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

Communications Security
Establishment Canada

Annual Report 2024–2025

Communications Security
Establishment Canada

Centre de la sécurité des
télécommunications Canada

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

Minister's foreword 2

Message from the Chief 3

Who we are and what we do 5

Our mandate 7

2024 to 2025 by the numbers 9

CSE is identifying, mitigating and responding to foreign threats 13

How aspects of the CSE mandate work together: an example 15

Collecting, analyzing and disseminating foreign signals intelligence 16

Conducting foreign cyber operations 20

Publishing cyber threat assessments 21

Protecting Canada's democratic institutions and critical infrastructure 24

Responding to and preventing cyber incidents 28

Providing support and expertise to global events 29

CSE is innovating and evolving 31

Promoting the responsible use of artificial intelligence 32

Improving classified infrastructure and services 33

Fostering innovation and partnerships through open sourcing 34

Conducting research and strengthening research partnerships 34

CSE is empowering and reaching Canadians 37

Finding new ways to educate Canadians 38

Expanding outreach activities 40

CSE is growing and learning 43

Improving our hiring, recruitment and outreach activities 44

Prioritizing inclusivity in everything we do 45

CSE is transparent and accountable 49

Maintaining our commitment to transparency and accountability 50

Supporting the Public Inquiry on Foreign Interference 52

Endnotes 53

Minister's foreword

Events of this past year, both within Canada and internationally, have reinforced the vital role of the Communications Security Establishment Canada (CSE) in safeguarding our national and economic security. As the threat landscape rapidly evolves, CSE plays a critical role in helping Canada navigate complex and emerging challenges. The expertise and dedication of the CSE team are world class, and their work is integral to Canada's national security. I extend my sincere gratitude to everyone at CSE for their unwavering commitment.

As foreign actors continue to deploy disinformation campaigns aimed at undermining trust in democratic institutions, Canada requires reliable, timely information on the activities, capabilities and tactics of these actors. CSE delivers precisely that—providing clear insights into the global threat environment and illuminating where and how adversaries seek to destabilize our society.

Cyber security incidents have become increasingly disruptive, affecting critical infrastructure and organizations across Canada. Through its Cyber Centre, CSE plays an essential role in defending federal, provincial, territorial, Indigenous and municipal institutions. The Cyber Centre also educates stakeholders, raises awareness, and builds capacity through expert advice, guidance and technical support. These efforts are critical to strengthening Canada's resilience against a growing spectrum of cyber threats.

The government's investment in CSE underscores the organization's crucial mandate and its significant impact on our national security landscape. CSE has a strong history of delivering on what matters most: protecting Canadians and safeguarding Canada. As cyber threats evolve and the defence of our nation grows ever more complex, the government is committed to equipping CSE with the tools and resources necessary to defend our sovereignty and advance Canada's intelligence priorities.

The tireless work of CSE's dedicated public servants makes all this possible. Their efforts are fundamental to ensuring the safety and security of Canadians today and into the future.

The Honourable David J. McGuinty
Minister of National Defence

Message from the Chief

It has been another momentous year for CSE. I am pleased to share this report to show Canadians some of the ways that our outstanding organization has been working to keep them safe. At CSE, we are driven by excellence. Our passion for working together and with our diversity of partners to solve complex problems sharpens our innovative edge.

This year's annual report highlights our commitment to Canada's security in action—from our ongoing work to produce actionable intelligence for federal decision-makers to our dedication to strong and varied partnerships to develop creative solutions that bolster Canada's cyber resilience. What we do, and the impacts we have on Canada's safety, prosperity and security, are very tangible, if not always publicly visible. Our work is shaping the decisions that protect Canada's citizens, defend our values, and reinforce Canada's role as a trusted partner on the world stage.

This year, we laid a solid foundation for the future. We did this by continuing to work closely with our Five Eyes partners and with our various partners in government and industry, both domestically and internationally. Together, we issued joint guidance on cyber threats, collaborated on challenges related to artificial intelligence (AI) and worked to protect the security of Canada's democratic institutions. CSE is more ready than ever to take on whatever comes next.

Diversity is CSE's mission strength. It's something we prioritize not only in recruitment, but also in how we shape our policies. Our continued growth shows that we are on the right track. We are stronger because of our diverse workforce, because we have built a culture where people are able to bring their best selves to work, where they feel supported and seen in the workplace. Equity, diversity, inclusion and accessibility inform everything we do and are essential to helping us deliver our mission.

National security and cyber security are team sports, and CSE is proud of the relationships we have built with other government departments, all levels of government and stakeholders and allies across the globe. At a time when the world faces an increasingly complex threat landscape—cyber threats, economic security threats, violent extremism, foreign interference, disinformation campaigns and more—I feel reassured knowing that our talented and skilled CSE team is working around the clock to help Canada confront these challenges head-on.

CSE doesn't operate in this arena alone. We work alongside independent oversight and external review bodies that ensure accountability for our work on behalf of Canadians and bolster our efforts toward transparency and trust.

This was a big year for CSE. We countered cyber threats from increasingly sophisticated adversaries, supported major events, published our AI strategy, and participated in the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, to name a few examples. And I know next year will be even bigger. Throughout our almost 80 years as an agency, CSE has witnessed and successfully navigated tremendous change. We are currently in the process of developing our Vision 2030, a whole-of-CSE effort that will drive our future plans, priorities and activities. Whatever challenges the next year may bring, we are preparing, and we are ready. We are One CSE.

Caroline Xavier (she/her)
Chief, CSE

WHO WE ARE AND WHAT WE DO

WE ARE INTELLIGENCE
WE ARE CYBER
WE ARE TRUSTED PARTNERS AND ADVISORS
WE ARE READY
WE ARE CSE
CSE | CST
Canada
NOUS SOMMES LE RENSEIGNEMENT
NOUS SOMMES LA CYBERSÉCURITÉ
NOUS SOMMES DES PARTENAIRES ET DES CONSEILLERS DIGNES DE CONFIANCE
NOUS SOMMES PRÊTS
NOUS SOMMES LE CST

The Communications Security Establishment Canada (CSE) is Canada's cryptologic agency, responsible for foreign signals intelligence, cyber security and foreign cyber operations. It is a standalone agency reporting to the Minister of National Defence.

CSE includes the Canadian Centre for Cyber Security (Cyber Centre), which is Canada's operational and technical lead for cyber security and information assurance. As part of CSE, it provides leading-edge advice and services to help prevent cyber incidents and keep critical services up and running.

CSE has a workforce of 3,841 full-time, permanent employees. CSE's total authorities for 2024 to 2025 were in excess of $1 billion. This report is an unclassified summary of CSE's activities from April 1, 2024, to March 31, 2025. Unless otherwise stated, "this year" refers to the 2024 to 2025 fiscal year.

Five Eyes

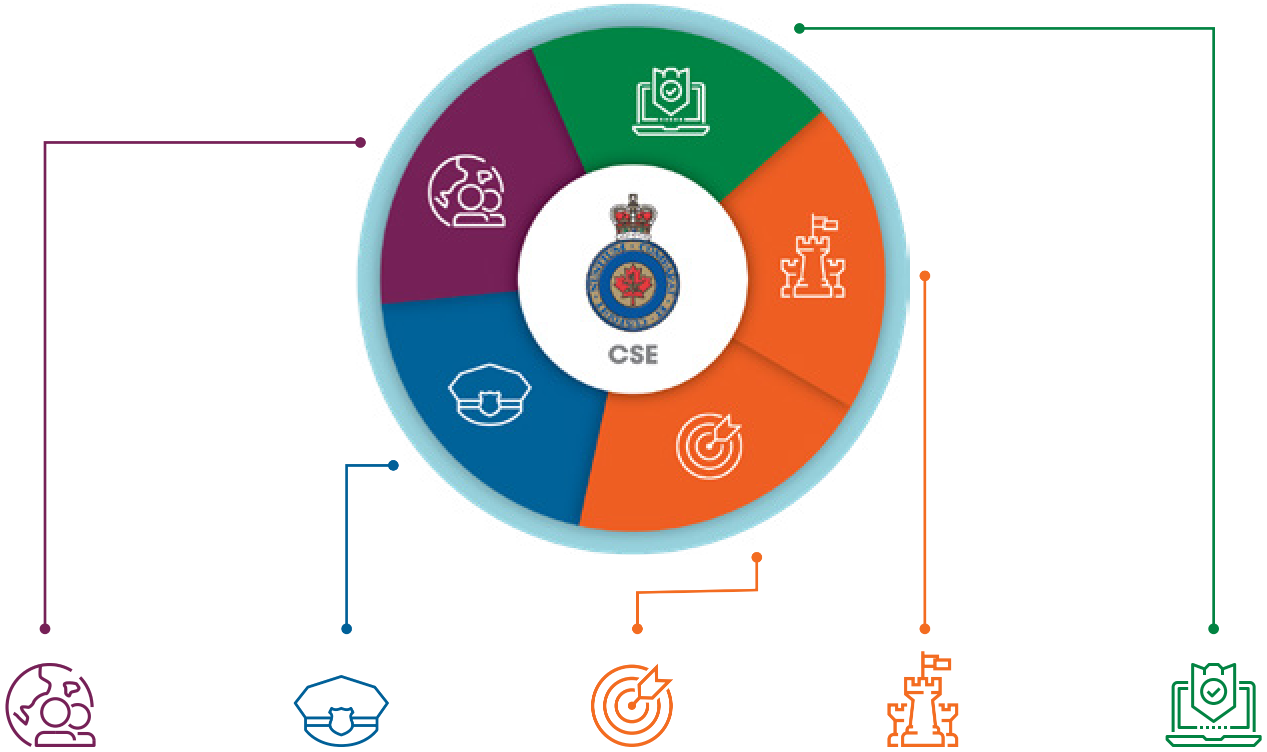
CSE is a proud member of the Five Eyes, the world's longest-standing and closest intelligence-sharing alliance. The Five Eyes include the signals intelligence and cyber security agencies of Canada, Australia, New Zealand, the United Kingdom (UK) and the United States (US).

Our mandate

CSE's mandate is detailed in the *Communications Security Establishment Act (CSE Act)*[1] and has 5 parts:

- foreign signals intelligence
- technical and operational assistance to federal partners
- active cyber operations
- defensive cyber operations
- cyber security and information assurance

This report showcases how our work this year made Canadians safer.



FOREIGN SIGNALS INTELLIGENCE

CSE's ability to collect foreign signals intelligence through the use of advanced techniques.

Acquire information from or through the Global Information Infrastructure located outside Canada, including by engaging or interacting with foreign entities located outside Canada.

TECHNICAL AND OPERATIONAL ASSISTANCE

Assist federal law enforcement and security agencies, the Canadian Armed Forces and the Department of National Defence.

Use advanced techniques to support partners' activities, including cyber operations for government-authorized missions.

ACTIVE CYBER OPERATIONS

Interfere with foreign online efforts that threaten Canada.

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.

DEFENSIVE CYBER OPERATIONS

Disrupt foreign cyber threats targeting important Canadian networks by taking online action.

Defend systems of importance to the Government of Canada.

CYBER SECURITY AND INFORMATION ASSURANCE

Defend important Canadian networks.

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.

2024-2025 BY THE NUMBERS

It was a productive year at CSE! Here are some key numbers that provide a snapshot of what we accomplished:

Our workforce in 2024 to 2025	
Total workforce	3,841
Attrition rate	3%* (1.3% voluntary)
Workforce increase compared with last year	6%
Workforce representation (by self-identification)	
↳ Women	33%
↳ Persons with disability	15%
↳ Racialized persons	19%
↳ Indigenous persons	3%
↳ 2SLGBTQIA+ persons	7%
Top Employer awards	2 awards (Top Employer for Young People and Top Employer in the National Capital Region)

Alerts and notifications issued to protect against malicious actions in 2024 to 2025	
Cyber Centre general inquiries received	13,500
Cyber security incidents responded to	Government of Canada: 1,155 Critical infrastructure: 1,406
Pre-ransomware notifications	336 notifications sent to 309 Canadian organizations
Ransomware incidents potentially averted through pre-ransomware notifications	Between 74 and 148, resulting in an estimated economic savings of $6 to $18 million
Supply chain risk assessments	1,371
Vulnerabilities disclosed to vendors	10

Foreign signals intelligence in 2024 to 2025	
Reports	3,385
Client departments	32
Individual clients	3,016
Requests for assistance	51

Reports, publications and guidance released in 2024 to 2025	
Cyber security guidance publications	29
Joint endorsement publications	20
Unclassified threat assessments	7
Intelligence reports on Arctic security	196

Engagement with other government departments and critical infrastructure industries in 2024 to 2025	
One-on-one briefings delivered	30
Group sessions conducted with IT and cyber security teams and senior executives	12
Government of Canada organizations engaged with to enhance their cyber resilience	150
Speaking engagements	200+
Briefings on preparing for the quantum computing threat to cryptography	30+
Tabletop exercises	13
Biweekly threat briefings for IT security professionals	38
“Walk-the-talk” sessions	7

Media and public engagement in 2024 to 2025	
Media queries	209
Interviews	19
National news conferences	3
Parliamentary appearances	15
Order Paper Question (OPQ) responses	142
Enrollments in Learning Hub courses	11,895

* This figure excludes term employment and retirements

Accountability, transparency and compliance in 2024 to 2025

Ministerial authorizations	12
Ministerial orders in effect	5
Ministerial directives	1
External reviews	
↳ Reviews and reports contributed to	25
↳ Briefings to review bodies	29
↳ Questions answered	412
Disclosures of Canadian identifying information	
↳ Received (Government of Canada)	669
↳ Received (Five Eyes)	83
↳ Approved	559
↳ Denied	95
↳ Pending	10
↳ Cancelled	88
Operational compliance incidents	
↳ Involving information related to Canadians	119
↳ Not involving information related to Canadians	22
External complaints	
↳ Sent to the Chief, CSE	3
↳ Sent to NSIRA	1
Open Government portal uploads	
↳ Datasets	5
↳ Information assets	47
Access to Information Act requests	61
Proactive disclosures	5 committee binders
Tabled documents	3
Internal audits	2
Internal program evaluations	3
Documents produced in support of the Public Inquiry into Foreign Interference	85,000+

CSE IS IDENTIFYING, MITIGATING AND RESPONDING TO FOREIGN THREATS

Canada is facing a dynamic and complex threat landscape. CSE is committed to defending Canada from hostile foreign threats while also advancing the country's strategic, economic, security, trade, defence and foreign policy interests. Working closely with domestic and international partners, we leverage our mandate to identify threats, defend against them and take action to disrupt the activities of malicious foreign actors. Our specialized teams are working around the clock to:

- collect foreign signals intelligence (SIGINT)
- inform the Government of Canada at the highest levels on economic security, diplomatic affairs, violent extremism, foreign interference, cyber threats, Arctic sovereignty, support to military operations, and more
- write and publish unclassified reports and guidance on cyber threats
- educate stakeholders at all levels of government and in critical infrastructure sectors—through briefings, courses, meetings and other outreach activities—about how they can protect themselves against cyber threats
- support security and law enforcement partners by providing them with relevant intelligence
- respond to cyber incidents, including by notifying potential victims of ransomware incidents
- conduct defensive and active cyber operations to respond to and counter threats
- collaborate with Five Eyes and other international partners to develop a complete understanding of the diverse threat landscape and to build strong networks and relationships to face these threats

As the threat landscape shifts and evolves, so does CSE. We adapt to stay ahead of the tradecraft of sophisticated nation state and criminal threat actors. In a tense and uncertain geopolitical climate, we provide Canada and our allies with a strategic advantage. We are constantly at the forefront of technological advances in the security and intelligence community to deliver on our mandate and fulfill our mission priorities.

Diversity at CSE

A diverse workforce is crucial to achieving our mission at CSE. Employees from various backgrounds bring a wealth of perspectives and expertise that are essential for accurate and comprehensive intelligence gathering. For instance, having native speakers who possess a deep understanding of the nuances of a foreign language and its associated culture ensures that information is interpreted correctly and contextually. This cultural insight helps in avoiding misinterpretations that could lead to flawed intelligence assessments.

A diverse team also brings varied problem-solving approaches and innovative ideas, enhancing our ability to address complex global challenges. Diversity at CSE enriches our ability to provide the Government of Canada with the right information to support strategic decision-making.

How aspects of the CSE mandate work together: an example

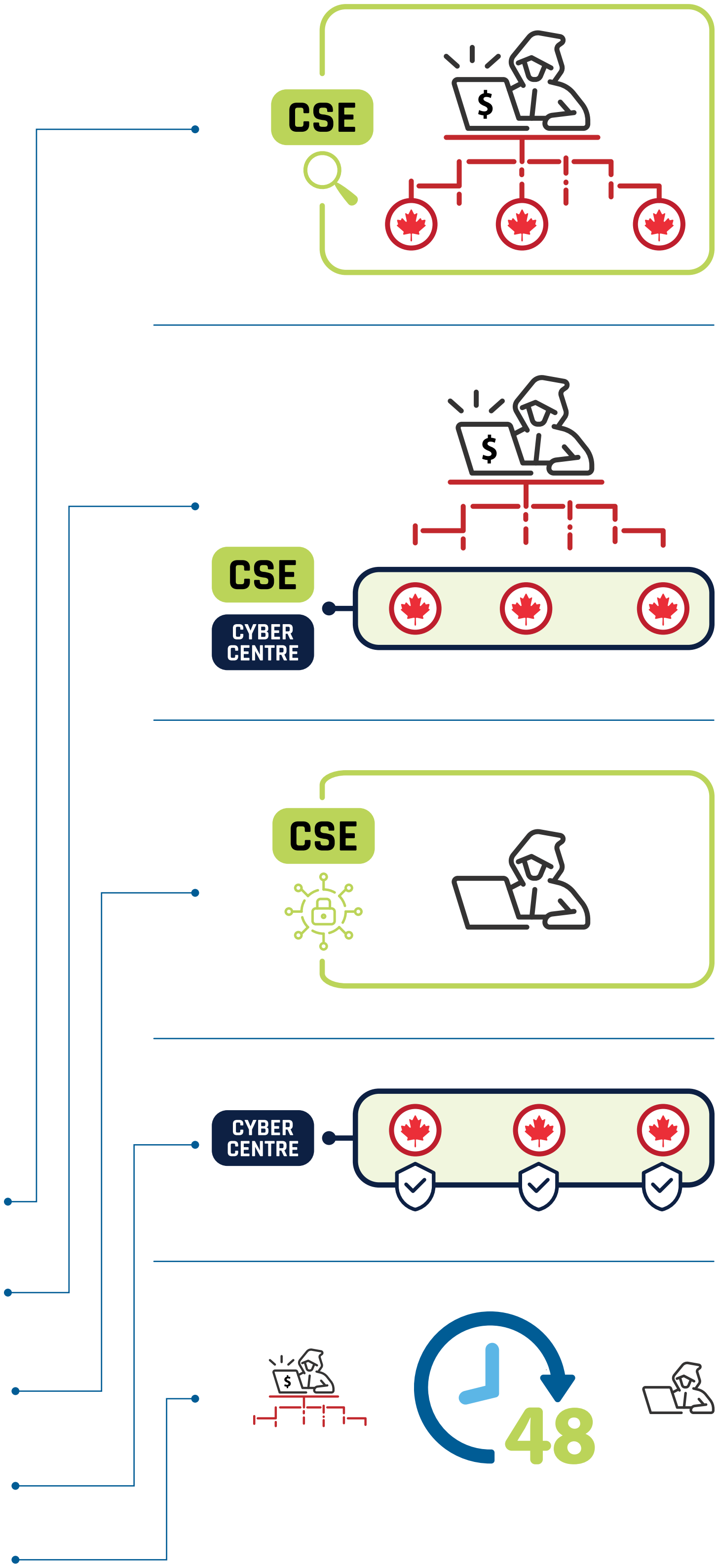
The *CSE Act* authorizes CSE to carry out 2 different types of foreign cyber operations: active and defensive. Both types of operations involve taking action in cyberspace to disrupt foreign-based threats to Canada.

Defensive cyber operations can be used to help protect systems of importance and federal institutions during major cyber incidents when cyber security measures alone are not enough.

Active cyber operations can be used proactively to disrupt foreign-based threats to Canada's international affairs, defence or security interests.

Here is an example of how our foreign intelligence, cyber security and cyber operations teams worked together this year to disrupt a threat to Canadians:

- In late 2024, CSE collected foreign signals intelligence about a ransomware group that was targeting Canadian victims in an industrial sector important to Canada's critical infrastructure
- CSE's foreign cyber operations team and the Cyber Centre worked together to identify the victims and disrupt the threat
- CSE's foreign cyber operations team conducted an operation to technically disrupt the threat actor's activities, neutralizing the threat
- At the same time, the Cyber Centre notified the victims and provided cyber security advice
- The threat was detected and disrupted within 48 hours



Collecting, analyzing and disseminating foreign signals intelligence

CSE collects, analyzes and disseminates foreign signals intelligence (SIGINT) to provide the Government of Canada with information about foreign-based threats in support of national interests. SIGINT is the interception, decoding and analysis of communications and other electronic signals. It can include any kind of electronic communication.

SIGINT also supports government decision-making and policy-making in defence, security, safety and international affairs by providing important insights into global events. CSE develops a broad range of sophisticated classified capabilities to acquire foreign intelligence from outside of Canada to respond to our adversaries' evolving technologies and capabilities.

Per the *CSE Act*, CSE's foreign intelligence collection activities are not directed at Canadians or anyone in Canada. Our foreign SIGINT activities are strictly guided by the Government of Canada Intelligence Priorities.

Canada's Intelligence Priorities

As one of Canada's core intelligence organizations, CSE supports Canada's Intelligence Priorities[2], which direct the Canadian intelligence community. We direct our work to ensure we are focusing on the most pressing and significant threats, as identified by the Government of Canada.
As an intelligence producer, CSE's efforts to deliver intelligence that meets Canada's Intelligence Priorities directly support national interests.

Arctic sovereignty

CSE works hard alongside domestic and international partners to support Canada's security and sovereignty in the Arctic—a priority for the Government of Canada. Canada's new Arctic Foreign Policy cites CSE as a key partner in bridging the intelligence gap to address the complex range of threats facing the Arctic, and we continue to invest to meet the growing demand for intelligence from a variety of Arctic stakeholders. We work closely with domestic partners and international allies to provide foreign intelligence and advance partnerships in areas such as cyber defence, economic security and countering foreign interference.

This year, we shared 196 intelligence reports on Arctic security with 20 Government of Canada departments and with Canada's international allies. These reports included information on foreign states' political intentions, military capabilities, technological advancements, economic interests and research activities in the region. CSE also actively pursues intelligence on foreign cyber actors seeking to exploit and compromise systems related to the Arctic.

Partnerships in the Arctic

This year, we took several steps to deepen our ongoing Arctic partnerships, including:

- participating in an annual Arctic security conference hosted in Yellowknife, Northwest Territories, with other federal organizations and territorial governments
- continuing to co-chair, alongside the Privy Council Office (PCO), the Arctic Intelligence Coordination Group, which coordinates Arctic security activities across the Government of Canada
- continuing to provide leadership at international forums dealing with polar issues
- hosting an in-person conference in Ottawa for an international forum on signals intelligence concerning both polar regions
    - CSE founded and continues to provide leadership to this forum
- participating in an all-source intelligence forum focused exclusively on the Arctic

CSE continues to support the Canadian Armed Forces (CAF) as they monitor and track threats from foreign adversaries in the Arctic region. This includes supporting the Royal Canadian Navy and the Royal Canadian Air Force as they patrol the high north and defend Canada's sovereignty from foreign actors. We also provide indications and warning of Russian aircraft as part of Canada's joint command of the North American Aerospace Defence Command (NORAD), and monitor naval-based threats in an increasingly crowded space.

Border security and illicit synthetics

In December 2024, the Government of Canada announced its plan to strengthen border security and Canada's immigration system. Specifically, the government announced an investment of $180M over 6 years to expand CSE's intelligence collection and foreign cyber operations capacity, enabling CSE to target transnational organized crime and fentanyl trafficking more effectively. CSE's vital intelligence relationships—within the Government of Canada and with international partners—are an asset as we put Canada's Border Plan into action.

This year, we developed new campaigns to identify and disrupt transnational criminal networks responsible for fentanyl and synthetic opioid supply chains into Canada. We are working closely with domestic and international partners to achieve this priority objective.

We remain closely engaged with our Five Eyes partners, particularly with US counterparts, to share information and coordinate operations aimed at disrupting the transnational criminal networks involved in the supply chain of illicit synthetics. CSE is proud of our strong allied partnerships, which are crucial to our collective security.

Joint Operational Intelligence Cell

CSE is a lead contributor and active participant in the Joint Operational Intelligence Cell (JOIC). We work alongside the following JOIC partners to enhance the production, analysis, sharing and actioning of timely and relevant intelligence with federal law enforcement agencies and police of jurisdiction across Canada:

- Royal Canadian Mounted Police (RCMP)
- Canada Border Services Agency
- Public Safety Canada (PS)
- Canadian Security Intelligence Service (CSIS)
- Financial Transactions and Reports Analysis Centre of Canada

Hostile state activity

CSE's foreign intelligence provides important information and insights to support Canadian and allied efforts to counter activities of hostile states. This year, our foreign intelligence reporting continued to provide the Government of Canada and allies with analysis to support:

- monitoring for foreign interference activities and strengthening democratic processes
- securing Canada's innovation ecosystem from foreign disruption
- hardening critical infrastructures against sophisticated espionage attempts

People's Republic of China

The People's Republic of China (PRC) operates, and continues to expand, one of the world's most extensive and dynamic security and intelligence systems. PRC state-sponsored activities are involved in covert operations targeting democratic nations globally, including in Canada.

The PRC cyber program's scale, tradecraft and ambitions in cyberspace are second to none. Notably, to serve its high-level political and commercial objectives, the PRC targets Canadian interests with cyber operations, including:

- espionage
- intellectual property theft
- malign influence
- transnational repression

This year, in response to this threat, CSE intensified its engagement with partners across the government and internationally to develop actionable and timely intelligence. Specifically, we produced foreign intelligence on PRC-sponsored cyber threat actors targeting institutions and individuals across:

- government
- civil society
- military and defence
- media
- critical infrastructure
- advanced research and development sectors

Our foreign intelligence was critical in:

- protecting Canada's research security and democratic institutions from PRC state-sponsored threats
- empowering policy-makers to make well-informed decisions for Canada's economic security programs
- enabling the Cyber Centre and international partners to mitigate cyberespionage campaigns targeting government networks and critical infrastructure
- providing timely insights on PRC capabilities and equipping cyber defenders with actionable intelligence
- assisting the Cyber Centre in blocking cyber threat activities from botnets that had compromised thousands of residential and small office routers, or that had exploited vulnerable edge devices
- supporting Canadian and allied cyber defence partners to identify and respond to a cyber espionage campaign that targeted government networks by leveraging zero-day vulnerabilities and backdoors on perimeter devices

Russia

The Russian state and Russian-state aligned actors continue to push beyond the boundaries of acceptable international behaviour. This includes conducting economic espionage, spreading disinformation, discrediting the West, conducting malicious cyber activity, and promoting influence operations against Canada and our allies.

CSE continues to leverage our foreign intelligence mandate to help counter these threats. This year, our intelligence and timely reporting:

- helped inform Government of Canada policy objectives, including by identifying financial and industry entities that the Russian government is using to circumvent international sanctions to support its economy and ability to fund the war in Ukraine
- continued to support Canadian and allied efforts to confront and counter Russia's persistent disinformation efforts, which are part of a broader campaign to promote their narrative on the war in Ukraine, discredit the West, promote Russian influence and push for an end to Western sanctions
- pursued efforts to prevent Russian state actors from interfering in, obtaining sensitive information about, and sabotaging Canadian interests, including through cyber attacks

RT (Russia Today)

In September 2024, Canada issued a statement strongly condemning activities by Russian state-owned media entity RT (formerly known as Russia Today). These activities included attempts to diminish Western public support for Ukraine, influence electoral outcomes in Western and non-Western states, and undermine support for a commitment to the rules-based international order.

Canadian intelligence, to which CSE contributed, noted that Russia was using non-traditional assets to spread disruption and support for its hostile activities on an international scale, including in Canada. This work led to revelations that RT had developed third-party media platforms and was using them as tools to covertly disseminate content to international and Western audiences.

Cybercrime

Cybercrime remains a persistent, widespread and disruptive threat, sustained by a thriving and resilient global cybercrime ecosystem. CSE continues to monitor and analyze the foreign cybercrime threat ecosystem to enrich Canada's and Five Eyes partners' knowledge of cybercrime threat actors and the fluidity of the cybercrime ecosystem.

CSE produces intelligence on the tactics, techniques and procedures used by foreign-based cyber criminals and state actors. This intelligence provides the Cyber Centre with high-confidence data to disrupt attempts to scan and breach Government of Canada systems and other systems of importance.

This year, we identified thousands of indicators of compromise, which helped to defend Government of Canada networks and facilitate timely victim notifications. We also leveraged our SIGINT capabilities to inform operations led by international law enforcement to disrupt and dismantle foreign-based financially motivated cyber criminal groups.

Countering violent extremism

CSE works to identify the activities of foreign-based extremists who pose a threat to Canada and our allies. We provide valuable foreign intelligence to protect Canadians and Canadian interests from terrorism and violent extremism. This includes threats from religiously motivated violent extremism (for example, al-Qaeda and Daesh affiliates) and ideologically motivated violent extremism (for example, xenophobic, anti-authority, gender identity–driven and grievance-driven extremist ideologies).

This year, our efforts to counter violent extremism extended to supporting victims of kidnappings, reporting on extremist threats to allies, and covering threats to public events and to Canadian embassies and missions. Other examples of our efforts in this space this year include:

- working closely with domestic partners to provide critical information on foreign extremists aiming to direct attacks in Canada
- identifying threat actors responsible for bombs threats against entities in Canada
- working with domestic and international partners to produce foreign intelligence that identified foreign threat actors seeking to influence or inspire "lone-wolf" attackers in Canada and abroad
- helping international partners, on multiple occasions, to mitigate and disrupt violent extremist threats in their countries
- monitoring extremist threats to international events
- creating a surge team that worked with multiple foreign partners to defend against threats to the 2024 Paris Olympic Games

Support to military operations

CSE plays a vital role in supporting military operations by providing time-sensitive warnings and situational awareness to ensure the safety of CAF personnel during deployments and exercises. This year, we delivered timely intelligence for many named operations, including operations UNIFIER, REASSURANCE and HORIZON. This included providing foreign intelligence that:

- identified counter-intelligence threats to CAF personnel
- assisted in the evacuation of Canadians from conflict zones
- examined the activities of state-owned enterprises with links to military end-use, especially those capable of targeting Canadian operations and exercises
- identified enemy electronic warfare tactics, techniques and procedures to provide CAF with more insight on adversarial electronic warfare systems

This year, CSE supported an intelligence effort to identify legitimate business entities covertly supporting the military, political and commercial goals of foreign governments to disrupt CAF and allied operations.

Additionally, CSE continued to work to identify command, control, communications, computers, intelligence, surveillance, reconnaissance and targeting by foreign adversaries that could pose a threat to Canadian and allied forces conducting operations.

CSE also provides valuable intelligence to partner forces. Our intelligence efforts this year enabled CAF to inform partner forces of adversarial intent and capabilities, and to provide force protection to deployed personnel.

Conducting foreign cyber operations

The *CSE Act* is clear on the boundaries that our foreign cyber operations must not cross. CSE is prohibited from using cyber operations to "obstruct, pervert or defeat the course of justice or democracy." Likewise, our cyber operations must not cause death or bodily harm and can only be used against foreign targets "as they relate to international affairs, defence or security."

Under the *CSE Act*, foreign cyber operations must be authorized by the Minister of National Defence. In addition, the Minister of Foreign Affairs must request or consent to active cyber operations and must be consulted ahead of defensive cyber operations.

At CSE, we have a well-established governance framework to guide our foreign cyber operations and ensure that these operations adhere to the *CSE Act* and Ministerial Authorizations. This includes working closely with Global Affairs Canada (GAC) to assess the foreign policy impacts and legal implications of proposed cyber operations, taking into account both Canadian law and international law applicable in cyberspace[3].

Expansion of our foreign cyber operations portfolio

Budget 2024 announced additional funding for CSE and GAC to enhance intelligence and cyber operations programs to respond to the increasingly evolving and complex threats to Canadian national security, prosperity and democracy. This funding has allowed CSE to strategically expand the scope and scale of its foreign cyber operations efforts.

CSE was also directed by the Prime Minister to use the funding allocated as part of the border security initiative to bolster cyber operations to disrupt illegal drug supply chains (for example, fentanyl).

Joint cyber operations capability

Through the Government of Canada's Defence Policy Update and Budget 2024, CSE received significant new investments to continue to expand our foreign cyber operations program to counter the growing number of threats impacting Canada's safety and security.

In this updated policy, CSE, the Department of National Defence (DND) and CAF were directed to stand up a "joint Canadian cyber operations capability." This joint capability builds on CSE's foundational elements, and we are actively advancing this initiative in close partnership with the newly established Canadian Armed Forces Cyber Command (CAFCYBERCOM).

By investing in our people, tools and partnership, CSE and DND/CAF are building the cyber force of the future while continuing to counter the threats Canada faces today.

This year, CSE conducted numerous foreign cyber operations to:

- defend Canadians from malicious state and non-state cyber threats
- disrupt espionage activities directed at the Government of Canada
- counter foreign disinformation campaigns
- protect Canadians from violent extremism

Below, we have provided examples of foreign cyber operations undertaken this year to counter ransomware and disrupt violent extremist organizations (VEOs).

Countering ransomware

This year, CSE stood up a campaign to counter the 10 most significant ransomware groups impacting Canada and our allies.

We also participated in a multinational operation aimed at disrupting the activities of a ransomware actor. CSE used a variety of covert techniques to degrade and disrupt the illicit operations of this group, significantly impacting the group's ability to target Canadians.

Disrupting violent extremist organizations

In addition to enabling real-world disruptions of foreign extremist activities, CSE intelligence informed our active cyber operations against VEOs. Using a multi-faceted approach that targeted VEOs' technical infrastructure and online presence, CSE conducted active cyber operations to:

- damage the credibility and influence of key group leaders, reducing their ability to inspire and lead
- weaken trust and reduce cohesion between leaders and followers, undermining the unity and strength of these organizations
- highlight the legal and personal risks associated with engaging in VEO activities, potentially deterring individuals from involvement
- remove violent and extremist content from online platforms, denying VEOs a vital tool for radicalization and recruitment

Collectively, these actions weakened the online presence and influence of VEOs, making it harder for them to operate and reducing the threat they pose to Canada and our allies.

Publishing cyber threat assessments

In today's ever-changing threat landscape, keeping Canadians informed is more important than ever. We are committed to ensuring that all levels of government, Indigenous communities, critical infrastructure stakeholders, IT professionals and the general public understand the cyber threats that Canada is facing. That's why we publish timely, unclassified cyber threat assessments. On top of helping readers to understand and address the cyber threats Canada faces, these assessments also help us set our mission priorities.

This year, we published 2 major cyber threat assessments, the forward-looking National Cyber Threat Assessment 2025-2026 and an update to Cyber Threats to Canada's Democratic Process. We also published 5 unclassified threat assessments:

- Targeted manipulation: Iran's social engineering and spear phishing campaigns
- Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity
- The cyber threat to research laboratories
- Cyber threat bulletin: The cyber threat to major international sporting events
- Cyber threat bulletin: People's Republic of China-sponsored cyber activity against Canadian provincial, territorial, Indigenous, and municipal governments

As a result of these assessments, the Cyber Centre responded to dozens of requests for information and provided over 100 threat briefings to critical infrastructure providers and different levels of government.

National Cyber Threat Assessment 2025-2026

The National Cyber Threat Assessment (NCTA) 2025-2026 outlines key cyber threats from state adversaries, cybercrime threats, and trends shaping Canada's cyber threat landscape. The NCTA contains 6 key judgments:

- Canada's state adversaries are using cyber operations to disrupt and divide
- the PRC's expansive and aggressive cyber program presents the most sophisticated and active state cyber threat to Canada today
- Russia's cyber program furthers Moscow's ambitions to confront and destabilize Canada and our allies
- Iran uses its cyber program to coerce, harass and repress its opponents, while managing escalation risks
- the Cybercrime-as-a-Service business model is almost certainly contributing to the continued resilience of cybercrime in Canada and around the world
- ransomware is the top cybercrime threat facing Canada's critical infrastructure

NCTA reach and impact

The NCTA is a flagship product for CSE, so its reach and impact are critical. There was a significant increase in viewership for this year's NCTA. The report had over 3 times as many views in its first week of publication compared with the previous edition. Within one week, the NCTA was viewed by over 7,500 people. This included readers from around the world, particularly in Five Eyes countries. We are proud of how many readers the NCTA reached this year and are exploring new ways to amplify future reports.

ISSN 2816-9174
CAT D98-4E-PDF
CANADIAN CENTRE FOR CYBER SECURITY
NATIONAL CYBER THREAT ASSESSMENT
2025 2026
Canada

Cyber Threats to Canada’s Democratic Process

In March 2025, CSE published an update on cyber threats to Canada’s democratic process, highlighting the growing use of AI by foreign adversaries to target elections worldwide, including in Canada. The report outlined the following key findings:

- foreign actors, particularly those affiliated with Russia and the PRC, are leveraging AI to sow division and distrust within democratic societies
- hostile foreign actors are using AI to flood the information environment with false information, including by enabling the creation of disinformation and of social botnets to spread it
- foreign actors are increasingly using generative AI to create and spread viral disinformation with the potential for greater impact as these methods evolve and become even more accessible
- cybercriminals and state-sponsored actors will likely use AI to enhance social engineering attacks against political figures and electoral institutions in the near future
- nation states are collecting massive amounts of data and are using AI to analyze it faster than ever, further enhancing their ability to conduct targeted influence and espionage campaigns
- AI is being used to create deepfake pornography targeting politicians and public figures, predominantly women and 2SLGBTQIA+ people

During the first week of the update’s release, the report’s page was visited almost 2,000 times and related social media posts had over 16,000 views. The report received widespread news coverage in major media outlets—reaching an estimated audience of over 13 million people.

ISSN 2563-8165
CAT D95-10E-PDF
Cyber Threats to
CANADA’S
Democratic Process
2025
Update
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada
Canada

Protecting Canada's democratic institutions and critical infrastructure

Across the globe, cyber threat activity targeting democratic processes and critical infrastructure is on the rise. In 2024 to 2025, CSE worked with key stakeholders to help protect the integrity of Canadian elections, democratic institutions and critical infrastructure. This included holding briefings to raise awareness on evolving threats and working with partners to increase cyber security resilience across this important landscape.

Support to federal institutions

CSE and the Cyber Centre continued to support federal institutions this year to respond to cyber incidents, mitigate cyber threats, brief departments that experienced cyber incidents, and generally enhance cyber resilience across the federal landscape. We worked with 150 Government of Canada organizations and delivered comprehensive briefings focused on small departments and agencies, which were identified as being at increased risk of cyber threats and attacks.

Throughout the year, we provided various support and services to federal institutions to help increase cyber resilience across the federal government landscape. This included:

- delivering advice and guidance
- conducting supply chain integrity assessments
- supporting secure communications capabilities
- monitoring and producing threat assessments in support of high-impact, high-priority and high-risk government projects, services and initiatives
    - » for example, Shared Services Canada's Endpoint Visibility Awareness and Security, the Government of Canada's Secret Infrastructure Next Generation, and the Employment and Social Development Canada (ESDC) Benefits Delivery Modernization program

Security and Intelligence Threats to Elections task force

The Security and Intelligence Threats to Elections (SITE) task force is a whole-of-government working group that coordinates Government of Canada collection and analysis efforts concerning threats to Canada's federal election processes. As a member of the SITE task force, CSE works alongside CSIS, the RCMP and GAC.

This year, the SITE task force monitored and assessed foreign interference threats to federal by-elections and, for the first time, a federal political party's leadership race. CSE's foreign signals intelligence program sought out foreign intelligence on:

- intent or action by foreign state actors to interfere in or influence Canada's democratic processes
- attempts to affect the outcome of Canadian democratic processes or undermine public confidence in the integrity of these processes
- foreign cyber threats directed at democratic institutions, including elections infrastructure, candidates or parties

The Cyber Centre helped to ensure the cyber security of these events by:

- monitoring for malicious cyber activity targeting Elections Canada or the electronic information and infrastructure of democratic institutions (including political parties)
- briefing the political parties on common cyber threats and cyber security best practices
- offering a 24/7 hotline for parties and candidates to report cyber incidents

Supporting preparation efforts for the 2025 general election

After the 2025 general election was called on March 23, 2025, CSE jumped into action to support Elections Canada. Our team secured the necessary accreditations, facilitated training, and ensured that the appropriate Elections Canada personnel had timely access to Canada's Top Secret Network to access critical, classified information.

The majority of the general election period occurred outside the 2024 to 2025 fiscal year and is therefore out of scope for this report. CSE looks forward to sharing details on our efforts during this period, including our work in support of the Critical Election Incident Public Protocol and in response to observed cases of transnational repression, in next year's annual report.

National Cyber Security Strategy

In February 2025, the Government of Canada released its new National Cyber Security Strategy (NCSS)[4]. The NCSS articulates Canada's long-term plan to partner with provinces, territories, law enforcement, industry, Indigenous communities and academia to tackle Canada's cyber security challenges.

An important player in the NCSS, CSE is responsible for:

- protecting government systems
- leading cyber security defence and incident response technical efforts
- acting as Canada's technical authority on cyber security
- providing advice, guidance and services to various sectors
- promoting collaboration, partnership, innovation and cyber skills across sectors

As Canada's operational cyber security leader, the Cyber Centre provides threat intelligence and guidance.

CSE's contributions through the NCSS

CSE has already made significant contributions through the NCSS. For example, in coordination with Five Eyes partners, we have closely followed cyber threat activity by PRC state-sponsored actors, including Volt Typhoon and Salt Typhoon. Additionally, the Cyber Centre has engaged directly with Canadian service providers to help contextualize the nature and significance of the threat posed by the Salt Typhoon hacking campaign.

The Canadian Cyber Defence Collective

Under the NCSS, the Government of Canada established the Canadian Cyber Defence Collective (CCDC). The CCDC's 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 to help protect systems of importance and reduce Canada's cyber threat surface

The CCDC-O includes a select group of trusted national and international cyber defender partners from both the public and private sectors. The composition of the CCDC-O will change according to operational needs.

The CCDC-O is still in the process of being stood up. This year, the focus was on establishing the processes and technology required to support coordinated activities between various industry partners. An initial meeting for one CCDC subgroup was held in January 2025.

The CCDC-SF, co-chaired by PS and the Cyber Centre, is the definitive 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. Like with the CCDC-O, work to stand up the CCDC-SF is currently underway.

Support to provinces and territories

Cyber threat actors like the PRC almost certainly view provincial, territorial, Indigenous and municipal governments as valuable targets for cyberespionage. Cyber threat activity targeting these levels of government likely mirrors the ongoing activity targeting the Government of Canada. All government networks hold information on decision-making and regional affairs, as well as personal information of Canadians.

Increasing cyber security collaboration with the provinces and territories remains a top priority for CSE. We are working with provincial and territorial partners to mitigate ongoing compromises and to warn of potential malicious cyber threat activity from sophisticated actors. We are also enabling other levels of government to better assess threats and remediate compromises to their systems.

In 2024 to 2025, following a series of cyber incidents targeting northern institutions, and with the Minister's authorization, the Cyber Centre began proactively deploying sensors to territorial government IT assets in Yukon, the Northwest Territories and Nunavut. These sensors 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.

Helping provinces and territories better understand their cyber security threat posture

This year, provinces and territories with access to our sensor services were also granted access to ObservationDeck, an interactive web application that aggregates data from Cyber Centre security services so that users can better understand their unique cyber security threat posture. ObservationDeck reporting is enriched with commercial, open-source and in-house analytics that summarize departmental IT assets and their vulnerabilities.

The Cyber Centre also hosted the second annual cyber security roundtable devoted solely to collaboration between federal, provincial and territorial cyber security leads. Discussion topics included incident response planning, supply chain risk management, support for elections, and threats introduced by disruptive technologies.

The Cyber Centre actively helps provinces and territories better understand their cyber security posture. This includes offering classified briefings, which give additional information on active and potential threats to the partners. This year, the Cyber Centre provided one classified threat briefing to provinces and territories, providing critical insights into current and emerging cyber threats. The Cyber Centre also delivered briefings at various classification levels to multiple provincial and territorial officials, including premiers and election authorities.

Support to Indigenous communities

The Cyber Centre has a dedicated Indigenous Partnerships team that focuses on building relationships based on the recognition of rights, respect, and partnership. We follow the principle of "Nothing about them without them" and ensure that initiatives and projects are community-driven and nation-based and are focused on removing barriers. This year, the Indigenous Partnerships team:

- participated in an Arctic Security Working Group that brings together federal, territorial and Indigenous governments
- participated in the National Indigenous Information Technology Alliance Conference
- offered Cyber Centre services and advice and guidance to Indigenous organizations
- built relationships with Indigenous entities in support of cyber incident response activities

We also published a cyber threat bulletin on PRC-sponsored cyber activity against Canadian provincial, territorial, Indigenous, and municipal governments[5], which we shared with Indigenous governments.

Support to critical infrastructure

Ensuring that we continue to develop strong partnerships with critical infrastructure is vital in preventing disruptions that could have widespread and severe consequences to Canadians. We establish strategic partnerships with Canada's critical infrastructure owners and operators to share advanced cyber threat information, promote the integration of cyber defence technology and foster strong engagement.

This year, we collaborated and built partnerships with critical infrastructure in the following ways:

- collaborating with mobile network operators and global security experts to identify emerging threats and initiate activities to increase the cyber resilience of Canadian 5G networks
- participating in over 200 speaking engagements across critical infrastructure sectors such as:
  - energy (electricity, oil, mining, nuclear)
  - small and medium organizations
  - water
  - defence industrial base
  - health
  - transportation
  - finance
  - telecommunications and information and communication technology
- providing 38 biweekly threat briefings, each of which had over 600 participants, for IT security professionals in Canada's critical infrastructure sectors

- participating in 13 tabletop exercises
- holding 7 "walk-the-talk" sessions to provide actionable information and expert briefings on technical topics like AI, the quantum threat and post-quantum cryptography, and cybercrime

Co-hosting the inaugural National Security Threat Forum for Federally Regulated Financial Institutions

In February, CSE was pleased to co-host the inaugural National Security Threat Forum for Federally Regulated Financial Institutions (FRFI) with our partners at CSIS and the Office of the Superintendent of Financial Institutions Canada (OSFI). The forum brought together over 150 representatives from FRFIs, federal and provincial authorities, and national security experts to discuss the threat environment as it relates to Canada's financial sector.

Subject matter experts from the Cyber Centre, as well as experts from CSIS's Financial Intelligence Centre and Economic Security and Technology Mission Centre, delivered tailored briefings on the threat environment to financial sector stakeholders.

In addition to increasing awareness of the threat environment among a key critical infrastructure audience, this event set the stage for strong partnerships and new collaboration opportunities with other government departments, including OSFI.

Supply chain risk assessments

As part of supporting and protecting federal critical infrastructure, CSE conducts risk assessments for Government of Canada clients looking to procure IT equipment. These assessments look at numerous factors, including technical vulnerabilities of products and the business practices, cyber maturity and foreign ownership of vendors. CSE increasingly works with partners outside the federal government—such as provinces, territories and private sector partners—on supply chain risks.

This year, CSE conducted 1,371 supply chain risk assessments. We also released 2 guidance publications related to supply chain security:

- Cyber supply chain security for small and medium-sized organizations (ITSAP.00.070)[6]
- Joint guidance on choosing secure and verifiable technologies[7]

Communications security

We are Canada's communications security (COMSEC) authority. Through our information assurance mandate, we continue to evolve our COMSEC program thanks to a collaborative and supportive COMSEC community that stretches across the Government of Canada.

As part of our secure communications program, we soft-launched the Trusted Integrator program[8] this year. This program recognizes third-party IT security organizations that have demonstrated knowledge and experience in the development, implementation and testing of secure tailored solutions.

This year, CSE also hosted our annual Secure Communications User Group workshop, bringing together operational and strategic COMSEC communities to identify synergies, improve workflows and reinforce secure practices.

Our COMSEC team also hosted Chief Security Officers and departmental and enterprise COMSEC authorities at a classified event to discuss the evolving cryptographic landscape and the importance of collaboration to stay ahead of threats.

Preparing for quantum safe cryptography

Cryptography is a fundamental part of cyber security and is essential to keeping data and communications secure. However, as early as the 2030s, quantum computers are expected to become large enough to break the cryptography currently in use worldwide.

At CSE, we don't panic, we plan. Through our information assurance mandate, CSE continues to modernize our cryptographic systems. We also took many steps to educate government, industry and critical infrastructure partners on the quantum threat and to help stakeholders prepare for the transition to post-quantum cryptography. Some key activities this year included:

- publishing updated cryptography guidance
- continuing to contribute to the international standardization process for quantum-safe cryptography; for example, by providing public feedback on 3 draft standards led by the US National Institute of Standards and Technology
- working with federal partners to plan for the rollout of quantum-safe cryptography across the Government of Canada once the international standards are finalized
- providing over 30 briefings to government, industry and critical infrastructure partners on the quantum threat and how to prepare for the quantum-safe transition, including briefings on the importance of using standardized and validated cryptography to prevent unnecessary security vulnerabilities
- participating in Migration to Post-quantum Cryptography Industry Day by delivering a presentation to key industry partners on the Government of Canada's transition strategy for post-quantum cryptography

Responding to and preventing cyber incidents

This year, the Cyber Centre's Intake Centre received, triaged and managed roughly 13,500 general inquiries, which included requests for:

- cyber security advice and guidance
- subscriptions to Cyber Centre services and tools
- incident management coordination and support

My Cyber Portal

The increase in general inquiries this year was partly driven by requests for new services offered through My Cyber Portal[9], a tool through which users across Canada can report cyber incidents and submit malware samples.

My Cyber Portal had over 1,000 Government of Canada and over 2,600 non-Government of Canada users this year. We also undertook work this year to expand My Cyber Portal and refresh the interface to allow federal institutions to receive and view cyber incident cases.

Incident management

This year, the Cyber Centre helped respond to 2,561 cyber security incidents across the Government of Canada (1,155) and Canadian critical infrastructure (1,406). This was an increase over last year (2,192 incidents), largely due to an increase in cases targeting critical infrastructure.

The Cyber Centre also received 843 cyber incident reports from federal institutions (463) and Canadian critical infrastructure (380).

The Cyber Centre's definition of a cyber incident[10] covers a wide range of attempted threat activity, whether successful or not.

Pre-ransomware notifications

Pre-ransomware notifications provide early warning to potential victims during the initial access stage of a ransomware incident. They enable network defenders to pinpoint the compromise and thwart it before any encryption or data theft occurs.

This year, the Cyber Centre issued 336 pre-ransomware notifications to 309 Canadian organizations. The would-be victims included every level of government and key sectors, such as healthcare, energy, manufacturing, finance and education.

Pre-ransomware notifications rely on 3 key sources of information:

- Cyber Centre research into the behaviour of malware and its related infrastructure
- collaboration with trusted industry partners
- collaboration with the US-led Joint Ransomware Task Force

Example of a pre-ransomware event

Here is an example of how the Cyber Centre responded to a pre-ransomware event this year:

- The Cyber Centre received information from a trusted partner that a Canadian critical infrastructure institution's system contained initial access malware for ransomware
- The Cyber Centre worked closely with Canadian partners in cyber incident response to deliver a pre-ransomware notification after hours to the affected institution
- The institution quickly disabled and blocked accounts and devices to mitigate any immediate threat
- The Cyber Centre met with the institution to provide advice and guidance on preventing similar future incidents

Financial impact of pre-ransomware notifications

According to the Statistics Canada bulletin The Impact of Cybercrime on Canadian Businesses[11], 16% of Canadian businesses experienced a cybersecurity incident in 2023. Among victims who paid a ransom, 84% paid less than $10,000, and 4% paid over $500,000. Total recovery costs in 2023 amounted to approximately $1.2 billion.

Using conservative assumptions and average recovery cost estimates, the Cyber Centre's pre-ransomware notifications may have averted between 74 and 148 ransomware incidents in 2024 to 2025, resulting in estimated economic savings of $6 to $18 million. This also only accounts for a portion of the true benefit since the Statistics Canada data does not include indirect costs such as reputational damage, operational downtime, legal fees, or insurance impacts.

Providing support and expertise to global events

CSE operates 24/7, ready to address threats to Canada or Canadians abroad. The CSE Operational Production and Coordination Centre (COPCC) coordinates responses to critical cyber incidents and international crises. This year, COPCC:

- alerted the Cyber Centre to 94 cyber security incidents after hours
- notified CSE stakeholders of 18 significant terrorist or global incidents
- notified CSE stakeholders of 82 potential significant events

Support to missions in the Middle East

During a year of war and upheavals in the Middle East, COPCC liaised with other Government of Canada departments and shared information on the conflict in Lebanon, the overthrow of the Assad regime in Syria, and the overall Middle Eastern geopolitical situation.

Additionally, COPCC coordinated CSE's support for commercial flight options for Canadians evacuating Lebanon and prepared for a possible non-combatant evacuation due to the Israel-Hezbollah conflict.

Support to the Paris 2024 Olympic Games

COPCC coordinated CSE's cyber security and intelligence efforts to ensure the security of the Olympic and Paralympic games in the summer of 2024. This included liaising with the Cyber Centre to deliver effective cyber security briefings to key stakeholders and attendees and engaging with international partners to share information and postures in support of the event.

Cyber security assistance to Ukraine and Latvia

The Cyber Centre has been working to support Ukraine and Latvia with cyber security since 2022, when the Minister of National Defence designated the cyber systems of these countries as being of importance to Canada.

Assistance to Ukraine

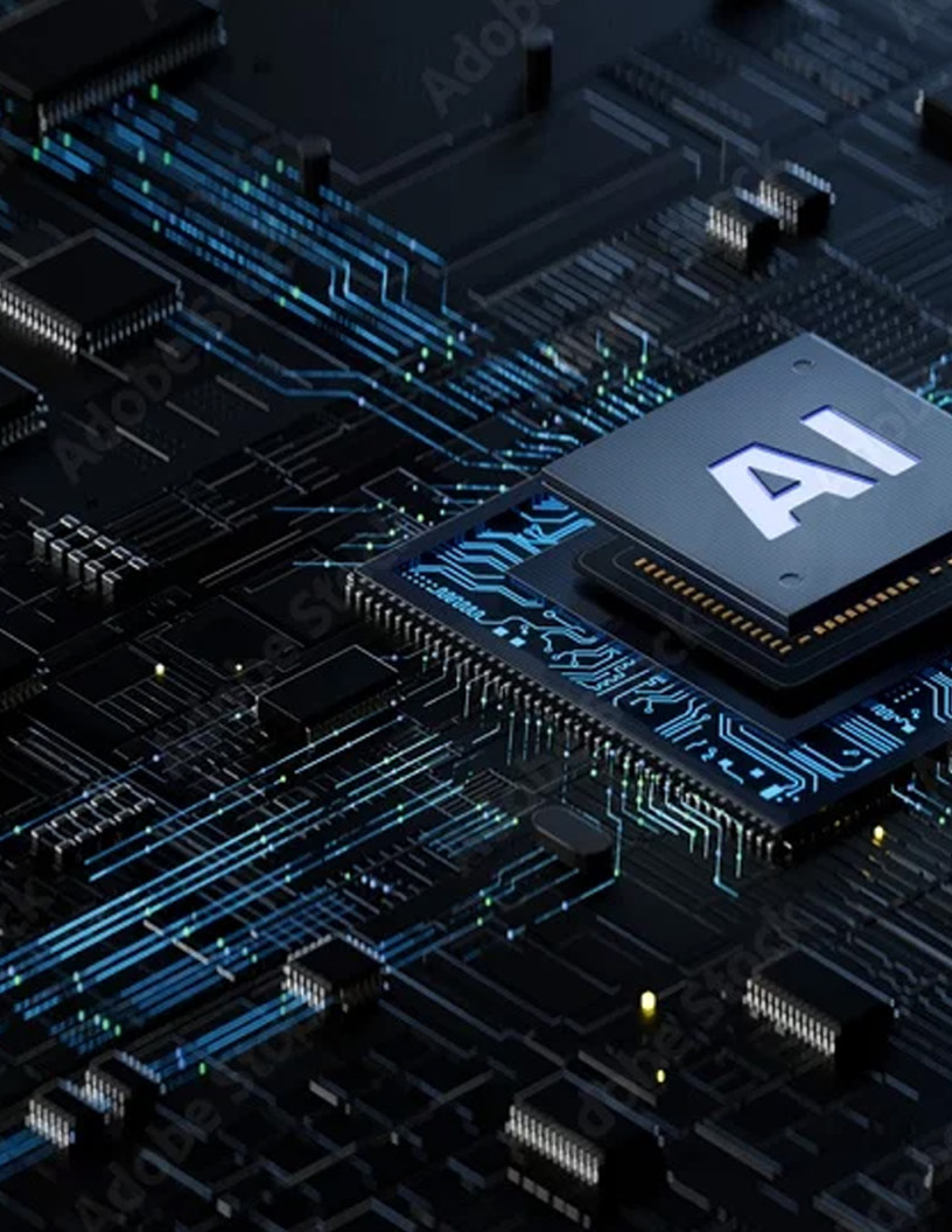
CSE continued to leverage our foreign intelligence mandate to support Ukraine's resistance to Russia's ongoing, unjustifiable invasion. As part of Operation UNIFIER, CSE has begun sharing our file triage and malware analysis platform with the Ukrainian Forces, providing the same in-depth malware discovery services that are used to protect Government of Canada networks.

By leveraging a common platform, both Ukrainian and Canadian (DND and CSE) analysts can collaborate on file investigation and provide valuable insights into newly discovered malware.

Assistance to Latvia

Cyber Centre teams deployed to Latvia 3 times this year in a joint effort with the CAF (Operation REASSURANCE) and Latvia's cyber security agency, CERT.LV. This included:

- a 5-week surge to Latvia
- a 2-week surge supporting a critical infrastructure organization in the energy sector
- a 1-week training deployment in Latvia focused on POLARIS, our advanced live cyber range, with participants from NATO Computer Emergency Response Teams (CERTs), the CAF and the Ukrainian military


AI

CSE IS INNOVATING AND EVOLVING

CSE is a learning organization. As a result, we are constantly collecting, interpreting and analyzing information and data. Innovation and research are paramount to our mission success. We are always working to remain at the forefront of advances in technology not only to defend Canada from threats but also to ensure that we are leveraging all available tools to deliver on our mandate.

Promoting the responsible use of artificial intelligence

AI has long been integral to CSE's operations, enhancing our mission by providing better and faster insights in a rapidly changing threat landscape. CSE made many exciting strides in the AI space this year, including:

- launching our AI strategy
- contributing to Government of Canada efforts to develop AI standards
- conducting outreach activities to address concerns about the growing use of AI
- exploring efficiencies with AI in the workplace

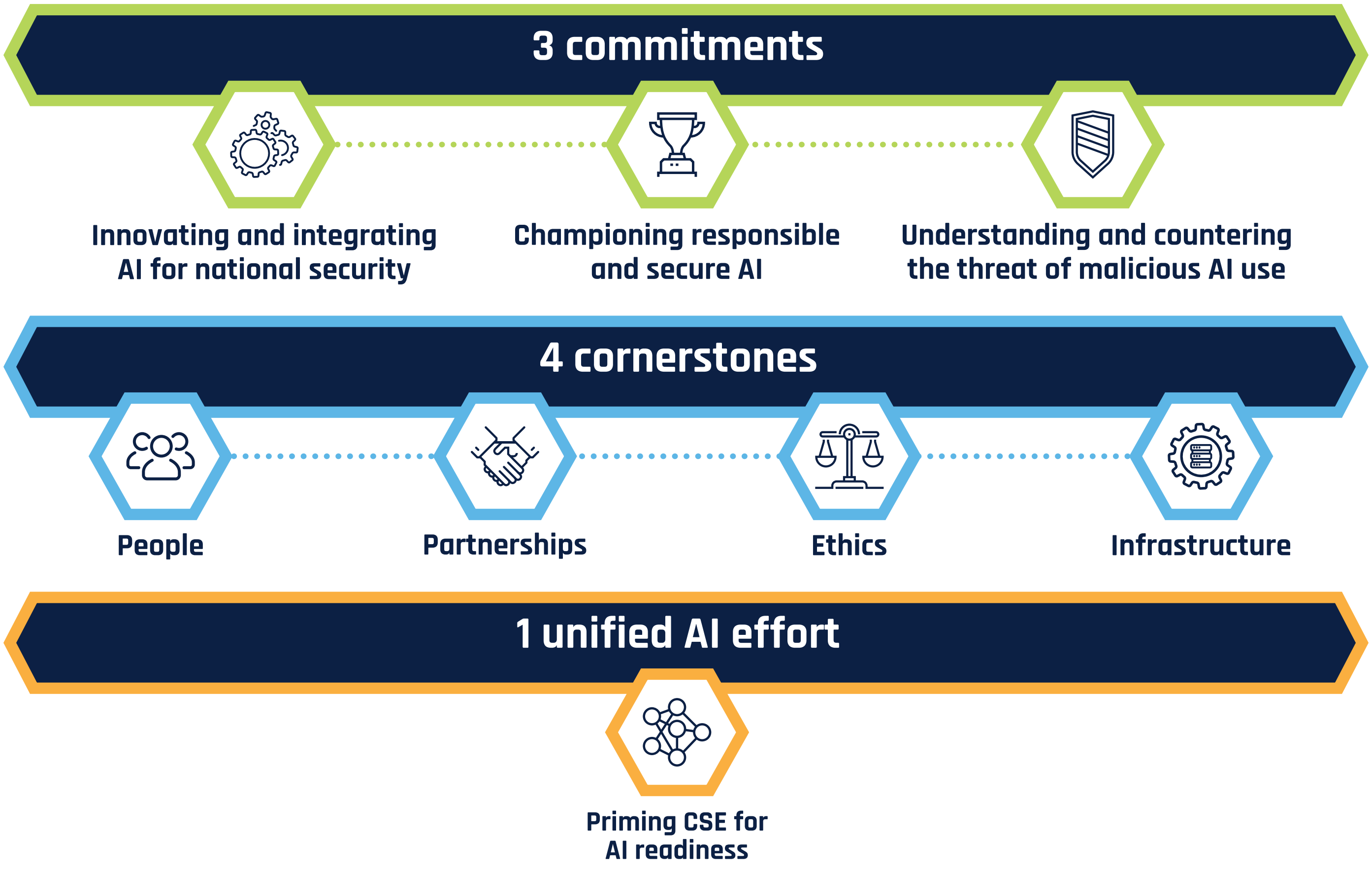
CSE's Artificial Intelligence Strategy

This year, we launched the CSE Artificial Intelligence Strategy[12]. This foundational document focuses on purposeful innovation, equipping our workforce, and expanding partnerships across industry, academia and with international allies.

The CSE AI Strategy is built on a 3+4+1 framework. Three key commitments define our purpose: innovating and integrating AI for national security, championing responsible and secure AI, understanding and countering the threat of malicious AI use. Four cornerstones—people, partnerships, ethics and infrastructure—underpin our efforts. And one unified AI effort will guide implementation, fostering a cohesive approach as we evolve our ways of working to achieve the strategy's objectives.

The CSE AI Strategy empowers our workforce to use AI responsibly and provides our team with a unique skillset in the federal government. It also complements wider Government of Canada priorities, such as the Canadian Artificial Intelligence Safety Institute (CAISI) and the AI Strategy for the Federal Public Service.

CSE is committed to building and using AI capabilities ethically, responsibly and securely—addressing AI's risks while maximizing its benefits.



3 commitments

Innovating and integrating AI for national security

Championing responsible and secure AI

Understanding and countering the threat of malicious AI use

4 cornerstones

People

Partnerships

Ethics

Infrastructure

1 unified AI effort

Priming CSE for AI readiness

Leveraging data science and artificial intelligence for in-house innovation

CSE hosts an annual workshop where participants from Canada and the Five Eyes work to solve complex problems facing the SIGINT community. This year, many teams used AI and data science to build new tools capable of analyzing very large datasets to automate tedious daily tasks and augment analysis capabilities.

As a result of this year's workshop, CSE implemented a Retrieval-Augmented Generation (RAG) prototype on analyst training material to enhance analytical processes and improve efficiency. This revolutionized the analyst learning experience, providing analysts with instant access to information and accelerating their skills development. Other exciting workshop outcomes included:

- applying data science techniques to explore datasets and reveal valuable insights about the intentions of malicious cyber actors
- implementing semantic search and topic modelling for rapid data triage to quickly identify and prioritize critical intelligence, leading to better reporting

Contributing to Government of Canada efforts in artificial intelligence

As a leader in AI research and innovation, CSE contributes to various efforts across the Government of Canada to assess AI risks and mitigations to ensure robust and secure AI deployment. In 2024 to 2025, this work included:

- serving as a member of the ESDC Benefits Delivery Modernization Innovation Office
- participating in the Shared Services Canada AI Governance Working Group
- providing strategic direction on plans, priorities and research projects for CAISI

Canadian Artificial Intelligence Safety Institute

Launched in November 2024, CAISI is an initiative led by Innovation, Science and Economic Development Canada (ISED) to support the safe and responsible development and deployment of AI. CAISI is dedicated to understanding AI risks, providing tools to mitigate these risks, and ensuring the safe and trustworthy adoption of AI technology.

Outreach activities related to artificial intelligence

To address growing concerns around AI threats, CSE and the Cyber Centre have been actively engaging with various stakeholders. This year, we delivered presentations to diverse audiences, including:

- the Federal-Provincial-Territorial Conference
- Alberta Energy
- BHP Saskatoon
- Elections Canada
- senior Government of Canada executives

These presentations covered topics such as AI threats, mitigation strategies, deployment considerations, phishing, malware and deepfakes.

AI-related training for public servants

This year, the Cyber Centre's Learning Hub launched 2 new courses on existing Government of Canada guidance for the use of generative AI, how users can leverage generative AI safely at work, and the ethical concerns and limitations of generative AI.

Testing Microsoft 365 Copilot

Like many other workplaces across Canada, CSE is exploring how AI can increase efficiencies and support our teams. This year, through Microsoft's Early Access Program, 300 users across CSE piloted Microsoft Copilot and Personal Assistant. Pilot participants ranged from working-level employees to executives.

CSE was able to tailor the tool to our specific functions, maintaining our secure environment and need-to-know posture, all while continuing to protect sensitive information. This pilot allowed CSE employees to test out a range of different ways to securely apply AI to support their work activities.

Improving classified infrastructure and services

As a security and intelligence organization, CSE conducts much of its work using classified networks and tools. In 2024 to 2025, we applied our dedication to innovation and agile information-sharing with partners to some exciting improvements.

SIGINT Canada project

This year, CSE undertook a groundbreaking initiative in data and information stewardship through the SIGINT Canada project. This project transformed the collection, management and secure sharing of sensitive data within Canada's national security infrastructure.

SIGINT Canada modernized IT infrastructure and streamlined the sharing of critical data and services between CAFCYBERCOM and CSE. By integrating advanced technologies, SIGINT Canada has enhanced the efficiency, security and interoperability of critical data-sharing systems across Canada's civilian and military SIGINT communities.

Key achievements of the SIGINT Canada project include:

- improved data sharing: deploying a standardized infrastructure across various agencies for secure, real-time access to critical data and services from multiple endpoints, improving collaboration and decision-making
- operational efficiency: introducing new systems and processes to streamline data management, which reduced complexity and increased the speed of decision making
- strengthened security: implementing advanced cyber security measures, which ensured that sensitive data was securely managed, shared and protected across high-security networks and international partners
- enhanced interoperability: creating a unified service delivery model that allowed for greater data integration and cross-agency collaboration, which facilitated smoother communication and data exchange between government entities and international partners

Expansion of Canada's Top Secret Network

Departments across the Government of Canada increasingly need to access intelligence to fulfill their mandates and deliver on their operational activities. As a result, CSE has seen continued growth and an increasing demand for Top Secret network services.

CSE operates Canada's Top Secret Network (CTSN), a secure IT network used to collaborate and communicate at the Top Secret level. This year, CSE supported major site expansions for existing CTSN clients, including the National Security and Intelligence Review Agency (NSIRA), PCO, Justice Canada and the RCMP, resulting in a 20% increase of deployed endpoints.

In the upcoming year, CSE will onboard 3 new government departments to CTSN:

- Environment and Climate Change Canada
- Public Prosecution Service of Canada
- Office of the Commissioner of Canada Elections

CSE also deployed a significant number of its Top Secret terminals at CAFCYBERCOM and its satellite stations across Canada, and in support of deployed military operations.

Upgrades to key enabling classified systems

This year, a system that provides the Cyber Centre with indicators of cyber threat infrastructure—which are detected through CSE's SIGINT systems—in near real time underwent a significant upgrade. This system supplies Government of Canada cyber defence tools with high-confidence data to dynamically disrupt malicious activity.

In line with our mandate, we implemented a similar system this year that detects Canadian victims of foreign cyber threats through CSE's SIGINT systems and reports this activity to the Cyber Centre.

These systems ensure that the Cyber Centre receives actionable information acquired through CSE's foreign intelligence operations. This, in turn, helps to defend Canadian networks and facilitates timely notifications to Canadian entities to mitigate the impact of foreign cyber threats.

Fostering innovation and partnerships through open sourcing

Over the past year, the Cyber Centre continued to pursue open-source projects to support the broader cyber defence community. The Government of Canada, systems of importance and private organizations continued to leverage and implement our open-source tools to support their cyber security infrastructures.

Our commitment to open sourcing has fostered new partnerships, enhancing the tools we develop and accelerating advancements in malware detection and triage. The Cyber Centre remains at the forefront of the community and looks forward to releasing additional tools as open source in the coming year.

Conducting research and strengthening research partnerships

CSE's Research Directorate partners with groups inside and outside the organization to help drive innovation and develop impactful new capabilities that support CSE's mission.

This year, the Research Directorate launched a new vision and strategic plan to inform their work from 2025 to 2027. The strategic plan will focus on the mathematical foundations of cryptography; foundations of machine learning and AI; model training, adaptation and security; and vulnerability research. The vision identified 5 key challenges that can be addressed through research:

- continually improving CSE's access to systems and data
- enhancing CSE's ability to process and refine massive quantities of information
- improving the efficiency and effectiveness of data and information analysis
- safeguarding the security and integrity of systems and information
- retaining a scientific or technological advantage over our adversaries

CSE is leveraging tools and developing innovative research partnerships to expand models and leverage talent, all in service of our mission.

Tutte Institute for Mathematics and Computing

Over the past year, the Tutte Institute for Mathematics and Computing (TIMC)[13] continued to develop foundational theory, innovative techniques and effective tooling in its 2 focus areas: cryptography and data science.

Where possible, TIMC makes its tools available publicly, publishes results in academic journals and presents at conferences. This year, TIMC contributed to the academic community by:

- publishing 12 journal articles
- producing 5 software releases of new or significantly updated code
- organizing 3 conferences
- editing 1 conference proceedings
- conducting a podcast interview and participating in multiple panel discussions
- giving 3 invited talks and 7 presentations at external conferences
- holding positions on the Canadian Mathematical Society Board and committees

Software libraries from TIMC averaged over 2.5 million downloads per month.

Fostering strong partnerships

TIMC is committed to fostering strong partnerships with the Canadian scientific community. TIMC provides financial support to mathematics and computer science conferences that align with its research interests and provides financial support to events organized by local universities.

This year, TIMC provided financial support to 8 mathematics and computer science conferences and to 8 events organized by local universities.

Vulnerability Research Centre

Through our Vulnerability Research Centre (VRC)[14], CSE continues to conduct applied vulnerability research in support of our mandate and those of our federal partners. Over the last year, we discovered numerous vulnerabilities and responsibly disclosed 10 vulnerabilities to the affected vendors.

This year, the VRC partnered with Ontario Tech University and the University of Toronto for the first time. The VRC also continued its partnership with Concordia University to improve vulnerability research tooling.

GeekWeek 9

For the 9th year in a row, the Cyber Centre hosted GeekWeek[15], an annual unclassified workshop that brings together key players in the field of cyber security to generate solutions to vital problems facing the industry. This year's theme was **Animating cyber security**[16]. The Cyber Centre was happy to welcome participants from government, the private sector, critical infrastructure, and international partners.

CSE-NSERC Research Community on Robust, Secure and Safe Artificial Intelligence

CSE continued our partnership with the Natural Sciences and Engineering Research Council of Canada (NSERC) to fund research communities to conduct unclassified research on cutting-edge technologies in areas 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 Robust, Secure and Safe AI for the project "An End-to-End Approach to Safe and Secure AI Systems." This community, led out of the University of Toronto, comprises 19 co-applicants from 5 Canadian universities. They will research, develop and demonstrate solutions for AI-related issues, including:

- creating methods to train AI models in situations where reliable, labelled data is unavailable without relying on external, untrusted pre-trained foundation models
- developing techniques to ensure AI models are robust, fair and interpretable
- establishing guidelines for AI use to ensure regulatory compliance and support the auditing process

This is the first of 4 communities created as part of the NSERC-CSE Research Communities grants[17].

CSE IS EMPOWERING AND REACHING CANADIANS

CSE delivers cyber security training and publishes clear guidance to empower Canadians to make responsible and informed choices. Through outreach activities, social media and innovative ad campaigns, CSE is reaching Canadians to ensure they understand how to navigate today's cyber environment.

Finding new ways to educate Canadians

Education is one of the best tools that Canadians can use to protect themselves from cyber threats. CSE and the Cyber Centre are dedicated to finding innovative, accessible ways to help Canadians educate themselves on cyber security, cyber hygiene and cyber threats.

Online learning and training

The Cyber Centre Learning Hub[18] provides training in cyber security and communications security. Services are available to those working within the Government of Canada, other levels of governments, critical infrastructure organizations, small and medium organizations and educators. This year, total enrollment for Learning Hub courses reached 11,895.

ChatterHigh collaboration

This year, the Learning Hub was pleased to collaborate with ChatterHigh on "Keep Canada Safe! Discover Careers in Cyber Security," a course for K-12 students. This course is available through ChatterHigh and is free for all Canadian teachers and students.

Discover Cyber Security

With the Canada School of Public Service, the Learning Hub co-developed the course, "Discover Cyber Security." Through this course, participants learn to recognize potential threats and how to protect themselves, their digital information, and the systems they use. This course is free and accessible to public servants at all levels and the general public.

Get Cyber Safe campaign

CSE shares cyber security advice directly with Canadians through our Get Cyber Safe public awareness campaign. Get Cyber Safe offers simple, practical tips to help Canadians protect themselves as they go about their lives online.

Get Cyber Safe produced over 46 new resources this year, expanding guidance on a range of cyber security topics, including:

- expanding our romance scam content with a quiz on how your love language can help you get cyber safe[19] and a blog post outlining romance scam tactics to watch for[20]
- adding new resources on e-transfer fraud[21]
- providing new information on staying safe with payment methods[22], in partnership with the Canadian Anti-Fraud Centre
- creating a video that shows Canadians how to report spam text messages[23] on their devices

We also added resources on the new ways that cyber criminals are using AI to trick people into falling for their scams, and some practical tips on how to stay safe:

- The next generation: Spotting content created with artificial intelligence[24]
- Recognize AI: 9 ways to spot AI content online[25]
- How cyber criminals are using AI for online threats[26]
- Why you should never give your personal information to AI[27]

Get Cyber Safe for Indigenous audiences

To better serve First Nations, Inuit and Métis audiences across Canada, CSE continued to expand outreach through culturally relevant and accessible resources. Like last year, this included translating Get Cyber Safe's most downloaded infographics into Ojibwe, Cree, Inuktitut and Mi'kmaq.

This year also marked the launch of a more structured outreach strategy through Indigenous Link, a trusted Indigenous-owned communications firm with a strong presence in rural, urban and remote communities. The partnership included:

- community bulletin board poster distribution
- targeted email campaigns to over 22,000 opt-in subscribers
- development of a landing page with translated materials[28]

Through these efforts, CSE sought to increase awareness and trust among Indigenous communities and ensure equitable access to cyber security information.

Get Cyber Safe for small businesses

No business is too small to be of interest to cybercriminals. However, for many small businesses, investing in costly or complex cyber security solutions is not always realistic. This year, CSE added to its series of resources for small business owners[29] with an incident plan template and learning topics to help business owners get the right training for their staff.

Cyber Security Awareness Month

Every October, CSE leads Cyber Security Awareness Month[30] (Cyber Month) in Canada. This year's theme was "Generation Cyber Safe: Because online security knows no age[31]." The campaign encouraged Canadians from all walks of life to take simple, meaningful steps to protect themselves online. From likable videos to catchy jingles and cross-platform content, the campaign was a national conversation starter.

National partners from both private and public sectors helped to co-create and share content, and over 300 organizations used our Cyber Month content to connect to their audiences. We are proud of the reach and impact of this year's campaign. Over the course of Cyber Month, the campaign's content

- was seen over 293,000 times
- was shared by 410 unique social media accounts
- generated 26 million impressions and reached 3.8 million users
- generated 73,081 website visits, up from 63,338 in the previous year

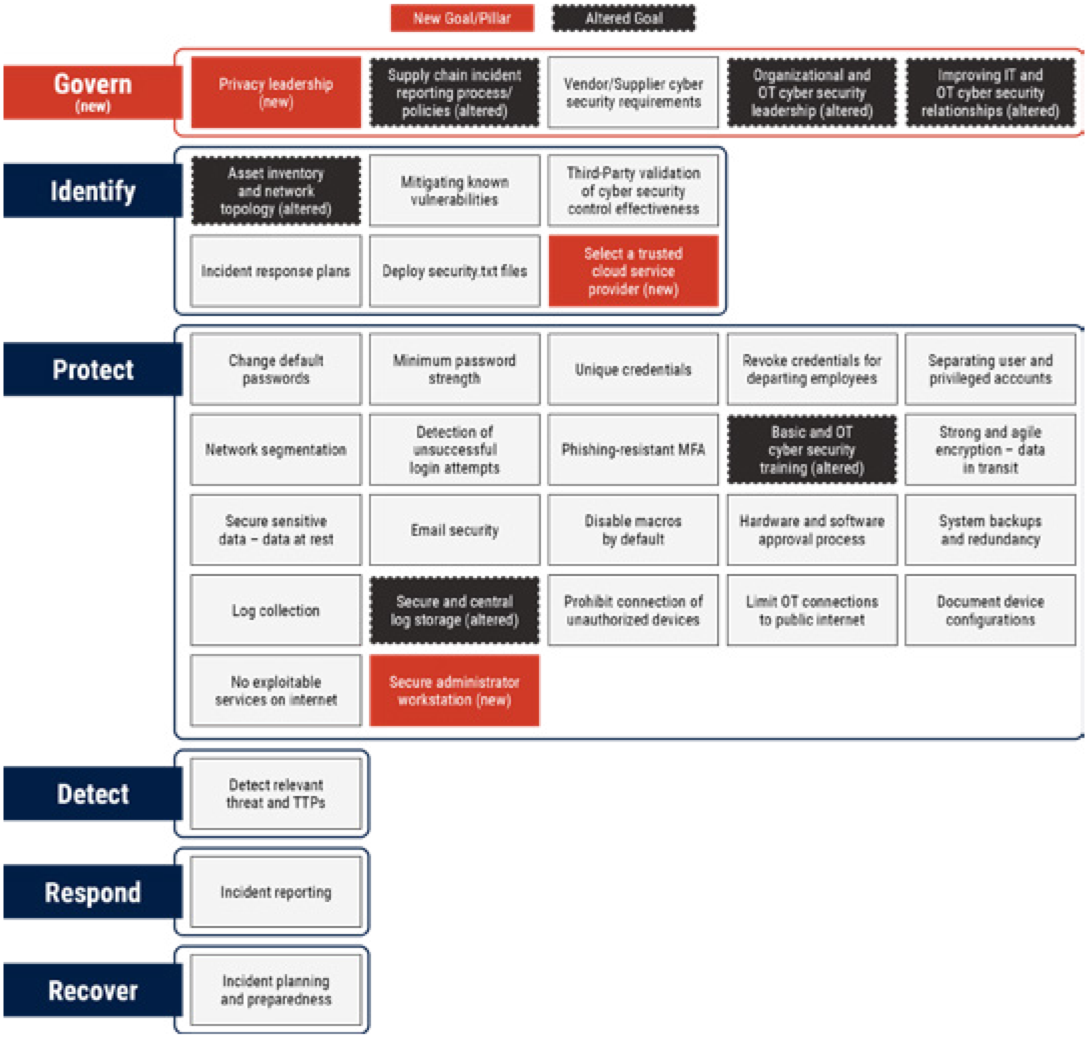
Cyber Readiness Goals

This year, we introduced the Cyber Security Readiness Goals (CRGs)[32], realistic and achievable goals to strengthen the cyber security of Canadian organizations, particularly critical infrastructure organizations.

The CRGs outline key objectives and important steps that organizations can take to improve the cyber security posture of both information technology and operational technology systems in the face of increasingly complex and evolving cyber security threats.

Composed of 36 foundational and voluntary goals, the CRGs consolidate baseline advice and guidance from the Cyber Centre on preventing, detecting and responding to cyber security threats.

The Cyber Centre has already delivered briefings on the CRGs to over 1,000 partners from a variety of key sectors, including energy, finance and transport.



New Goal/Pillar | Altered Goal

Govern (new)	Privacy leadership (new)	Supply chain incident reporting process/ policies (altered)	Vendor/Supplier cyber security requirements	Organizational and OT cyber security leadership (altered)	Improving IT and OT cyber security relationships (altered)
Identify	Asset inventory and network topology (altered)	Mitigating known vulnerabilities	Third-Party validation of cyber security control effectiveness		
	Incident response plans	Deploy security.txt files	Select a trusted cloud service provider (new)		
Protect	Change default passwords	Minimum password strength	Unique credentials	Revoke credentials for departing employees	Separating user and privileged accounts
	Network segmentation	Detection of unsuccessful login attempts	Phishing-resistant MFA	Basic and OT cyber security training (altered)	Strong and agile encryption – data in transit
	Secure sensitive data – data at rest	Email security	Disable macros by default	Hardware and software approval process	System backups and redundancy
	Log collection	Secure and central log storage (altered)	Prohibit connection of unauthorized devices	Limit OT connections to public internet	Document device configurations
	No exploitable services on internet	Secure administrator workstation (new)			
Detect	Detect relevant threat and TTPs				
Respond	Incident reporting				
Recover	Incident planning and preparedness				

Guidance publications

Another important service that CSE and the Cyber Centre provide to keep Canadians informed is publishing guidance on threats, mitigation techniques and more to our Cyber security guidance[33] webpage. These publications target a range of audiences, including the Canadian general public, IT practitioners, federal and provincial democratic institutions, private sector executives and allies.

We published 29 cyber security guidance publications this year, plus another 20 joint endorsement publications with our Five Eyes partners.

Edge devices

This year, the Cyber Centre released the guidance publication Security considerations for edge devices[34] as part of a Five Eyes guidance campaign. This was the first time that the Cyber Centre has written guidance jointly endorsed by its Five Eyes partners.

Expanding outreach activities

Although it might seem strange for an intelligence organization to actively pursue outreach and engagement, at CSE, we understand the value of working with the broader community. Cyber security is a team sport, and none of the work we do exists in a vacuum.

This year, CSE and the Cyber Centre remained dedicated to conducting community outreach activities, partnering and engaging with other government departments, and building strong relationships with the media.

Community outreach

Our growing community outreach program includes sponsoring not-for-profit programs, volunteer opportunities and in-school workshops for elementary and high school students to encourage the development of STEM skills and interest in STEM careers. The program aims to create opportunities in STEM for groups that may face barriers and that are underrepresented in the field. Some of the programs and events that we sponsored this year include:

- Hackergal
- CyberSci
- BlackBoys Code
- Raspberry Pi

This year, the Cyber Centre also hosted the CyberSci National Championships, which included 100 student participants. This was our third year sponsoring and coaching Team Canada, which won first place in the guest category at the European Cybersecurity Challenge 2024 for the third year in a row!

Promoting cyber security awareness among Indigenous communities

The Cyber Centre engages with Indigenous communities to enhance overall cyber security awareness and resilience. By promoting best practices, encouraging strong cyber hygiene and supporting local capacity building, these efforts help strengthen digital safety and support community-driven approaches to cyber security.

In March 2025, Manitoba First Nations SchoolNet hosted a Cyber Security Workshop in Churchill, Manitoba. The workshop brought together over 30 Indigenous youth aged 18 to 24, representing First Nations communities across the province. All participants were interns supporting their communities with IT, connectivity and digital initiatives.

The Cyber Centre delivered a hands-on session focused on cyber safety and awareness. This initiative aimed to equip youth with practical cyber security skills to strengthen digital resilience in their communities, while also advancing digital equity and connectivity across Manitoba's First Nations communities.

Engaging with the wider Government of Canada

Beyond operational engagement, we engaged with over 150 Government of Canada organizations this year to coordinate services and enhance cyber resilience across the federal landscape. This included:

- 25 one-on-one briefings with federal organizations
- bimonthly standing briefings open to all Government of Canada IT and cyber security teams and senior executives

The Cyber Centre launched a Government of Canada–wide Community of Interest call, establishing a platform for knowledge-sharing between the Cyber Centre and IT and cyber security professionals across the Government of Canada. This initiative supports government-wide cyber security strategies by providing insights on emerging cyber threats targeting the Government of Canada, sharing updates on key Cyber Centre initiatives, and highlighting critical programs that enhance the government's cyber security posture.

To increase awareness across the Government of Canada of its services, the Cyber Centre also published its first-ever brochure this year. The brochure was disseminated across the Government of Canada and included explanations of all the Cyber Centre can offer, as well as relevant contact information.

Cyber security briefing for Canadian journalists

This year, we were pleased to host a cyber security briefing for Canadian journalists. This unclassified, in-person briefing coincided with the publication of Mitigating cyber threats with limited resources: Guidance for civil society[35], a joint publication between CSE and international partners that warned the civil society sector about real and growing threats to their cyber security. Attendees represented a diverse group of accredited media organizations from across the country.

The briefing was not for news coverage. Instead, our intent was to provide attendees with useful information to improve their personal and professional cyber security. In total, 15 journalists attended the briefing, which was delivered in both official languages.

Montreal National Presence pilot project

In August 2024, the Cyber Centre opened an office in Montreal, its first office outside of the National Capital Region. We aim to work closely with local partners in cyber security and critical infrastructure within the Montreal region to deliver programs and services, cultivate relationships, and facilitate information exchange. In addition to promoting partnerships with critical infrastructure and other key stakeholders, this pilot project will allow us to assess the impact and benefit of further expanding CSE's national presence, including exploring the possibility of expanding to other locations in Canada.

CSE IS GROWING AND LEARNING

CSE takes a "talent in, talent up and talent augmentation" approach to strengthening our workforce, ensuring that employees get the support they need to succeed. To fulfill our mission and enable our work, we need a strong, diverse and healthy workforce. This year, CSE's total workforce grew to 3,841, a 5.9% increase from last year. This growth will help us to continue to deliver on our mission and provide critical intelligence and cyber security services to Canada.

Equity, diversity and inclusion and accessibility (EDIA) are central tenets to everything we do. Our world-class workforce is made up of engineers, data scientists, cyber security experts, intelligence analysts, policy advisors, project managers, counsellors, accountants, lawyers, communications professionals, human resources specialists, and everything in between. Our diversity—whether in our backgrounds, skills, talents or motivations—is our strength. We are proud of the various achievements we made this year to grow and learn as one inclusive CSE. Some key highlights include:

- embedding EDIA into performance assessments and merit-based promotion processes to signal that inclusivity is not just a value but a measurable priority for all employees
- creating a dedicated EDIA-focused division to underline our strategic approach to embedding EDIA in long-term planning and growth
- awarding over 5% of procurement contracts to Indigenous businesses in a proactive effort to advance economic reconciliation and Indigenous partnerships
- purchasing and displaying art from Indigenous artists so that our Indigenous employees feel more welcome within the walls of the organization and to share Indigenous culture with all CSE employees
- adopting features like name pronunciation tools in MS Teams to encourage respect and inclusivity in day-to-day interactions
- welcoming inspiring and diverse guest speakers to participate in various events and celebrations

Through these efforts, CSE is creating a truly inclusive environment to support our workforce in making impactful, innovative contributions to our mission.

CSE is a top employer

We think our organization, work environment and team are fantastic—and it turns out we aren't the only ones! This year, CSE was once again named one of Canada's Top Employers for Young People. We are proud to have received this recognition every year since 2017. This was also our 10th year being named a Top Employer in the National Capital Region.

Improving our hiring, recruitment and outreach activities

Our candidate outreach team travelled across Canada and participated in 178 events this year, including career fairs, hackathons, information sessions, conferences, webinars and networking events.

Among these outreach activities, 24% had a specific focus on EDIA and accounted for all 4 employment equity groups. We ensured that internal subject matter experts who represented these groups were included in these recruitment events. These efforts have led to an increasingly diverse workforce, with representation exceeding the workforce availability in 2 of the 4 designated groups (persons with a disability and Indigenous persons).

CSE also held 2 in-house recruitment events for women and non-binary university students enrolled in STEM programs across Canada.

Certified Inclusion Professional

This year, CSE hired a Certified Inclusion Professional who ensures that all external recruitment communications elements and materials are reviewed with a Gender-based Analysis Plus (GBA Plus) lens, promoting fairness and accessibility. This has also led to initiatives like dedicated parking for pregnant employees.

Indigenous Career Navigator

CSE was thrilled to welcome our first Indigenous Career Navigator this year. The Indigenous Career Navigator works with Indigenous employees and applicants to help them navigate their career paths and set and achieve professional goals. They also collaborate with managers to ensure Indigenous employees are considered in all hiring and staffing decisions, including promotions and mentorship opportunities.

Sponsorship program for racialized and Indigenous employees

In 2023, CSE launched a sponsorship program for racialized and Indigenous employees, which resulted in 90% of participants earning merit-based career-advancing development opportunities. This year, CSE relaunched the program and expanded it to include persons with disabilities.

The relaunched program has almost double the number of proteges of the original pilot program and welcomed proteges at all career stages. For example, 48% reported being at an early stage in their career and 26% said they were at a later stage. In terms of self-declaration,

- 15% self-identified as being neurodiverse or a person with a disability
- 11% self-identified as Indigenous
- 18% self-identified as Black
- 56% self-identified as racialized

Security program updates

Security is paramount to CSE operations, and our security processes and policies need to reflect our values and priorities. Over the past year, our security team has worked closely with internal partners to enhance the inclusivity and transparency of CSE's security processes, all while preserving the integrity of these processes. These consultations led to a number of encouraging results:

- The security interview process was updated to improve inclusivity
- The security screening questionnaire was reviewed through a GBA Plus lens to identify and remove potentially biased elements, ensuring equal access and fair treatment across all groups
- Job posters for security positions were reviewed, and our security teams were diversified to foster equitable hiring and break down systemic barriers

In addition, this year, CSE completed its participation in the NSIRA review of the polygraph program. CSE will continue to implement new and improved practices to strengthen the security process, ensuring it remains robust while safeguarding the privacy of all applicants.

Prioritizing inclusivity in everything we do

Diversity and inclusivity underpin every step of every process at CSE, from recruitment to policy development. CSE is committed to inclusive, representative and supportive actions in everything we do—our mission delivery depends on it. Diversity in all its forms helps us solve complex problems to protect Canada and Canadians.

Bilingualism and official languages

CSE takes great pride in being a workplace where people feel free to express themselves in the official language of their choice. Linguistic duality and bilingualism in the workplace remain priorities for CSE, and we are proud of our achievements this year, which include:

- developing new procedures for hosting events to ensure a parallel experience in both official languages
- investigating and experimenting with simultaneous translation capabilities for virtual and in-person events
- adding accents to names in Outlook and Teams
- taking proactive human resources measures to prepare for upcoming changes to the *Official Languages Act*

CSE's Réseau franco affinity group also began working with the Official Languages team to develop a vision and plan for official languages at CSE. Furthermore, our Centre of Expertise for Second Language Learning continued to provide a variety of tools and resources to help employees build skills and confidence in their second language.

Inclusivity in our external representation

CSE's passion for championing EDIA extends beyond the walls of our buildings. We worked hard this year to embed EDIA into every facet of our work, including our parliamentary appearances and participation in external events. For example:

- including pronouns and a land acknowledgement in opening remarks for parliamentary appearances
- building knowledge on parliamentary engagements and encouraging diverse members of CSE's leadership community to consider themselves as potential candidates for parliamentary appearances, resulting in many first-time appearances
- steadily increasing EDIA items in programs and agendas of major multilateral gatherings
- considering diversity of representation when selecting delegations for representation abroad
- opening new avenues for Five Eyes collaboration through the first Five Eyes EDIA Summit, which enabled us to leverage and share best practices at a partnership level and opened pathways to future knowledge exchange
- starting to embed EDIA best practices at an institution level in our Five Eyes partnerships through 2 EDIA-specific delegations

Gender-based Analysis Plus

GBA Plus has been transformative for CSE, shaping our organizational culture and enhancing our policies. GBA Plus training is mandatory for all staff, which has helped our entire workforce develop an understanding of how gender and intersectional factors like age, ethnicity and ability influence experiences and outcomes. This foundational knowledge has strengthened CSE's capacity to identify biases and barriers within our processes, ultimately leading to more inclusive practices.

Here are some of the ways that we integrated GBA Plus into our work this year:

- applying GBA Plus to our Treasury Board submissions, operational policies and the application of the Duty to Accommodate policy to promote inclusivity and address systemic barriers, creating policies that are both equitable and practical
- integrating GBA Plus into our Memoranda to Cabinet and decision-making processes to ensure that we consider the intersectionality and experiences of Canadians, fostering better mission outcomes
- embedding GBA Plus into our Code of Conduct to reinforce CSE's commitment to EDIA as central organizational principles

GBA Plus has become more than a tool at CSE; it's ingrained in our reflexes, enabling us to lead by example and strengthen our credibility and impact both internally and externally.

Lighthouse Award of Communications Excellence

CSE is very proud of the various members of our Communications teams who received the Lighthouse Award of Communications Excellence[36] for their outstanding work on "One CSE: The Collection." This was an organization-wide initiative that gamified EDIA principles. Over the course of a year, this initiative encouraged staff to take concrete actions that led to significant advancement of CSE's EDIA goals. Playing cards were used to represent EDIA actions, earning points for branches and promoting camaraderie. This initiative is one of many ways that CSE champions wellness in the workplace. We are constantly striving to foster a healthy, diverse and equitable environment.

Affinity groups

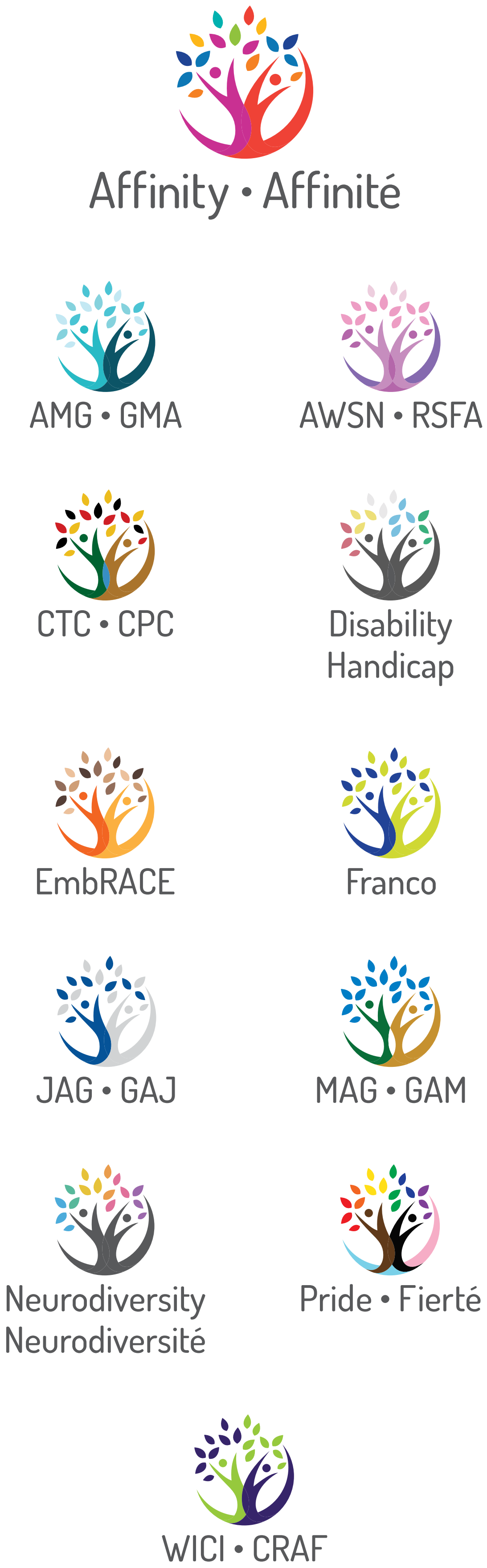
Affinity groups provide community support and help CSE advance workplace objectives and priorities by providing their perspectives and advocating for their needs. They also provide safe environments for a diverse workforce and create unique opportunities for teamwork and unity. Affinity groups often work together to collaboratively champion events and corporate initiatives. Affinity groups are invited to decision-making tables and their leaders deliver annual presentations to CSE executives on challenges, needs and progress. There are 11 affinity groups at CSE:

- Pride Network
- Women in Cyber Intelligence (WICI)
- Access Women's Support Network
- EmbRACE, including:
    - » Black Employee Circle
    - » Middle East and North Africa chapter
    - » Asian and South Asian Heritage
- Neurodiversity Group
- Disability Group
- Jewish Affinity Group
- Muslim Affinity Group
- Réseau franco
- Code Talkers Circle (Indigenous Heritage)
- Audible Minorities

Updated Values and Ethics Charter

This year, after a year of review and consultations across the organization, we launched the updated CSE Values and Ethics Charter. We wanted our charter to enable important CSE priorities like truth and reconciliation. We also wanted our charter to be more reflective of our diverse employees, our organizational culture, today's working environment and Canada's public service.

Learn more about our updated Values and Ethics charter in the following section, "CSE is transparent and accountable."



CSE IS TRANSPARENT AND ACCOUNTABLE

Because of the nature of CSE's mandate, much of our work must remain classified. But we recognize how important it is to share as much information with Canadians as possible. CSE is committed to being open, transparent and accountable. This includes participating in external reviews, monitoring and measuring internal compliance, responding to ATIP requests, conducting audits, and more.

Maintaining our commitment to transparency and accountability

As part of CSE's ongoing commitment to transparency and accountability, we are a full partner in the Government of Canada's open government plans and activities. We uploaded 5 datasets and 47 information assets to the Open Government Portal this year.

Ministerial authorizations

Under the *CSE Act*, certain activities must be authorized by the Minister of National Defence. There are different authorizations for the different aspects of CSE's mandate. Authorizations are valid for 1 year.

Before conducting any activities under a foreign intelligence authorization or cybersecurity authorization, CSE must receive approval from the Intelligence Commissioner[37]. This year, CSE submitted 8 authorizations to the Intelligence Commissioner and all were approved:

- 1 cybersecurity authorization to help protect federal institutions
- 4 cybersecurity authorizations to help protect non-federal institutions
- 3 foreign intelligence authorizations

The number of authorizations for foreign cyber[38] operations this year remained the same as last year. Authorizations are valid for 1 year and may include multiple operations or none.

- active cyber operation authorizations: 3
- defensive cyber operations authorizations: 1

Ministerial orders

The Minister of National Defence signs Ministerial Orders (MOs) to designate people or organizations with whom CSE can share information or provide tailored cyber security support. As of March 31, 2025, CSE had 5 MOs in effect. These MOs designate:

- recipients of Canadian identifying information 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

No new MOs were issued this year and no existing MOs were amended.

External review

Like any federal government department, CSE's activities are subject to review by federal review bodies such as the Privacy Commissioner and the Auditor General. These external review bodies verify, on behalf of Canadians, that CSE's activities comply with the law. CSE supports these independent reviews as they are key to ensuring transparency and accountability in our important work. We value their insights and use them to improve our processes.

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

This year, to increase transparency, CSE began publishing its responses to review body recommendations[39] on our website. We published responses to recommendations from 3 NSIRA review reports this year.

Supporting external reviews into foreign interference

Of the 25 external reviews CSE supported this year, 3 were reviews into foreign interference in Canada's federal elections. These reviews were conducted by NSIRA, NSICOP and the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions.

CSE facilitated the finalization and publication of the following reports on foreign interference, which were tabled in Parliament:

- NSIRA's Review of the dissemination of intelligence on People's Republic of China political interference, 2018-2023[40]
- NSICOP's Special Report on Foreign Interference in Canada's Democratic Processes and Institutions[41]

Internal compliance

CSE's compliance team conducts a range of monitoring activities to ensure compliance with internal policies. All of CSE's internal compliance findings and assessments are available for review by external review bodies.

This year's statistics include a new category: compliance incidents that do not involve information related to Canadians. This allows for enhanced tracking and analysis of all CSE operational compliance incidents. In 2024, CSE's compliance team identified:

- 22 operational compliance incidents that did not involve information related to Canadians
- 119 operational compliance incidents that involved information related to Canadians

Example of an operational incident and its mitigation

All operational incidents are triaged, assessed and appropriate mitigations are put in place. Some incidents require additional briefings to CSE executives or even to the Minister. For example, this year, we notified the Minister of an incident where CSE improperly shared information. CSE identified an activity where, between 2020 and 2023, we shared some information with international partners without properly removing Canadian information that had been acquired incidentally when targeting valid foreign intelligence targets. Although the information remained safeguarded, this activity did not meet CSE's policy requirements.

CSE acted quickly to contain the issue. Corrective actions included placing strict limits on information sharing and seeking assurances from CSE's trusted partners that the shared information was deleted. We continue to update our policies and procedures to prevent reoccurrence.

The incident did not constitute a material privacy breach that would otherwise be reported in CSE's Annual Report to Parliament on the Administration of the *Privacy Act*[42]. However, we proactively reported the incident to our oversight and review bodies, including the Office of the Privacy Commissioner, and kept these bodies informed of the results of our internal investigations.

Complaints

This year, CSE received 3 external complaints directed to the Chief of CSE and responded to 1 complaint sent to NSIRA regarding CSE activities.

CSE also responded to findings and recommendations from NSIRA's investigation into a complaint involving CSE's recruitment and security process. NSIRA's report concluded that all allegations were unfounded, with the exception of 1 which was partially founded. CSE remains committed to continuous improvement and is addressing NSIRA's recommendations.

Audit and evaluation

CSE's audit and evaluation teams provide impartial, evidence-based advice and services directly to senior leadership to help CSE achieve its strategic objectives.

This year, CSE completed 2 audits and 3 program evaluations to improve the effectiveness and efficiency of our operational activities. Audit and evaluation functions are subject to reviews themselves, and this year the teams underwent a successful external review and neutral assessment.

Our audit and evaluation program is supported by CSE's Departmental Audit Committee (DAC), which provides advice and strategic direction. Through its advisory role, the DAC offers an unbiased, professional and independent perspective while remaining informed, relevant and trusted by the Chief and other levels of senior management.

Cyber security audit program

Since 2018, CSE has provided a collection of free tools[43] for auditors to assess their organizations' cyber security status. To date, we have received over 200 requests for these tools from auditors across the Government of Canada and the private sector.

Innovation in auditing at CSE

At the 2024 National Conference of the Institute of Internal Auditors Canada, CSE's audit and evaluation team was pleased to present an innovative tool for auditing cloud security. The team will continue to publish guidance for auditors within and external to the Government of Canada.

Values and ethics

The updates to CSE's Values and Ethics Charter reflect requests that we received from employees for more clarity on their obligations and for a charter that better reflects the core public service value "Respect for People."

Respect is now one of CSE's 6 organizational values, emphasizing our prioritization of accessibility, anti-racism, equity, inclusion and reconciliation. The updated charter includes actionable principles to guide employees in their daily activities and interactions.

In combination with CSE's new Code of Conduct—which expands upon the charter to outline specific expectations for behaviour—CSE employees now have a modern and comprehensive blueprint to help them conduct their duties ethically and responsibly as representatives of CSE and the Government of Canada.

CSE also established an annual Confidential Report process this year. All employees are required to complete conflict of interest attestations yearly. This will increase individual accountability and adherence to the charter.

Over the next year, CSE's Ethics Office will continue to update its scenario-based ethics training and provide guidance on topics such as conflict of interest, personal social media use, non-partisanship and the use of AI.

Supporting the Public Inquiry on Foreign Interference

In January 2025, the Final Report on the Public Inquiry into Foreign Interference[44] was released. This inquiry examined interference by foreign states or non-state actors and assessed federal entities' capacity to protect Canada's democratic processes. The report identifies 51 recommendations. CSE, in coordination with the Government of Canada, is carefully reviewing the findings and recommendations and will take appropriate actions.

CSE was pleased to cooperate with and support this inquiry. CSE collaborated with PCO and CSIS to set up teams in Montreal, Toronto and Ottawa with secure network connections and equipment for the inquiry.

Furthermore, CSE produced over 85,000 documents in support of the Commission and provided access to senior management, including our Chief, in both public and in-camera appearances to support the effort.

Endnotes

[1] https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html#h-1170321

[2] https://www.canada.ca/en/privy-council/services/publications/canada-intelligence-priorities.html

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

[4] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

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

[6] https://www.cyber.gc.ca/en/guidance/cyber-supply-chain-security-small-medium-sized-organizations-itsap00070

[7] https://www.cyber.gc.ca/en/news-events/joint-guidance-choosing-secure-and-verifiable-technologies

[8] https://www.cyber.gc.ca/en/tools-services/secure-communications-solutions#trusted

[9] https://portal-portail.cyber.gc.ca/en

[10] https://www.cyber.gc.ca/en/glossary#c

[11] https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm

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

[13] https://www.cse-cst.gc.ca/en/mission/research-cse/tutte-institute-mathematics-computing

[14] https://www.cse-cst.gc.ca/en/mission/research-cse/vulnerability-research-centre

[15] https://www.cyber.gc.ca/en/geekweek

[16] https://www.cyber.gc.ca/en/geekweek/geekweek-9

[17] https://www.cse-cst.gc.ca/en/cse-nserc-research-communities-grants

[18] https://www.cyber.gc.ca/en/education-community/learning-hub

[19] https://www.getcybersafe.gc.ca/en/resources/your-love-language-can-help-you-get-cyber-safe

[20] https://www.getcybersafe.gc.ca/en/blogs/scam-tactics-watch-out-valentines-day

[21] https://www.getcybersafe.gc.ca/en/blogs/e-transfer-fraud-protect-your-online-transactions

[22] https://www.getcybersafe.gc.ca/en/payment-methods

[23] https://www.getcybersafe.gc.ca/en/resources/video-spam-7726

[24] https://www.getcybersafe.gc.ca/en/next-generation-spotting-content-created-with-artificial-intelligence

[25] https://www.getcybersafe.gc.ca/en/resources/recognize-artificial-intelligence-ai-9-ways-spot-ai-content-online

[26] https://www.getcybersafe.gc.ca/en/blogs/cyber-criminals-are-using-artificial-intelligence-ai-online-threats

[27] https://www.getcybersafe.gc.ca/en/blogs/why-you-should-never-give-your-personal-information-ai

[28] https://indigenous.link/cse-cybersafe/

[29] http://www.getcybersafe.ca/business

[30] https://www.getcybersafe.gc.ca/en/cyber-security-awareness-month

[31] https://www.getcybersafe.gc.ca/en/resources/be-part-generation-cyber-safe

[32] https://www.cyber.gc.ca/en/cyber-security-readiness/cyber-security-readiness-goals-securing-our-most-critical-systems

[33] https://www.cyber.gc.ca/en/guidance

[34] https://www.cyber.gc.ca/en/guidance/security-considerations-edge-devices-itsm80101

[35] https://www.cyber.gc.ca/en/news-events/mitigating-cyber-threats-with-limited-resources-guidance-civil-society

[36] https://www.canada.ca/en/government/system/government-communications/communications-community-office/communications-awards-excellence/team-awards.html#t4

[37] https://www.canada.ca/en/intelligence-commissioner.html

[38] https://www.cse-cst.gc.ca/en/mission/cyber-operations

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

[40] https://nsira-ossnr.gc.ca/en/reviews/our-reviews/review-of-the-dissemination-of-intelligence-on-peoples-republic-of-china-political-foreign-interference-2018-2023/report/

[41] https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf

[42] https://www.cse-cst.gc.ca/en/accountability/transparency/reports#par

[43] https://www.cyber.gc.ca/en/tools-services/cyber-security-audit-program

[44] https://foreigninterferencecommission.ca/reports/final-report

Canada