canada, primarily in computer engineering, computer science, mathematics, and business

In fall 2025, CSE continued its recruitment efforts by running an advertising campaign that encouraged individuals to apply for various positions within the organization. The campaign used multiple digital channels and reached Canadians working in STEM, with a focus on women and visible minorities. It generated:

- over **11 million ad impressions**
- more than **205,000 clicks**
- over **195,000 visits** to our careers page

Foreign language intelligence analyst campaign

We also ran specialized campaigns to recruit key talent to attract the best and the brightest Canada has to offer.

In winter 2026, a targeted ad campaign to recruit Chinese-language intelligence analysts used both traditional and culturally specific channels. It generated over **43,000 visits** to CSE's website, and we continue to seek people with language skills to support the breadth of our mission.

Security program updates

Protecting sensitive information is central to CSE's mission.

As we hold top-secret intelligence on our country's operations, we take extensive measures to safeguard it. Throughout the year, we regularly review and update our security processes and policies, while ensuring alignment with our values and priorities.

This year, we upgraded our Security Assurance Program to strengthen reliability screening and security clearances. New tools and measures improve how we manage risks for both current and departing employees. This ensures our workforce remains robust and adaptive to today's dynamic and evolving threat landscape.

We also:

- launched a foundational security training and awareness program for all new employees
- published new guidance on our external website, to help candidates understand security requirements when applying to CSE

Launch of the Wellness Info Hub

This year, CSE launched a centralized Wellness Info Hub, giving employees easier access to resources and personalized support. A new Wellness Navigator role and consultation forum further strengthen our approach to employee wellness.

Improvements to mental health support services for Black employees

We are committed to growing mental health resources at CSE. As part of our work, we continue to refine our mental health services to better meet employees' needs. This includes more culturally responsive options, such as the ability for Black employees to work with mental health professionals who reflect their communities.

Early-talent pipeline

Students and early-career professionals play an important role at CSE.

Each year, we hire over **235 students**, and approximately **two-thirds** transition into permanent roles. This year, we hired 91 students into full-time roles, and 16% of our workforce was under 30 years old.

This reflects our commitment to identifying and fostering early talent, ensuring sustainable growth and a strong, future-ready workforce.

Mission to Move

Led by Chief Caroline Xavier, Mission to Move encouraged employees to stay active amid busy days at the office and support their wellbeing.

Over several weeks, employees embraced the challenge and took part in activities that promoted both physical and mental health, demonstrating a strong culture of connection, resilience, and balance.

Fostering inclusion, belonging and accessibility

Creating an inclusive workplace is essential to delivering our mission and meeting the operational demands of tomorrow.

At CSE, we are committed to creating a workplace where every employee can contribute fully and be at their best. Guided by our One CSE framework[49], we continue to embed EDIA into everything that we do, not as an aspiration but as a core part of how we operate.

Launch of CSE's 2026 to 2028 Accessibility Plan

This year, we launched an updated Accessibility Plan for 2026 to 2028[50] to further reduce barriers in our workplace. With innovation and adoption as core components of our mandate, we regularly revisit our accessibility provisions for employees. This year, we met with the Government of Canada's Chief Accessibility Officer to discuss accessibility and empowerment from a CSE lens. Through these important touchpoints, we continue to explore and put in place how technology can support accessibility, showing that even high-security environments can be inclusive and adaptable.

Did you know?

14.1% of CSE employees identify as **Persons with disabilities**.

A barrier-free environment in a high-security organization

CSE is committed to making its workplace accessible to all employees, including those with disabilities and neurodivergent employees. In this pursuit, we are driven to take innovative approaches to accessibility, even within high-security environments.

An AI-powered captioning tool to support accessibility and workplace accommodation

With a view toward enhanced accessibility, a pilot is being explored for an offline mobile AI-powered captioning tool. This solution will benefit employees with hearing impairment or neurodivergences by improving comprehension, reducing cognitive load, and sustaining focus. By taking a proactive approach, CSE demonstrates that high-security environments and inclusive workplaces are not mutually exclusive.

Secure mobile medical devices

This year, we expanded workplace accommodations for employees with medical needs, including a pilot that introduced medical technologies in the workplace to support employees who rely on digital health monitoring tools. These tools help employees manage their health safely and discreetly during the workday.

We also continued to review worn medical devices regularly, assessing current technologies and evaluating new ones as

they emerge. This helps ensure our accessibility approach keeps pace with evolving medical technologies and reduces barriers before they affect employees.

These efforts demonstrate that accessibility is not a constraint, it strengthens performance, inclusion, and innovation. They also reflect our commitment to building an accessible workplace where employees can fully contribute and thrive. This helps us attract and retain the top talent we need to deliver our mission.

Citizenship ceremony

In January 2026, CSE, in partnership with Immigration, Refugees and Citizenship Canada (IRCC), had the privilege of proudly hosting its third citizenship ceremony at our Vanier facility, welcoming 60 new Canadians from 26 countries. This event reflects our ongoing commitment to inclusion and community.

One CSE: The Collection – Season 2

Building off the momentum created through Season 1 of "One CSE: The Collection," Season 2 was launched in January 2026. This follow-up is designed with the One CSE Framework[51] in mind, and serves as an extension of CSE's driving principles: cultural growth, continuous learning, consultation and transparency, freedom from barriers and discrimination, and a deep commitment to inclusion.

Season 2 builds on the success of Season 1, which was awarded the Lighthouse Award of Communications Excellence for its model of employee engagement among similar initiatives across the Government of Canada.

Gender-based Analysis Plus

Gender-based Analysis Plus (GBA Plus) continues to strengthen how we make decisions by considering diverse perspectives and lived experiences.

GBA Plus directly supports **One CSE** through identifying and addressing systemic biases and barriers, further shaping our organizational culture and enabling more equitable outcomes for all.

We continue to integrate GBA Plus by:

- embedding it into our processes, including Memoranda to Cabinet, Treasury Board submissions, and Budget proposals, to enable data-driven decision-making, deliver inclusive and responsive initiatives and enable mission success
- applying a "whole person" approach in the development of policies, processes, services and initiatives, ensuring they are inclusive, accessible and respond to the diversity of the CSE community
- integrating GBA Plus into our foundational documents, including our Ethics Charter, Code of Conduct and Duty to Accommodate
- equipping and empowering our employees to apply an intersectional lens to their work by:
    - building foundational knowledge through mandatory GBA Plus, cultural bias and unconscious bias training
    - allocating dedicated advice, guidance and feedback resources to support the development of responsive initiatives
    - providing resources and on-the-job learning tools for employees and teams to build analytical confidence and capacity

We also collaborate across the Government of Canada by:

- regularly participating in interdepartmental engagements
- co-chairing the Cyber Identity/Inclusion, Diversity, Equity, and Accessibility Working Group with Public Safety Canada, to share lessons learned, best practices, resources and identify areas for collaboration

As a past recipient of the Lighthouse Award of Communications Excellence, CSE has been recognized as a leader in the GBA Plus and EDIA space across the Government of Canada, for thoughtfully supporting interactions between employees while building a lasting awareness of EDIA principles.

Women in Defence and Security Awards Breakfast 2026

In March 2026, eight CSE employees received the Remarkable Leader award at the Women in Defence and Security Awards Breakfast[52]. They were recognized alongside recipients from the extended security and defence community.

CSE Chief, Caroline Xavier, delivered a heartfelt keynote on the theme of an ignited community and influencing change for the greater good.

Affinity groups

Affinity groups are employee-led networks where members can build community, share perspectives, and address barriers they may encounter in the workplace. They play an important role in strengthening the organization by offering insights that help inform policies, programs, and initiatives that advance workplace priorities and improve the overall employee experience.

In addition, affinity groups are invited to decision-making tables and share annual updates with CSE executives on progress, challenges, and emerging needs.

There are 14 affinity groups at CSE, including:

- Pride Network
- Women in Cyber Intelligence (WICI)
- Access Women's Support Network
- EmbRACE, including:
  - Black Employee Circle
  - Middle East and North African
  - Asian Heritage
  - South Asian Affinity Group
- Neurodiversity Group
- Persons with Disabilities Affinity Group
- Jewish Affinity Group
- Muslim Affinity Group
- Réseau Francophone
- Code Talkers Circle (for employees identifying with the Indigenous community)
- Audible Minorities

Five Eyes Indigenous Summit

CSE hosted the Five Eyes Indigenous Summit from June 24 to 26, 2025, in close collaboration with CSIS who chaired the event, and in collaboration with the Code Talkers Circle. CSE and CSIS coordinated the summit at our Vanier facility to bring partners together and discuss partnerships with Indigenous communities, particularly around the subject of security. The summit also included a traditional Indigenous teaching, offering a meaningful cultural perspective that grounded discussions in Indigenous knowledge.

CSE's Young Professionals Network (YPN)

The YPN was founded in 2012 as a dynamic network for young and new employees. Members consistently foster a cohesive working environment and promote positive change for a sustainable workforce at CSE. The target audience typically includes co-op students and employees with less than 10 years of service in the public service, with no prescribed age limit. Whether an employee is new to their career, a new CSE recruit, or young at heart, all are welcome to join the network!

This year, the YPN hosted 14 events across the organization that ranged from training and professional networking to social mixers and interdepartmental events. Executives and newer employees alike mingled with the broader Government of Canada community and explored topics like professional development, cross-sectional representation, sustainability, and general wellness.

Recognizing CSE's workplace culture for young professionals

In October 2025, the YPN Steering Committee was awarded the Cabot Trail Award at the National Capital Region-wide Young Professional Network's annual Champions Appreciation Event. CSE's YPN was recognized for being "consistently active, engaged, and pushing the envelope" within the Government of Canada community.

Empowering our workforce to embrace digital transformation

In line with our commitment to continuous innovation, CSE empowers its workforce to embrace new and emerging technologies, allowing us to be at the forefront of responsible digital transformation. Under the framework of an AI-enabled organization, our employees leverage new technologies to carry out their work guided by the CSE AI Strategy[53].

Adopting artificial intelligence responsibly

CSE made considerable progress in embedding artificial intelligence into its operations this year, expanding the adoption of AI-enabled technologies across the organization. Guided by the principles set out in the CSE AI Strategy and supported by robust governance and risk-management frameworks, we are ensuring that our workforce has access to cutting-edge tools within a secure and governed environment.

As part of this effort, CSE continued to evaluate and integrate commercially available AI tools, including generative AI capabilities, into day-to-day workflows. Security considerations were assessed at every stage to maintain the integrity of our information environment, with controls embedded from the outset. Ongoing user education and engagement helped ensure safe and effective adoption, with employees guided by a core principle: always verify AI-generated processes and results.

Early results have been positive, with users reporting measurable improvements to productivity and workflow efficiency. These insights are informing future decisions on enterprise-wide AI adoption, ensuring that CSE continues to empower its workforce while safeguarding sensitive information and maintaining public trust.

Building a governance framework for responsible AI

This year, CSE formally launched a Responsible AI Toolkit, to help employees make safe and secure decisions around AI adoption at work. Inspired by best practices shared among international allies, the Toolkit includes an AI risk-management process and an AI use case registry. By routinely documenting, assessing, and mitigating risks across the organization, CSE is exercising due diligence while integrating AI constructively.

CSE also launched a foundational AI learning program for employees, helping to standardize AI literacy across the workforce. By making use of secure technology, our employees are well-placed to advance CSE's work in the domain.

Endnotes

1 https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng

2 https://www.cyber.gc.ca/en/guidance/ransomware-threat-outlook-2025-2027

3 https://www.cyber.gc.ca/en/news-events/joint-guidance-malicious-cyber-threats-sd-wan-networks

4 https://www.cyber.gc.ca/en/alerts-advisories/al25-016-internet-accessible-industrial-control-systems-ics-abused-hacktivists

5 https://www.canada.ca/en/communications-security/news/2025/11/joint-statement-on-malicious-cyber-activity-targeting-canadian-critical-infrastructure.html

6 https://www.cyber.gc.ca/en/news-events/joint-cyber-security-advisory-worldwide-network-compromises-peoples-republic-china-state-sponsored-actors

7 https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign

8 https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity

9 https://www.cyber.gc.ca/en/guidance/cyber-threat-marine-transportation

10 https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-water-systems-assessment-mitigation

11 https://www.cyber.gc.ca/en/guidance/ransomware-threat-outlook-2025-2027

12 https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign

13 https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-canada-israel-iran-conflict

14 https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-water-systems-assessment-mitigation

15 https://www.cyber.gc.ca/en/guidance/cyber-threat-marine-transportation

16 https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026

17 https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-peoples-republic-china-sponsored-cyber-activity-against-canadian-provincial-territorial-indigenous-and-municipal-governments

18 https://www.cyber.gc.ca/en/guidance/ransomware-threat-outlook-2025-2027

19 https://www.cyber.gc.ca/en/guidance/top-10-artificial-intelligence-security-actions-primer-itsap10049

20 https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089

21 https://www.cyber.gc.ca/en/guidance/defending-against-adversary-middle-threats-phishing-resistant-multi-factor-authentication-itsm30031

22 https://www.cyber.gc.ca/en/news-events/threat-detection-sharepoint-vulnerabilities

23 https://www.cyber.gc.ca/en/news-events/threat-detection-sharepoint-vulnerabilities

24 https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

25 https://www.canada.ca/en/department-national-defence/corporate/reports-publications/industrial-strategy/security-sovereignty-prosperity.html

26 https://www.canada.ca/en/department-national-defence/corporate/reports-publications/industrial-strategy/security-sovereignty-prosperity.html

27 https://www.cse-cst.gc.ca/en/mission/research-cse/communications-security-establishment-canada-artificial-intelligence-strategy

28 https://www.cse-cst.gc.ca/en/mission/research-cse/vulnerability-research-centre

29 https://www.canada.ca/en/communications-security/news/2025/07/cse-and-nserc-to-fund-research-on-exploratory-analysis-of-unstructured-data.html

30 https://www.cse-cst.gc.ca/en/cse-nserc-research-communities-grants

31 https://www.cyber.gc.ca/en/education-community/academic-outreach-engagement/post-secondary-cyber-security-related-programs-guide

32 https://www.youtube.com/watch?v=Q5V0yap77yg

33 https://www.canada.ca/en/campaign/online-disinformation.html

34 https://cybersecuritychallenge.ca/en

35 https://www.getcybersafe.gc.ca/en/resources/spot-romantic-red-flags-online-dating

36 https://www.getcybersafe.gc.ca/en/blogs/phishing-scams-youre-more-likely-encounter-when-travelling

37 https://www.getcybersafe.gc.ca/en/blogs/social-media-habits-could-hurt-you-and-strengthen-your-cyber-security

38 https://www.getcybersafe.gc.ca/en/blogs/talk-your-loved-ones-about-cyber-security

39 https://www.getcybersafe.gc.ca/en/resources/backups

40 https://www.getcybersafe.gc.ca/en/resources/password-managers

41 https://www.getcybersafe.gc.ca/en/resources/hackable-are-you

42 https://www.getcybersafe.gc.ca/en

43 https://www.getcybersafe.gc.ca/en/resources/video-letter-future-you-cyber-month-2025-jingle

44 https://www.getcybersafe.gc.ca/en/blogs/free-online-cyber-security-workshop-series-older-adults-during-cyber-month

45 https://www.ctvnews.ca/video/deception-decoded/2026/02/25/canadas-critical-infrastructure-is-being-targeted-in-cyber-attacks-deception-decoded

46 https://www.canada.ca/en/intelligence-commissioner.html

47 https://www.cse-cst.gc.ca/en/accountability/transparency/responses-reports-reviews

48 https://www.cyber.gc.ca/en/tools-services/cyber-security-audit-program

49 https://www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion

50 https://www.cse-cst.gc.ca/en/accessibility/communications-security-establishment-canada-accessibility-plan-2026-2028

51 https://www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion

52 https://www.wids.ca/events/details&e=97

53 https://www.cse-cst.gc.ca/en/mission/research-cse/communications-security-establishment-canada-artificial-intelligence-strategy


Canada