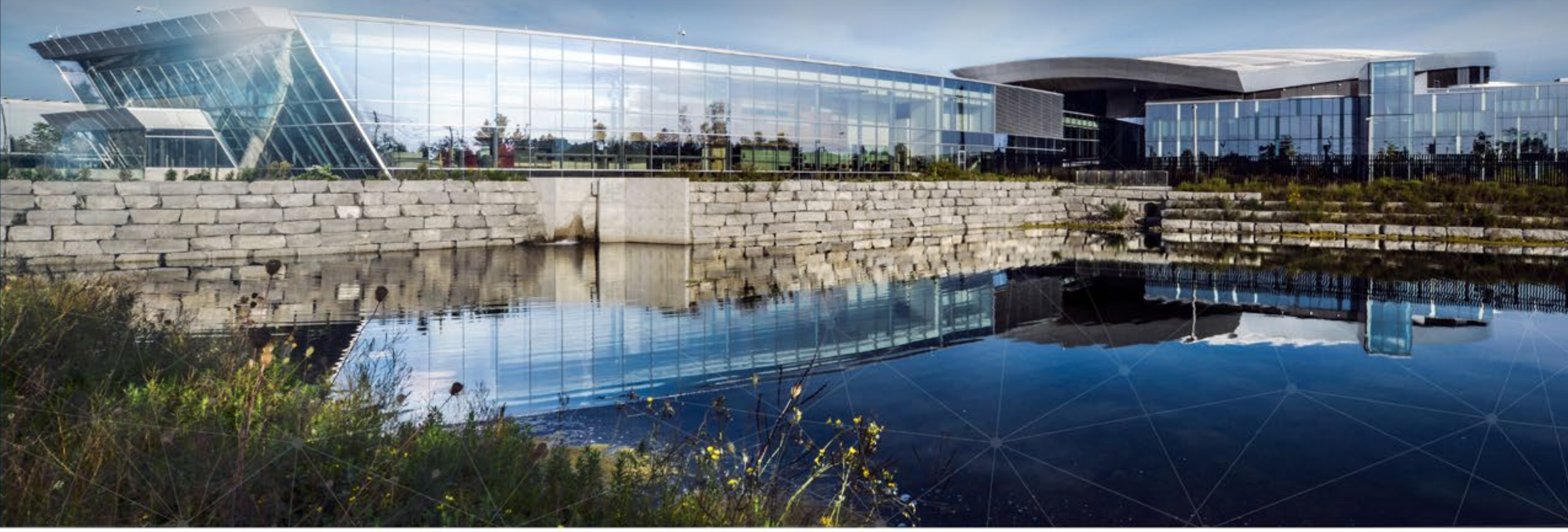
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

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

Communications Security Establishment

ANNUAL REPORT 2023 2024



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

About CSE	2
Minister’s foreword	3
Message from the Chief	4
Foreign signals intelligence	6
Supporting the Canadian Armed Forces	7
24/7 operational response	8
Technical and operational assistance	8
How we share intelligence	9
Cyber security	10
Russia’s invasion of Ukraine	20
Hostile state activity and foreign interference	21
Counter terrorism	26
The Arctic	27
Canada’s Indo-Pacific Strategy	29
Foreign cyber operations	31
Cybercrime	32
Communications security	35
Empowering Canadians	36
Innovation	40
Artificial intelligence	45
Accountability	50
People	55
Key numbers	65
Endnotes	66

About CSE

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 the federal government's operational and technical lead for cyber security.

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

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

CSE is part of the Five Eyes, the world's longest-standing and closest intelligence-sharing alliance. The Five Eyes includes the signals intelligence and cyber security agencies of Canada, Australia, New Zealand, the United Kingdom (UK) and the United States (U.S.).

CSE has a workforce of 3,529 full-time, permanent employees. Our total authorities for 2023 to 2024 were just over $1 billion.[2]

This report is an unclassified summary of CSE's activities from April 1, 2023, to March 31, 2024. Unless otherwise stated, "this year" refers to the 2023 to 2024 fiscal year.

Minister's foreword

Canada is facing new and evolving security threats, including climate change and its impacts on the Arctic, cybercrime, violent extremism, and threats from Russia, China, and other nation states to the international rules that keep us all safe. But the work CSE is doing across all aspects of its mandate plays a significant role in protecting Canada from these threats now and into the future.

We are pleased to present this annual report, which details CSE's record of success in combating cybercrime and the emerging threats facing Canada and the world. The report highlights to Canadians what CSE has done over the past year. Reports like these are vital for an open and accountable government and help build public faith in our institutions.

In April 2024, the Prime Minister and I released Canada's new defence policy—Our North, Strong and Free: A Renewed Vision for Canada's Defence. It included major investments for CSE to support foreign cyber operations and foreign intelligence collection capabilities. Accounted for in Budget 2024, these include $917 million over the next 5 years, expanding to $2.83 billion over 20 years.

These proposed investments reflect that CSE's mandate will be key to countering the evolving threats Canada faces. CSE has an exemplary track record of delivering outcomes that help to safeguard Canada's national security, economic prosperity, democratic values, and the safety of Canadians. These investments will help bolster CSE's work, so it can continue to keep Canada safe.

CSE is made up of dedicated public servants who will continue to deliver on the agency's mission and work tirelessly to protect Canadians.

Hon. Bill Blair, PC, COM, MP
Minister of National Defence

Message from the Chief

Reading through this report, it's hard to believe how much has happened in just one year. I am impressed every day by the hard work and ingenuity that CSE employees bring to our mission, but seeing it all in one place is a testament to what I see and witness on a daily basis.

This report doesn't even tell the whole story because not everything we do can be shared in a public report, but that doesn't mean we operate without oversight or external review. What we can and cannot do is laid out very clearly in the *CSE Act*, and our external review bodies are there to scrutinize our work on behalf of Canadians.

In fact, what we do has never been under more scrutiny, especially in the context of the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions. CSE welcomes the fact that foreign interference is being taken so seriously. This is something we have been warning about publicly since 2017 and most recently in our latest report Cyber Threats to Canada's Democratic Process: 2023 update.[3] As that report shows, artificial intelligence is poised to take the threat to the next level due to its potential for spreading disinformation and distrust. The Hostile state activity and foreign interference chapter in this report outlines the work CSE is doing to counter these threats but overcoming them will take sustained effort across the whole of government and the whole of society.

While there is plenty of cause for concern, CSE has achieved some notable successes this year. We contributed to the fight against cybercrime by conducting our first ever defensive cyber operation, and a series of active cyber operations helped to tackle cybercrime at the roots. Meanwhile, CSE's Cyber Centre gave early warnings about potential ransomware compromises to over 250 Canadian organizations, before any damage was done. The number of critical infrastructure organizations engaging with us has grown and the majority of federal institutions, including Crown corporations, now have at least one of our sensors to help detect cyber threats.

These are just some of the many examples you'll find throughout the report that showcase the ways we've delivered on our mission consistently and effectively this year. However, there is always more to do. CSE continues to innovate through new partnerships and new technologies to meet the growing demands of today and tomorrow.

Above all, it is CSE's people who make these outcomes possible. As the People chapter shows, this is an organization that aims to put its employees first. We do this not just because it's the right thing to do or because it makes coming to work more enjoyable (though both are true), but because **that** is how you achieve extraordinary results.

CSE is changing quickly. Our workforce has grown significantly in the past year and the investments announced in Canada's new defence policy and Budget 2024 will see us grow even more. As we navigate these changes, we will continue to work towards making CSE a workplace where everyone feels valued, respected and empowered.

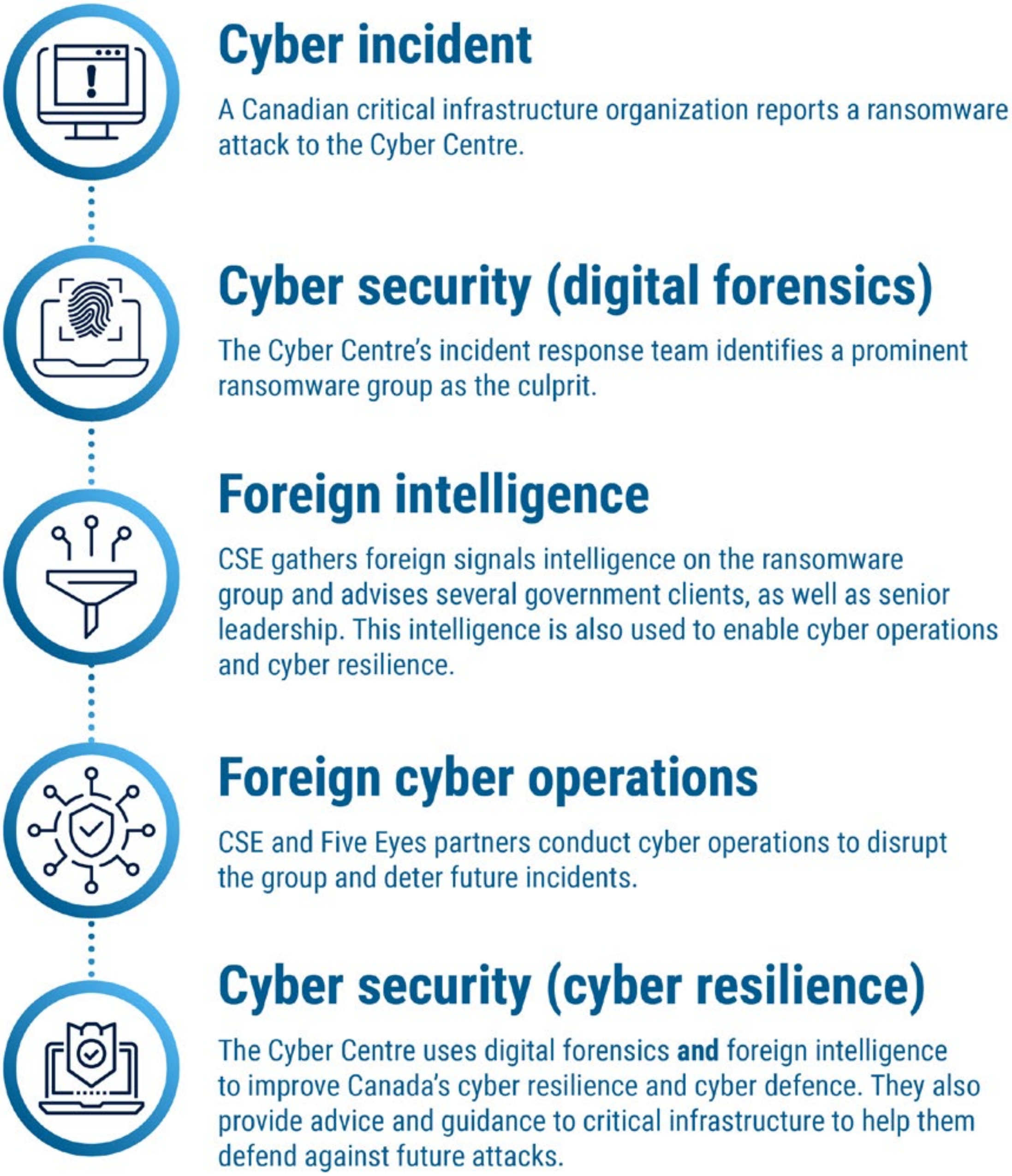
In this rapidly evolving threat environment, CSE's work has never been more important. Canada has put its trust in us to bring our best, and I can confidently say that we are more prepared than ever before to rise to the challenge.

Caroline Xavier (she/her)
Chief, CSE

How the parts of CSE’s mandate work together

CSE’s cyber security, foreign intelligence and cyber operations mandates work together to achieve a range of outcomes that benefit Canadians. Having one agency to carry out this full mandate provides CSE and Canada with unique advantages.

The following example is based on a past cyber operation in CSE’s ongoing campaign against cybercrime.



Cyber incident

A Canadian critical infrastructure organization reports a ransomware attack to the Cyber Centre.

Cyber security (digital forensics)

The Cyber Centre’s incident response team identifies a prominent ransomware group as the culprit.

Foreign intelligence

CSE gathers foreign signals intelligence on the ransomware group and advises several government clients, as well as senior leadership. This intelligence is also used to enable cyber operations and cyber resilience.

Foreign cyber operations

CSE and Five Eyes partners conduct cyber operations to disrupt the group and deter future incidents.

Cyber security (cyber resilience)

The Cyber Centre uses digital forensics **and** foreign intelligence to improve Canada’s cyber resilience and cyber defence. They also provide advice and guidance to critical infrastructure to help them defend against future attacks.

Foreign signals intelligence

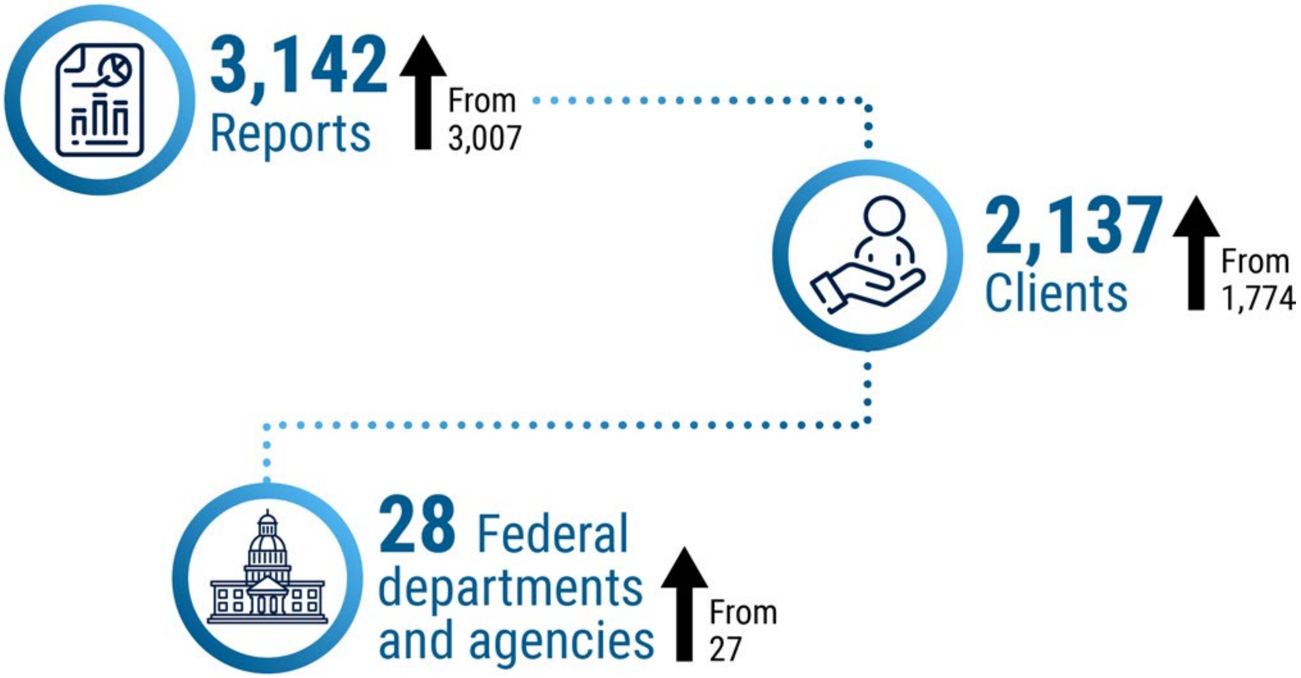
CSE collects foreign signals intelligence (or SIGINT) to provide the Government of Canada with information about foreign-based threats. SIGINT can include any kind of electronic communication, from text messages to satellite signals. Under the *CSE Act*, CSE's foreign intelligence collection activities must not target Canadians or anyone in Canada.

Foreign intelligence priorities

This year, CSE provided foreign intelligence reports in response to Government of Canada priorities, including:

- hostile state activity, including:
  - → disinformation
  - → espionage
  - → foreign interference and malign influence
  - → counter intelligence
  - → intellectual property theft
  - → cyber threat activity
- terrorism and violent extremism
- cybercrime
- Russia's invasion of Ukraine
- People's Republic of China (PRC) and Indo-Pacific regional stability
- Israel-Hamas war
- instability in Haiti
- Arctic sovereignty
- support to Canadian Armed Forces (CAF) operations
- kidnappings of Canadians abroad
- threats to Canadians abroad
- urgent and emerging world events

CSE foreign intelligence reporting in 2023 to 2024



3,142 Reports ↑ From 3,007

2,137 Clients ↑ From 1,774

28 Federal departments and agencies ↑ From 27

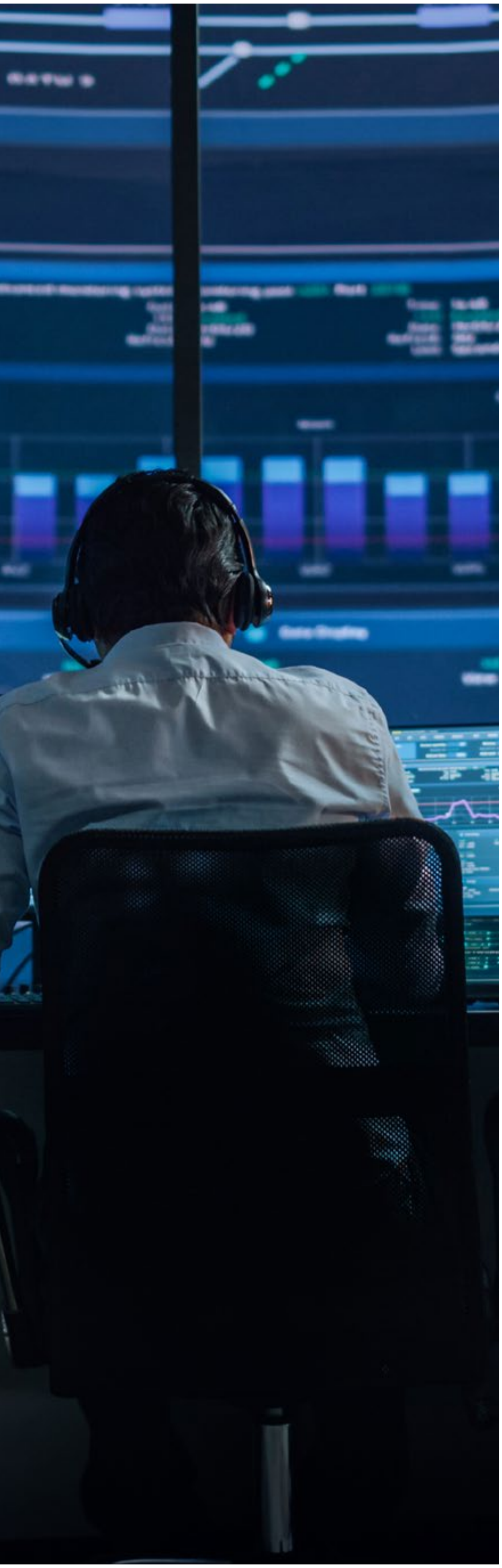
Supporting the Canadian Armed Forces

The CAF is one of CSE's most important federal partners. CSE's support to the CAF includes:

- signals intelligence
- communications security
- cyber security
- assistance with and collaboration on foreign cyber operations
- linguistic support

This year, CSE worked closely with the CAF to support activities including:

- protecting CAF missions abroad
- defending Canada's Arctic sovereignty
- supporting North American Continental defence
- delivering against the CAF's intelligence requirements including those related to the conflict in Ukraine (Operations Unifier and Reassurance)
- enabling Special Forces operations
- supporting deployed CAF operations such as the assisted departure of Canadians abroad



24/7 operational response

CSE is a 24/7 agency. When crisis situations arise that pose a threat to Canada or Canadians abroad, CSE stands ready to meet the Government of Canada's urgent needs in accordance with our mandate.

CSE's Operational Production and Coordination Centre (COPCC) works around the clock to coordinate CSE's efforts in response to critical cyber incidents and international crises. This year, COPCC provided senior decision makers with timely information about multiple global events impacting Canada (see foreign intelligence priorities). COPCC also worked with Global Affairs Canada (GAC) and the CAF to support the evacuation of Canadians from Sudan and Israel.

Ever vigilant, COPCC stands watch to ensure CSE is able to provide the Government of Canada with the information it needs when it matters most.

Technical and operational assistance

CSE's mandate allows CSE to assist federal security, law enforcement and defence partners at their request and under their legal authorities.

In 2023 to 2024, CSE received 45 requests for technical and operational assistance from federal partners and provided assistance in 43 of those cases.

Requests for assistance numbers

- 2023 to 2024
  → Received: 45
  → Approved: 43
- 2022 to 2023
  → Received: 62
  → Approved: 59

How we share intelligence

CSE intelligence reports can only be read by authorized users across the Government of Canada and the Five Eyes. CSE has robust mechanisms in place to make sure this highly sensitive information gets where it needs to go without falling into the wrong hands.

Electronic dissemination

CSE runs Canada's Top Secret Network (CTSN). This is a secure IT network used to collaborate and communicate at the Top Secret level. For example, CTSN enables clients across the Government of Canada and the Five Eyes to access CSE's intelligence reporting. It also supports Top Secret voice and video calls.

Authorized clients can view CSE and Five Eyes intelligence reports by logging into CTSN to access CSE's reporting database. The reports do not leave the database, and the system will not allow clients to copy, save or send reports to others. It logs and tracks information such as who reads each report and when.

Client relations officers

Client relations officers (CROs) are CSE employees embedded across the Government of Canada. They deliver hard copies of CSE intelligence reports to authorized users, such as Cabinet ministers and senior officials. CROs are responsible for tracking readership and destroying any hard copies of intelligence reports.

SIGINT dissemination officers

SIGINT dissemination officers (SDOs) are employees of other Government of Canada departments who have access to the reporting database through CTSN. They are accredited by CSE to share foreign intelligence reports with authorized clients within their own departments. SDOs use the same tools as CSE CROs to track and log readership.

Improvements

In May 2023, the report by the Right Honourable David Johnston, Independent Special Rapporteur on Foreign Interference[4] called for better tracking of intelligence reporting within the Government of Canada. In response, the security and intelligence community made various changes to the way classified products are disseminated. CSE's efforts included:

- increasing the number of CROs and SDOs to support additional senior officials
- supporting Deputy Ministers and Cabinet ministers in new forums for intelligence sharing and awareness
- expanding access to CSE's electronic dissemination system to the broader security and intelligence community, allowing for greater tracking and logging

Major updates to Canada's Top Secret Network

This fiscal year, CSE carried out a complete overhaul of CTSN, improving its security, capacity and reliability. New features include high-definition video and end-to-end encryption. The refresh also allowed CSE to start consolidating several functions that used to exist both on CTSN and on CSE's in-house network, reducing duplication and saving on costs.

Cyber security

The Cyber Centre is Canada's technical and operational authority on cyber security. As part of CSE, it provides leading-edge advice and services to help prevent cyber incidents and keep critical services up and running.

The Cyber Centre's mandate covers federal institutions and systems of importance, which include critical infrastructure. Under the *CSE Act*, the Cyber Centre can also assist any other entity designated by the Minister of National Defence as being of importance to the Government of Canada. Examples this year include providing cyber defence services to the territories (see Securing the North) and cyber security assistance to Ukraine and Latvia (see Cyber security assistance to Ukraine and Latvia).

Federal institutions

The Cyber Centre works with Shared Services Canada, the Treasury Board of Canada Secretariat and other federal partners to protect the IT assets of the Government of Canada. The Cyber Centre also works on an opt-in basis with Crown corporations and other federal institutions outside the core network.

Sensors

Sensors are software tools that can detect malicious cyber activity on devices, at the network perimeter and in the cloud. They are one of the Cyber Centre's most important tools for defending Government of Canada networks.

The Cyber Centre uses machine learning (ML) to help detect anomalies in the sensor data and block suspicious or malicious activity automatically.

This year, the Cyber Centre blocked an average of 6.6 billion potentially malicious actions a day ranging from routine scans to sophisticated intrusion attempts.

The number of federal institutions covered by the Cyber Centre's sensor program continued to grow this year. This included an increase in the number of Crown corporations and small departments and agencies opting in voluntarily.

The Cyber Centre has also deployed sensors to help protect the cyber systems of a small number of high-priority non-federal institutions. This year, it began the process of deploying sensors on Northwest Territories, Nunavut and Yukon government systems (see Securing the North).

Sensor deployments as of March 2024

- Host-based sensors (HBS): 102 federal institutions (up from 85)
- Cloud-based sensors (CBS): 80 federal institutions (up from 72)
- Network-based sensors (NBS): 84 federal institutions benefit from our sensor deployed at the network perimeter (no change)
- Virtual network-based sensors: 5 federal institutions (no change)

Sensor deployments by institution type

The number of institutions with at least 1 sensor as of March 2024 was as follows:

- 167 out of 217 federal institutions, including:
  - → 23 out of 46 Crown corporations (up from 11 in 2023)
  - → 42 out of 43 small departments and agencies (up from 26 in 2023)[5]
- 4 non-federal institutions

Sensor program at a glance

900,000
Devices

167
Federal institutions and Crown corporations

6.6 BILLION
Blocks a day

Protecting Government of Canada mobile devices

This year, the Cyber Centre added a new capability to improve the cyber security of Government of Canada mobile devices. The Cyber Centre established a secure connection to retrieve cyber security data from Government of Canada mobile device management (MDM) servers. The Cyber Centre runs the data through various threat intelligence and analytical models to detect vulnerabilities and patterns of cyber threat activity on government-issued handsets. The Cyber Centre reports its findings to the MDM operators who can use it to mitigate threats. For example, they might issue updates or remove prohibited applications.

Critical infrastructure

This year, the Cyber Centre engaged with almost 1,900 Canadian critical infrastructure (CI) organizations to increase Canada's cyber resilience across all sectors.

Critical infrastructure organizations are considered systems of importance because they are essential for Canada to function. Key sectors include:

- democratic institutions
- education
- energy
- finance
- food
- health
- information and communications technology
- manufacturing
- municipal, provincial, territorial and Indigenous governments
- transportation
- water

Energy sector

This year, the Cyber Centre put added emphasis on working with Canada's energy sector to improve its cyber resilience.

In June 2023, the Cyber Centre published an assessment of the cyber threat to Canada's oil and gas sector.[6] The report identifies ransomware as the main threat to Canada's oil and gas supply while assessing that state-sponsored cyber activity targeting this sector is very likely to continue. This includes both cyberespionage and pre-positioning activities to be able to deploy destructive cyber attacks against Canada's oil and gas infrastructure.

In tandem with the release of the report, CSE held classified briefings at secure facilities across Canada to give oil and gas sector executives additional information that is too sensitive to share publicly. CSE took this unprecedented step because of the importance of this sector to Canada's national security.

Over the course of the year, the Cyber Centre signed up 3 more partners in the oil and gas sector to subscription services such as cyber security notifications and the Cyber Centre's automated threat data feed.

The Blue Flame Program,[7] in partnership with the Canadian Gas Association (CGA), doubled its membership from 4 organizations to 8. In July 2023, the Cyber Centre hosted a workshop with the CGA to identify ways to improve information sharing and to enhance the services available to Blue Flame members.

This year, the Cyber Centre became a government member of the newly formed Energy Security Technical Advisory Committee.[8] This information sharing and collaboration group was spearheaded by the CGA and brings industry and Government of Canada partners together to enhance the sector's cyber security maturity.

> **It is difficult to overstate the importance of the oil and gas sector to national security.**
>
> - Canadian Centre for Cyber Security, The cyber threat to Canada's oil and gas sector

Provinces and territories

Increasing cyber security collaboration with the provinces and territories was a high priority for the Cyber Centre this year (see also Securing the North).

In May 2023, the Cyber Centre hosted its first cyber security round table devoted solely to collaboration between federal, provincial and territorial cyber security leads. The 2-day agenda focused on how the Cyber Centre could best support the provinces and territories in terms of cyber defence services, incident response support and building cyber resilience.

Based on feedback from the round table, in November 2023, the Cyber Centre rolled out secure communications capabilities to senior provincial and territorial officials. This end-to-end encrypted platform allows for secure communications with Cyber Centre senior leaders in the event of a cyber incident.

Defence contractors

In June 2023, the Government of Canada announced a new cyber security certification program to protect Canada's defence supply chain.[9] To win government defence procurement contracts, companies will need to prove their cyber security posture meets defined standards. The program aligns with U.S. requirements, meaning companies doing business in both countries only need to be certified once.

In August 2023, the Cyber Centre stood up a new team to help Canadian defence contractors prepare for the new technical requirements.

Briefings and engagements

This year, Cyber Centre experts continued to share actionable cyber security information with critical infrastructure partners across all sectors through:

- 23 cyber threat briefings
- 7 Walk-the-Talk sessions on topics including
  - → cybercrime
  - → supply chain threats
  - → secure artificial intelligence (AI) development
- around 230 speaking engagements

Tools and services

The Cyber Centre shares tools and services to help cyber defenders do their jobs. Some are available only to government and critical infrastructure partners. Others are publicly available.

Automated threat data feed

The Cyber Centre continued to share cyber threat data through its automated threat intelligence feed, Aventail. This year, Aventail shared over 30,700 unique indicators of compromise to help organizations find malicious activity on their networks. That's around 84 per day.

- March 2024
  - → Total organizations with Aventail: 230
    - Federal institutions: 57
    - Critical infrastructure: 173
- March 2023
  - → Total organizations with Aventail: 152
    - Federal institutions: 20
    - Critical infrastructure: 132

Malware analysis

Partners can submit suspicious files to Assemblyline,[10] the Cyber Centre's malware detection and analysis platform. It will tell them quickly if a file is malicious and will recommend specific mitigations for the type of malware. This is especially helpful in the case of suspected phishing emails or during the response to a cyber incident.

Assemblyline uses ML (a subset of AI) to help power its analytics. As of February 2024, Assemblyline added several optional functions powered by large language models (a subset of generative AI).

Users now have the option to:

- create an executive summary of the malware analysis
- generate a printable report with more detailed analysis
- analyze sections of code and explain what the malware does
- interact with an AI chatbot to navigate Assemblyline and ask follow-up questions

This year Assemblyline scanned over 1 billion suspicious files. The number of organizations using the service grew by 35%.

- March 2024
  - → Total partners: 308
    - Government of Canada: 58
    - Critical infrastructure: 250
- March 2023
  - → Total partners: 228
    - Government of Canada: 45
    - Critical infrastructure: 183

Security posture dashboard

ObservationDeck is an interactive dashboard that allows Government of Canada departments to see potential vulnerabilities on their IT assets. It combines information from the Cyber Centre's sensors with open-source data to highlight potential risk factors and attack vectors.

This year, the number of Government of Canada departments using ObservationDeck grew from 57 to 70.

Alert triage platform

This year, the Cyber Centre developed Howler, a new platform for Security Operations Centre (SOC) teams. The platform was released publicly in April 2024. Howler is an alert triage platform, meaning it helps analysts to sort and filter large quantities of cyber alerts. These alerts are generated in vast numbers by automated threat detection systems. Howler allows triage analysts to:

- automate repetitive tasks
- filter out known scenarios
- reduce false alerts
- customize the information they receive

All of this helps analysts to identify and respond more quickly to cyber incidents.

Learn more about Howler.[11]

Threat detection pilot

The Cyber Centre is exploring ways to help critical infrastructure organizations improve their own cyber threat detection capabilities. This year, the Cyber Centre worked with a partner in the energy sector on a pilot project called SLAM (Security Logs Analysis and Monitoring).

Like a tailoring service, the Cyber Centre calibrated the partner's generic threat detection analytics to better fit their specific operating environment. The initial results suggest this approach has the potential to reduce the number of false positives and the alert fatigue that can stem from them. The Cyber Centre is conducting a comprehensive analysis of the pilot. The results will inform future cyber security offerings to critical infrastructure partners.

Cyber security notifications

The Cyber Centre continued to notify the cyber security community about potential issues throughout the year. Different notifications are used for different situations. Each type gives technical details and guidance for system owners to mitigate the threat.

Advisories and alerts

The Cyber Centre publishes advisories and alerts on its website and social media channels. Advisories are used for routine cyber security issues while alerts concern urgent or high-risk threats.

Cyber flashes

Cyber flashes are alerts that cannot be shared publicly because they contain sensitive information. They are shared directly with Cyber Centre partners.

Priority notifications

Priority notifications are sent directly to partners who have subscribed to the Cyber Centre's National Cyber Threat Notification Service (NCTNS). This service analyzes multiple threat feeds for references to assets identified by subscribers. NCTNS may send priority notifications in tandem with alerts or cyber flashes to let partners know that their networks are exposed.

Scorecards

Scorecards offer a monthly summary of a partner's NCTNS data along with that of anonymized peers in the sector to encourage improvement of their cyber security posture.

Notifications in 2023 to 2024

- 779 advisories
- 20 alerts
- 10 cyber flashes
- 18 priority notifications
- over 1,100 NCTNS subscribers
- over 175,000 NCTNS notifications
- 267 scorecards subscribers

Pre-ransomware notifications

This year, the Cyber Centre began issuing pre-ransomware notifications based on early detection of certain strains of ransomware. The Cybercrime chapter contains more information about pre-ransomware notifications.

Incident management

When cyber incidents happen, acting quickly and taking the right steps can significantly reduce the harm and speed up the recovery process.

This year, the Cyber Centre helped respond to 2,192 cyber security incidents across the Government of Canada and Canadian critical infrastructure. This is slightly more than the previous year.

The Cyber Centre's definition of a cyber incident[12] covers a wide range of attempted threat activity, **whether successful or not**.

Cyber incident cases opened by the Cyber Centre

- 2023 to 2024
  → Total cases: 2,192
    - Federal institutions: 1,017
    - Critical infrastructure: 1,175
- 2022 to 2023
  → Total cases: 2,089
    - Federal institutions: 957
    - Critical infrastructure: 1,132

Cyber threat intelligence

CSE gathers SIGINT on foreign state, state-aligned and cybercrime groups that pose a threat to Canada. This includes intelligence on their tactics, techniques and procedures (TTPs), the infrastructure they rely on, as well as the threat actors themselves.

This year, CSE identified foreign state and state-aligned cyber activity targeting Canada and enabled the defence against and mitigation of cyber threats impacting Canada and our partners.

CSE also provided insights into how foreign cybercrime groups operate and identified concrete ties between the groups, their partners and affiliates targeting critical infrastructure. This intelligence contributed to Canadian and allied efforts to disrupt, degrade and counter cybercriminal group capabilities (see Foreign cyber operations to counter cybercrime). It also supported allied governments' issuing of indictments and sanctions.

CSE intelligence also helped to inform the Cyber Centre's activities to help the Government of Canada, critical infrastructure partners and other systems of importance mitigate cyber threats. For example, SIGINT supported Cyber Centre advisories and threat assessments and contributed thousands of indicators of compromise to its automated threat data feed, Aventail.

Cyber threat intelligence case study

In early 2023, CSE's foreign intelligence allowed the Cyber Centre to respond to a cyber incident that could have caused serious damage to property and life. The intelligence discovered that a state-aligned actor had directed a cyber attack against Canadian CI to disrupt its operation and risk grave injury.

The state-aligned actor was able to gain access to the network and maliciously configure it to malfunction by taking advantage of an Internet-connected device with poor security protection. CSE's foreign intelligence brought the activities to light, and our Cyber Centre worked with security and intelligence partners, including the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS), to inform public safety officials. Officials then worked with the critical infrastructure provider to successfully mitigate the threat before any damage occurred.

Although it was not established that this activity was state sponsored, this situation demonstrates the growing cyber threats to our country's most essential systems, and how CSE is uniquely placed to address them using our foreign intelligence mandate. It also reinforces the importance of following and implementing the Cyber Centre's advice and guidance to increase cyber resilience.

International cyber security partners

The Cyber Centre works with other cyber security agencies around the world to mount a unified defence to cyber threats.

Five Eyes joint endorsements

When the Five Eyes and like-minded allies speak with one voice, the message is amplified around the world. This year, CSE and the Cyber Centre endorsed a record number of joint publications on issues of common concern, including:

- state-sponsored cyber threat activity targeting critical infrastructure
- cybercrime activity
- guidelines on the secure development and use of AI (see the Artificial Intelligence chapter)

You can find links to all 14 joint endorsements published this year on the Cyber Centre's website under news and events.[13]

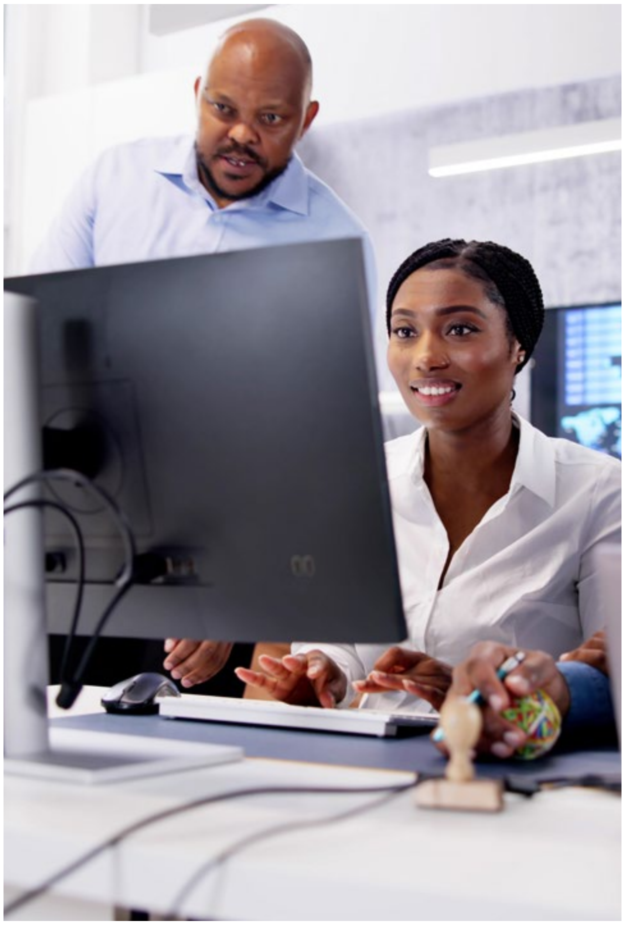
> **Canada has been with us at the head of the pack on cyber security and our relationship on cyber security is extremely strong and deep. It's the deepest of the Five Eyes actually and they have pioneered some things that we are using, including how you monitor for threats across government, and similarly we've shared capability in the other direction. So I think Canada is really nimble and they're very focused on cyber security.**
>
> \- Praise from our UK partners, GCHQ (Government Communications Headquarters) – UK Intelligence and Security Committee report,[14] December 2023

Sharing threat data at machine speed

Since its creation in 2018, the Cyber Centre has shared cyber threat information with international partners via email, web portals and other collaborative tools.

In March 2023, the Cyber Centre began hosting a new platform to share high-value cyber threat data with trusted international partners at machine speed. The platform is multi-directional. Indicators of compromise shared by one partner can be accessed by all participating partners in accordance with their mandates.

As of March 2024, 8 countries were using the platform, including Canada. The Cyber Centre is working to expand the membership over the next year.



FIRST conference

The Forum of Incident Response and Security Teams (FIRST) is an international non-profit association that brings together cyber response teams from over 100 countries. Founded in 1990, FIRST provides an invaluable forum for cyber defenders to share ideas, tools and best practices to improve cyber security on a global scale.

In June 2023, the Cyber Centre was the local host and provided the program chair for the 35th annual FIRST Conference[15] in Montreal. The theme was "Empowering communities". As the lead of multiple sessions, the Cyber Centre shared lessons learned from recent case studies to help organizations prepare for complex or unconventional cyber incidents. The Cyber Centre also delivered a full-day workshop on Assemblyline, our flagship malware analysis tool that is available open-source to cyber defenders worldwide.

Cyber security training

The Cyber Centre provides training through the Learning Hub[16] in cyber security and communications security (COMSEC). In the past, Learning Hub training was only available to Government of Canada employees and IT professionals in critical infrastructure sectors. This year, the Learning Hub introduced e-learning courses for 2 new target audiences:

- Introduction to Cyber Security for Educators[17]
- Cyber Security for Small and Medium Organizations[18]

The new courses are self-paced, free and open to all. They offer practical knowledge to help learners meaningfully improve their cyber security. The course for educators includes teaching resources to pass the learning on to students.

Training for public servants

To protect the Government of Canada's sensitive information and networks, it's critical that all public servants have a solid awareness and understanding of cyber security.

This year, the Learning Hub launched an update to its Cyber Security Fundamentals[19] course. It introduces Government of Canada employees who are not cyber security or IT security specialists to cyber security basics and the cyber threat landscape.

The Learning Hub also produced a new training series for the Canada Revenue Agency on developing software and web applications that are secure-by-design. The instructor-led training consists of 4 courses and takes 8 days to complete. The training will be made available to all Government of Canada departments in 2024.

The Learning Hub in 2023 to 2024

- Total participants: 12,273 (up 146%)
- Format
  - → E-Learning: 68%
  - → Instructor-led: 32%
- Audience
  - → Government of Canada: 93.5%
  - → Other: 6.5%

Russia's invasion of Ukraine

This year, CSE continued to leverage our foreign intelligence mandate to support Ukraine's resistance to Russia's ongoing, unjustifiable invasion.

For example, CSE identified financial and industry entities used by the Russian government to support its ability to fund the war in Ukraine by circumventing international sanctions. Canada and its allies used this information to put pressure on international entities that continue to do business with Russia.

In addition, CSE produced actionable intelligence for the Government of Canada and its allies to:

- detect and deter malicious Russian activity against Ukraine and other allies
- provide insights into military, political and economic developments related to the invasion
- monitor Russian disinformation campaigns
- monitor malicious Russian cyber activity against Canada and allies
- help protect Canadian government and allied military personnel in Ukraine
- support Operation Unifier, the CAF training mission in support of Ukraine

Meanwhile, the Cyber Centre continued to offer cyber security assistance to Ukraine and Latvia.

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 those countries' cyber systems as being of importance to Canada.

Over the past year, the Cyber Centre has continued to share information with both Latvia and Ukraine about cyber threats to their critical infrastructure. This information includes:

- cyber security vulnerabilities in critical networks
- technical cyber threat information
- unauthorized network access by malicious cyber actors

Cyber Centre teams have deployed to Latvia a total of 6 times in a joint effort with the CAF (Operation Reassurance) and Latvia's cyber security agency, CERT.LV. The 2 deployments this year occurred in the fall of 2023 and early 2024, each lasting roughly 3 weeks.

The teams conducted successful cyber threat discovery operations on the networks of the Latvian government and critical infrastructure organizations, and shared vital cyber defence information to aid in countering sophisticated cyber threat actors.

> “Cyber threat activity poses a real and growing threat to Canada's democratic processes.”
>
> - Cyber Threats to Canada's Democratic Process: 2023 update

Hostile state activity and foreign interference

Hostile state activity and foreign interference take many forms and often involve a cyber dimension. Examples include covert attempts to influence democratic processes, online disinformation, state-sponsored cyber threat activity and economic espionage.

CSE and the Cyber Centre play key roles in monitoring and defending against foreign efforts to interfere in Canada’s affairs. Consult the Accountability chapter for information about Reviews into foreign interference.

Cyber threats to Canada’s democratic process

Cyber threat activity targeting elections is on the rise worldwide. Online disinformation is now ubiquitous in elections around the world, and generative AI is increasingly used to influence elections.

Those are some of the key findings of CSE’s latest report on the topic: Cyber Threats to Canada’s Democratic Process: 2023 update.[20]

Published in December 2023, the report predicts that malicious cyber threat activity is more likely to happen during Canada’s next federal election than in the past. This includes the “very likely” use of AI-generated content to influence voters.

The report found that cyber-enabled influence campaigns, such as hack-and-leak operations, were 7 times more common than attempts to target voting infrastructure. It also observed that cyber threat actors are getting better at covering their tracks.

The report also notes that increased tensions between Canada and a hostile state in the run-up to a national election would very likely result in cyber threat actors targeting Canada's democratic processes or disrupting Canada's online information ecosystem. The report names the PRC and Russia as the most active foreign state actors engaged in cyber threat activity targeting elections, democratic institutions, government officials and diaspora communities worldwide.

In addition, the Independent Special Rapporteur on Foreign Interference, appointed to look into the extent and impact of foreign interference in Canada's electoral processes, published a May 2023 report which shared examples of how the PRC is particularly active when it comes to foreign interference activities in Canada.

Monitoring for interference in federal by-elections

As a member of the Security and Intelligence Threats to Elections (SITE) Task Force, CSE worked with CSIS, the RCMP and GAC to monitor and report on threats to 6 federal by-elections held this year, for the first time.

CSE's foreign signals intelligence program monitored for signs of foreign interference, including attempts to affect the outcome of the by-elections or to undermine public confidence in the integrity of the process.

Meanwhile, the Cyber Centre helped to ensure the cyber security of the by-elections by:

- monitoring for malicious cyber activity targeting Elections Canada
- 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

During the by-election periods, the SITE Task Force provided weekly situation reports to the Deputy Minister Committee on Intelligence Response. Following the by-elections, the Task Force shared its findings with the public in unclassified reports.[21] As stated in those reports, the Task Force did not detect any attempts at foreign interference aimed at the by-elections or any cyber incidents that would suggest foreign state actors were specifically targeting Elections Canada during the by-election periods.

CSE continues to work closely with partners to develop and report foreign intelligence to monitor and respond appropriately to increased threats by highly capable and motivated threat actors.

Supporting provincial and territorial election integrity

Foreign interference is an issue for every level of government.[22] This year, the Cyber Centre worked with provincial and territorial electoral management bodies (EMBs) to combat foreign cyber threats to elections. For example, the Cyber Centre:

- relaunched a quarterly community call with provincial and territorial EMBs
- developed guidance about cyber threats to elections
- supported provincial and territorial initiatives such as the Elections BC Election Integrity Working Group
- supported training for Canadian election officials
- supported EMBs on the secure use of electronic voting systems and electronic poll book systems
- participated in EMB information sessions for political parties

Online disinformation

State actors use online disinformation as a tool for foreign interference. Disinformation also causes people to make decisions that are not in their best interests such as investing in cryptocurrency scams or bogus health products.

Advances in AI mean that threat actors can now create and spread misleading content with ease, including deepfake videos that are increasingly difficult to spot.

CSE and the Cyber Centre have drawn attention to the threat posed by disinformation in 2 recent flagship reports:

- National Cyber Threat Assessment 2023-2024[23] (October 2022)
- Cyber Threats to Canada's Democratic Process: 2023 update[24] (December 2023)

> **Disinformation has become ubiquitous in national elections.**
>
> - Cyber Threats to Canada's Democratic Process: 2023 update

Online disinformation awareness campaign

This year, CSE led phase 2 of an advertising campaign on behalf of the Government of Canada to raise awareness about online disinformation. The campaign encouraged Canadians to be skeptical about content they come across online and used the tagline “If it raises your eyebrow, it should raise questions”.

- Online disinformation campaign video “If it raises your eyebrow, it should raise questions”[25]

The campaign videos and online ads led to an updated online disinformation[26] web page about the harm disinformation causes and tips and tools to spot it.

The campaign ran from January to March 2024 on various digital platforms, including X (Twitter), TikTok and YouTube. The ads were displayed 159 million times, generating over 12 million video views and over 400,000 visits to the web page.

State-sponsored cyber threat activity

The Cyber Centre assesses that "the state-sponsored cyber programs of China, Russia, Iran and North Korea pose the greatest strategic cyber threats to Canada."[27]

This year, CSE and the Cyber Centre continued to share information about these threats through a combination of public communications and warnings sent directly to Cyber Centre partners.

People's Republic of China sponsored cyber threat activity

In May 2023, CSE and the Cyber Centre joined their Five Eyes partners to warn about a cluster of cyber threat activity associated with the People's Republic of China.[28] The joint advisory highlighted a technique called "living off the land," which is hard to detect because it closely resembles normal cyber activity. While the activity detected was mostly directed at critical infrastructure in the U.S., the same technique could be used against any target anywhere in the world.

In February 2024, the Cyber Centre endorsed a joint advisory on PRC state-sponsored actor Volt Typhoon[29] compromising U.S. critical infrastructure networks. This was followed in March by joint guidance for critical infrastructure leaders[30] about the same PRC cyber activity. The advisory assessed that the activity is intended to pre-position for disruptive or destructive cyber attacks in the event of a major crisis or conflict with the U.S. Any disruption of U.S. critical infrastructure would also likely impact Canada since our infrastructure is closely linked.

Both advisories included technical guidance on how to detect and defend against the methods described.

Russia-aligned cyber threat activity

On April 12, 2023, the Cyber Centre issued a cyber flash to warn critical infrastructure partners about a notable rise in Russia-aligned cyber threat activity against Ukraine's allies, including Canada. The activity included attempts to compromise operational technology (systems used to control physical equipment). It also included distributed denial of service (DDoS) attacks against government and business websites.

On April 13, 2023, the Minister of National Defence amplified the cyber flash by issuing a public statement about Russia-aligned cyber threat activity.[31] The statement urged critical infrastructure organizations to secure their systems and pointed them to the relevant Cyber Centre guidance.

In September 2023, CSE issued a further warning to the Canadian cyber security community[32] ahead of an official visit by Ukrainian President Volodymyr Zelenskyy.

In February 2024, CSE again urged Canadian organizations to be vigilant around the 2-year mark of Russia's invasion of Ukraine.[33]

In addition, CSE and the Cyber Centre endorsed joint cyber security advisories from Five Eyes partners warning about:

- sophisticated Russian spear-phishing campaigns[34]
- Russian state actors adapting their tactics to access cloud infrastructure[35]

Economic security

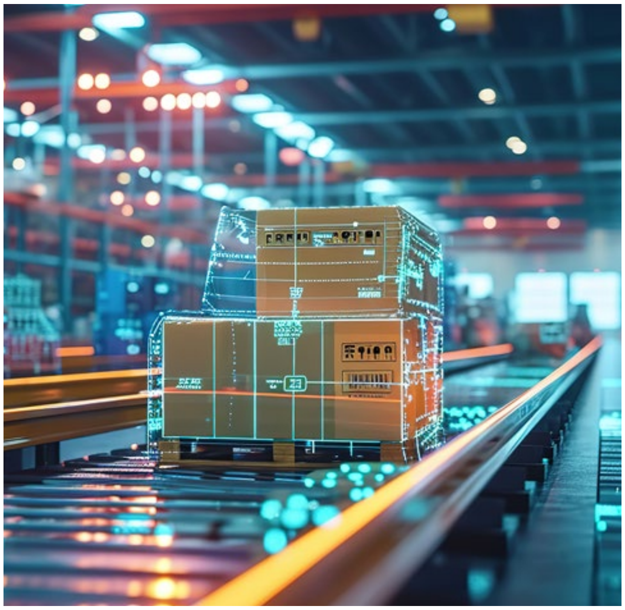
CSE works with federal partners to protect Canada's economy from hostile state activity and foreign interference, including national security threats, economic espionage and supply chain risks. Our economic security programs draw on the foreign intelligence and cyber security aspects of CSE's mandate as well as our expertise in cutting-edge technologies.

Research security

In January 2024, the Government of Canada implemented new measures to protect Canadian research in sensitive technology areas. The Policy on Sensitive Technology Research and Affiliations of Concern[36] offers guidance to help Canadian researchers avoid links with organizations that pose a high risk to Canada's national security. Examples include institutes with ties to government or military entities in Russia, China and Iran. CSE contributed to both the list of sensitive technology research areas and the list of organizations of concern.

Supply chain integrity

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 as well as the business practices, cyber maturity and foreign ownership of vendors. CSE increasingly works with partners outside the federal government, such as provinces and private sector partners, on supply chain risks. This year, CSE conducted 1,291 supply chain risk assessments.



Protecting Canada's telecommunications infrastructure

Canadians rely upon connectivity in their day-to-day lives. This year CSE continued to work with Canadian mobile network operators (MNOs) to improve the security and resilience of Canada's 4G and 5G networks by:

- identifying and mitigating cyber security and supply chain risks
- sharing threat information and best practices

For example, threat actors such as state actors and cybercriminals can exploit mobile network signalling to track the location of cell phone users. CSE leveraged industry threat intelligence to alert MNOs to the presence of this type of threat activity on their networks. CSE also shared technical guidance with MNOs on how to optimize their network defences against this specific threat.

International standards

Threat actors can influence the security of products in the standards development process, before the products are even designed. CSE works with federal and international partners in this increasingly contested space to ensure that standards for IT and cryptography remain rigorous.

This year, CSE continued to certify commercial IT products under the Common Criteria program (for cyber security) and the Cryptographic Module Validation Program (for cryptographic integrity). CSE is also working with federal and international partners to develop international standards for AI technologies.

National security reviews

This year, CSE continued to conduct national security reviews in support of the:

- *Investment Canada Act*
- *Export and Import Controls Act*
- *National Security Guidelines for Research Partnerships*

Counter terrorism

CSE continued to provide foreign intelligence of value to protect Canadians and Canadian interests from terrorism and violent extremism, including:

- religiously motivated violent extremism (RMVE)
- ideologically motivated violent extremism (IMVE)

Examples of RMVE threats include al-Qaeda and the numerous affiliates of Daesh (ISIS), whereas IMVE threats include a range of xenophobic, anti-authority, gender identity-driven and grievance-driven extremist ideologies. CSE's focus is on using online tools and techniques to identify the activities of foreign-based extremists who pose a threat to Canada or Canadians.

This year, CSE continued to work with Government of Canada departments and agencies to identify and gather intelligence on foreign extremists attempting to inspire and enable "lone wolf" or small-cell attacks in Canada. As an example, CSE worked with CSIS and RCMP to identify foreign extremists of concern and to provide critical information on their recruitment, radicalization and attack planning activities.

CSE also pursued foreign intelligence on foreign extremist threats against Canadians and Canadian interests abroad. CSE's efforts ranged from support to victims of kidnappings to coverage of threats against public events, Canadian embassies and missions, and extremist threats to allies. On multiple occasions, CSE intelligence helped international partners to mitigate and disrupt violent extremist threats, potentially saving lives.

In addition to enabling real-world disruptions of foreign extremist activities, CSE intelligence informed our active cyber operations against violent extremists and organizations (see Countering violent extremism).

The Arctic

Maintaining Canada's sovereignty in the Arctic is a Government of Canada priority that involves both the cyber security and foreign intelligence aspects of CSE's mandate.

Scanning the horizon

The Arctic is a region rich in natural resources and strategic importance. Climate change and technological advances are making it easier to access the region. As Canada's Arctic and Northern Policy Framework states, this "brings safety and security challenges to which Canada must be ready to respond."[37]

CSE works with domestic partners and international allies to provide foreign intelligence relating to Arctic activities of foreign actors and to understand their long-term strategic goals. This includes producing foreign intelligence reports on foreign states' political intentions, military capabilities, technological advancements, economic interests and research activities in the region.

This year, CSE shared 132 intelligence reports on Arctic security with 17 Government of Canada departments, as well as with Canada's international allies.

Domestic partners

CSE continued to work with the CAF to make sure the Government of Canada has the intelligence it needs to defend Canada's security and sovereignty in the Arctic. This included tracking vessels by air and sea, and other objects in the region.

Alongside the Privy Council Office, CSE continued to co-chair the Arctic Intelligence Coordination Group, which coordinates Arctic security activities across the Government of Canada.

International allies

CSE continued to participate in two multinational intelligence forums to coordinate with like-minded allies on Arctic security. One forum, chaired by CSE, is specific to signals intelligence and concerns both polar regions. The other is an all-source intelligence forum focused exclusively on the Arctic.

CSE led 2 international conferences in support of these forums this past year. These in-person events served to identify key intelligence questions, to agree on shared priorities and to deconflict lines of effort related to the Arctic.

Securing the North

A series of cyber incidents targeting northern institutions have highlighted the vital strategic importance of cyber security in the North.

In November 2022, the Cyber Centre conducted an urgent rollout of its sensors in response to a cyber incident affecting the Government of Northwest Territories.

Following that incident, the Cyber Centre identified 2 urgent priorities for securing the North:

- to provide the territorial governments with capabilities for secure communication with Cyber Centre leadership
- to deploy sensors on territorial government IT assets to detect malicious cyber activity on an ongoing basis

By November 2023, the Cyber Centre had established secure communications with all 3 territories, and in January 2024, the Cyber Centre began the sensor rollout process. This is the first time the Cyber Centre has deployed sensors to a non-federal organization proactively rather than in response to a cyber incident.

Throughout the year, the Cyber Centre continued to work with partners in the North to:

- improve processes for threat information sharing
- provide better vulnerability notifications
- help manage supply chain risks

This included visiting each territory to meet with critical infrastructure providers and other systems of importance including airports, energy providers and universities.

Timeline of cyber incidents in the North

November 2022

Cyber incident affects Government of Northwest Territories

January 2023

IT systems compromised at Qulliq Energy Corporation, Nunavut

July 2023

Database hacked at Nunatsiavut Government

September 2023

DDoS attack on government websites across Canada, including Nunavut and Yukon

Canada’s Indo-Pacific Strategy

In November 2022, the Government of Canada published its Indo-Pacific Strategy, designed to guide Canada’s policies and engagement in the Indo-Pacific region over the next several decades.

The strategy aims to enhance Canada’s intelligence and cyber security capacity to help protect Canadians from threats such as:

- foreign interference
- cyber threats
- hostile activities by state actors
- economic-based national security threats

The strategy also aims to deepen security partnerships and build cyber security capacity in the region.

This year, CSE supported Canada’s Indo-Pacific Strategy by responding to increased requests for intelligence related to the region and by engaging with regional partners.

The People's Republic of China and Indo-Pacific regional stability

The PRC continues to be a sophisticated state actor with a broad and capable security and intelligence apparatus.

The PRC has demonstrated a variety of behaviours that threatens the safety of Canadians. Some examples include unsafe intercepts of CAF deployed operations in international waters in support of Canada's Indo-Pacific Strategy[38] and the persistent threat of PRC cyber activity directed against Canada and its allies.[39] Canada continues to call out this behaviour noting the increasingly worrisome pattern of acts of intimidation by the PRC in regions like the South China Sea.[40]

CSE works closely with security and intelligence partners, both domestic and international, and a variety of intelligence clients to deliver against Canada's foreign intelligence requirements to inform, deter and counter the malign activities of the PRC government and its intelligence services. The PRC continues to use a broad range of overt, covert and clandestine methods to advance its interests having significant implications for Canada and Indo-Pacific nations and will remain an enduring threat to the rules-based international order as it seeks to reinterpret these rules for its own benefit.

In reaction to heightened strategic competition in the region, CSE has increased its foreign intelligence reporting capacity in support of the Government of Canada and our allies. Reports produced by CSE this year provided insight to:

- detect and mitigate cyber threats from the PRC to Canada and our allies
- monitor influence campaigns that promote Chinese Communist Party narratives and undermine trust in democratic institutions
- uncover activities deliberately detrimental to Canadian prosperity and economic interests
- inform on trends and events that pose a threat to stability in the region

Support to Indo-Pacific cyber security

The Cyber Centre routinely exchanged information on cyber threats with partners in the Indo-Pacific region. This information helped to enhance the Cyber Centre's guidance for Canadian critical infrastructure organizations and the Government of Canada. The Cyber Centre continued to build relationships with regional cyber security partners by participating in events such as:

- Singapore International Cyber Week
- a cyber security conference co-organized by the Embassy of Canada to the Philippines
- the annual meeting of the Pacific Cyber Security Operational Network

Foreign cyber operations

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 (DCO) 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 (ACO) can be used proactively to disrupt foreign-based threats to Canada's international affairs, defence or security interests.

CSE often conducts foreign cyber operations in coordination with our Five Eyes partners to achieve common goals. We also conduct joint cyber operations with the CAF to support their mission objectives.

Responsible cyber power

The *CSE Act* is clear on certain boundaries that CSE's 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, 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.

CSE has a well-established governance framework for guiding its foreign cyber operations and ensuring that they adhere to the *CSE Act* and Ministerial Authorizations issued. This includes close consultation with GAC for assessing the foreign policy impacts and legal implications of proposed cyber operations. These assessments take into account both Canadian law and international law applicable in cyberspace.[41]

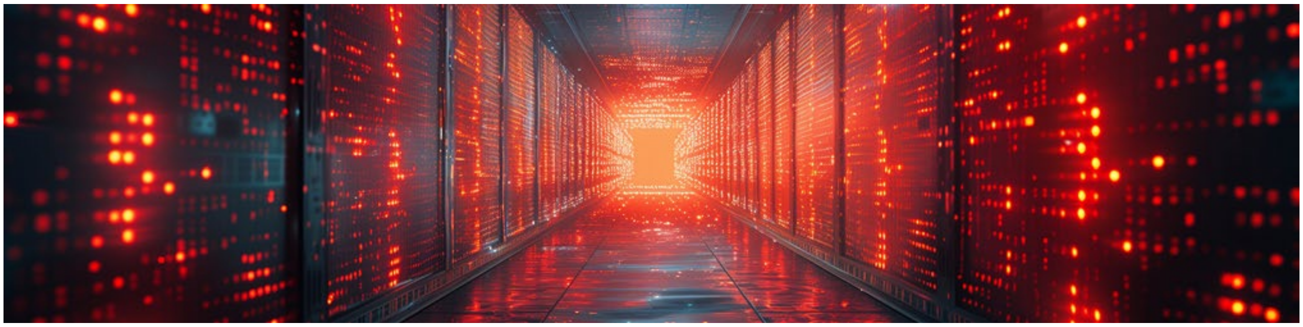
Countering hostile state activity

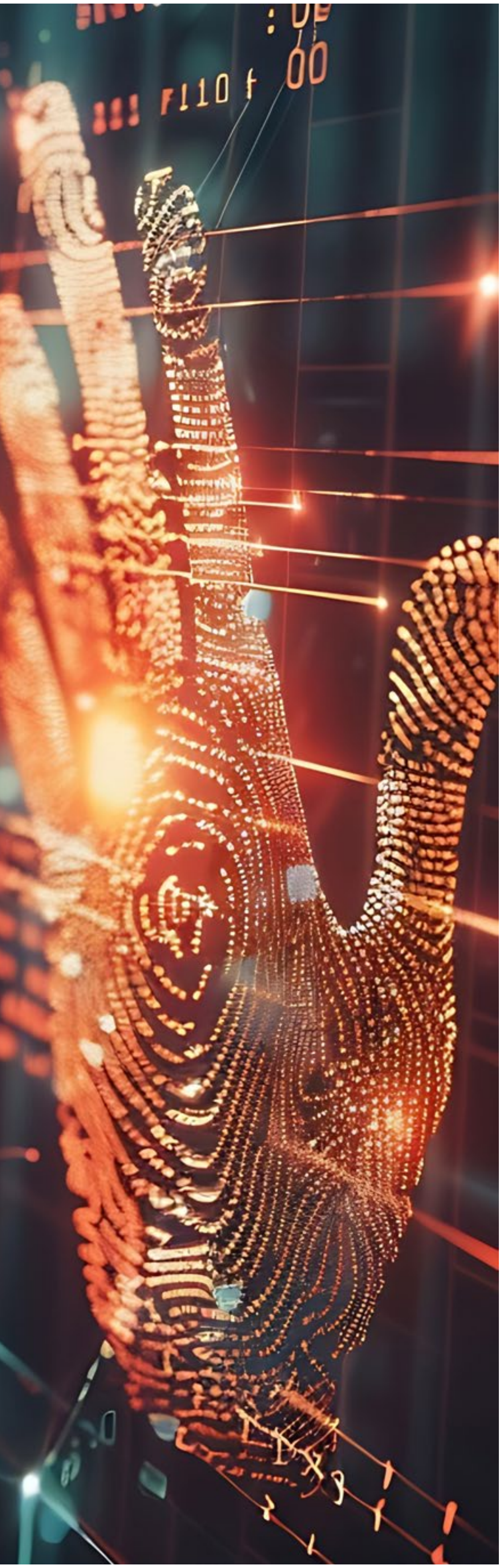
This year, CSE continued to use its ACO capabilities to counter hostile activity by foreign state actors. These operations have disrupted threats offshore, countering them before they impact the security of Canadians. These threats include:

- foreign interference and malign influence directed at Canada and its allies
- disinformation operations
- malicious cyber threat activity
- espionage

Countering cybercrime

CSE is engaged in an ongoing campaign to disrupt the activities of cybercrime groups. Consult the Cybercrime chapter for details on CSE's use of Foreign cyber operations to counter cybercrime.





Countering violent extremism

CSE continued to conduct active cyber operations to counter the dissemination of violent extremist materials online. This year, CSE used ACO to counter foreign groups involved in both ideologically motivated and religiously motivated violent extremism.

These extremists use violent videos and images to spread their ideologies and to recruit and radicalize followers. By hampering their online propaganda activities, CSE reduced the extremists' credibility and ability to influence others online.

Why we can't say more

CSE strives to be as transparent as possible while safeguarding classified information. As a rule, CSE cannot share any information that would:

- allow the target of a cyber operation to identify CSE as the source of the disruption
- describe the techniques or capabilities CSE uses
- reveal the extent of CSE's capacity to conduct cyber operations

Any of the above could result in serious harm to Canada's national interest, which is why we can't provide details on the specific targets we disrupted, how or when. We're not being secretive for the sake of it. We're preserving those capabilities for the next time they are needed to defend Canada and Canadians.

Cybercrime

Cybercriminals continue to target Canadian organizations with increasing brazenness and sophistication. A 2023 survey of large Canadian organizations suggests that 1 in 3 were impacted by ransomware with an average ransom payment of over $1 million CAD.[42]

The Cyber Centre calls ransomware "the most disruptive form of cybercrime facing Canada" because of its potential to impact the critical services Canadians rely on.[43] This has been demonstrated by high-profile Canadian examples like the 2021 ransomware attack on the healthcare system of Newfoundland and Labrador which affected more than 1 in 10 people in the province, and the 2023 targeting of 5 hospitals in Ontario.

Countering cybercrime is a high priority for CSE and involves every aspect of our mandate.

Foreign cyber operations to counter cybercrime

In 2023, CSE used its DCO capabilities for the first time against a foreign ransomware group that was targeting multiple Canadian critical infrastructure organizations. While the Cyber Centre worked to mitigate the compromise within Canada, CSE's foreign cyber operations team took action in cyberspace. The DCO interfered with the cybercriminals' foreign servers, reducing the effectiveness and profitability of their activities. Most importantly, CSE's actions reduced the impact of the incident on the victims.

Following that first DCO, CSE continued to conduct other DCOs over the course of the year. This included an operation to counter a cybercriminal group that was conducting DDoS attacks against Canadian federal institutions and critical infrastructure organizations.

CSE also continued its ongoing ACO campaign to disrupt the activities of foreign ransomware groups. Working with Five Eyes partners, CSE used ACO to undermine the activities of foreign ransomware groups and to degrade the online tools they use. These ongoing operations make it harder for cybercriminals to launch ransomware attacks against Canadian organizations and to profit from the theft of Canadian data. CSE prioritizes its operations based on the Cyber Centre's assessments of which ransomware groups pose the greatest threat to Canada.

Lasting impacts

Last fiscal year, CSE led a multinational foreign cyber operations campaign against a foreign-based ransomware group. The group had been linked to cyber incidents affecting healthcare systems and other critical sectors in Canada and allied countries. CSE led this operation with our Five Eyes partners to disrupt the technical infrastructure the group was using. This was the first multinational operation led by CSE. As a result of it, the ransomware group appeared to break apart and cease its activities. Since the campaign, CSE has not seen the cybercrime group reconstitute itself or commit any further threat activity in Canada.

Public Service Award of Excellence

In 2023, CSE's Counter Cybercrime Team received a team award at the 2022 Public Service Awards of Excellence for their work to reduce the impact of cybercrime on Canadian organizations. The award recognized the team for its "innovations and exceptional contributions" in the global fight against cybercrime.

> **“Through their innovations and exceptional contributions, the team has shown Canada to be a strong contributor in the global fight against cybercrime.”**
>
> \- The Public Service Award of Excellence 2022

Pre-ransomware notifications

In May 2023, the Cyber Centre launched a new pilot initiative in the fight against ransomware. 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.

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 U.S.-led Joint Ransomware Task Force

Since the launch of the pilot, the Cyber Centre has issued pre-ransomware notifications to over 250 Canadian organizations. The would-be victims range across every level of government and key sectors like healthcare, energy, manufacturing, finance and education.

The Cyber Centre has also worked with 10 international partners, including the Cybersecurity and Infrastructure Security Agency (CISA), to issue pre-ransomware notifications to organizations outside Canada.

While pre-ransomware notifications are a useful tool in the fight against ransomware, they are not a silver bullet. Ransomware remains a persistent and pervasive threat. As threat actors continue to evolve their tactics, the Cyber Centre will continue to partner with Canadian and international organizations to mitigate ransomware and make cyber systems more resilient. Contact the Cyber Centre[44] for guidance on how to harden your defences.

Pre-ransomware notifications 2023 to 2024

OVER 250
Canadian organizations

10
International partners

Cybercrime publications

In August 2023, the Cyber Centre published its Baseline cyber threat assessment: Cybercrime.[45] The report traces the evolution of cybercrime and assesses its current implications for Canada.

The report finds that "cybercriminals will almost certainly continue to target high-value organizations in critical infrastructure sectors in Canada and around the world" and that Russia and Iran act as "cybercrime safe havens." The report shows that there is no pattern to the Canadian organizations that have fallen victim to ransomware. No sector is immune.

The Cyber Centre produced profiles of 6 cybercrime groups this year. All 6 were shared with cyber defenders. For the first time, 2 were also published online:

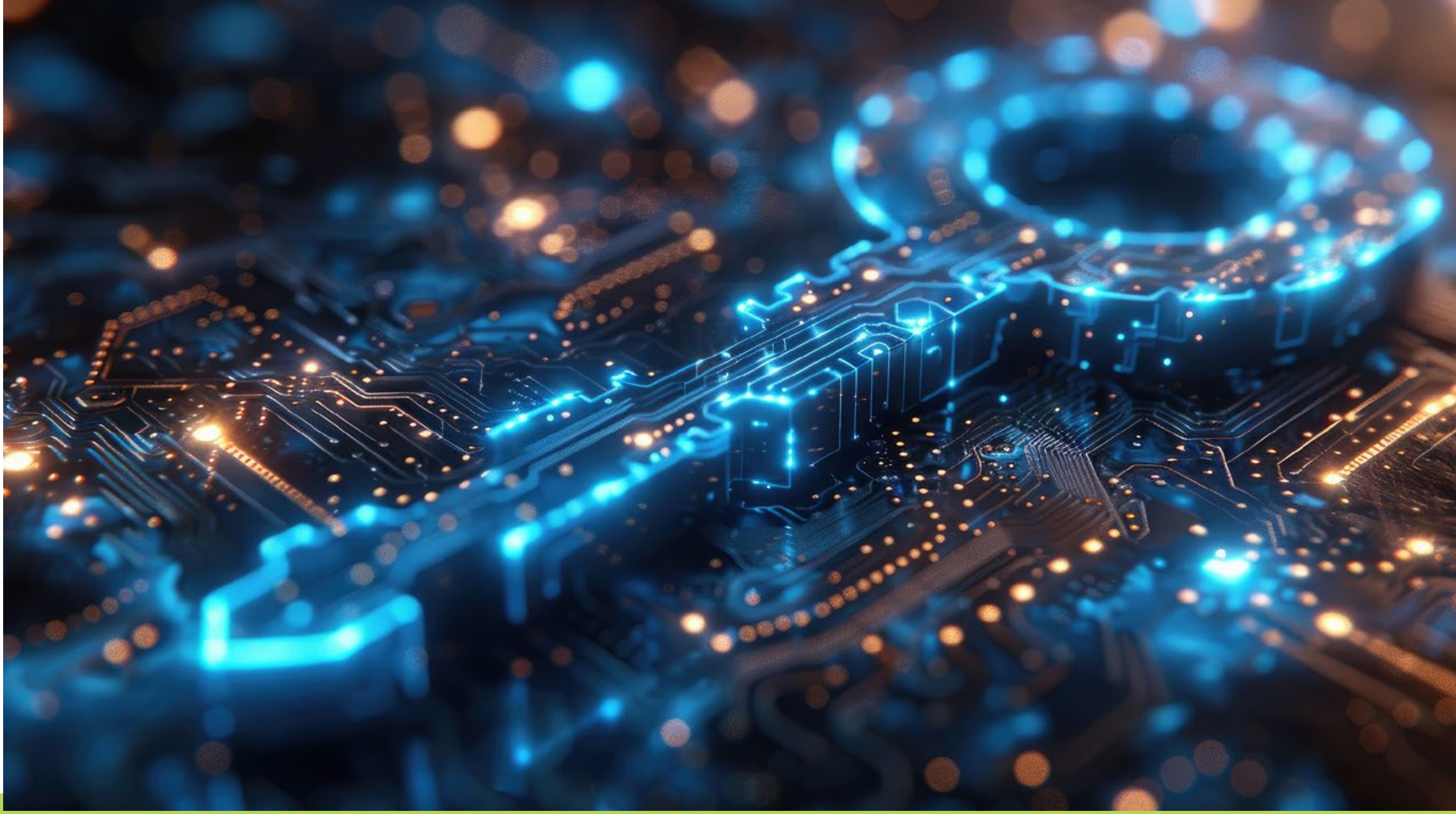
- Profile: ALPHV/BlackCat ransomware[46]
- Profile: TA505 / CL0P ransomware[47]

The Cyber Centre also contributed to 2 joint cyber security advisories with Five Eyes partners:

- Joint advisory on Truebot malware[48]
- Joint advisory on Lockbit ransomware[49]

The Cyber Centre continued to produce ransomware threat ranking products and other classified reporting to help identify opportunities for deterrence and disruption.

Communications Security Establishment
Centre de la sécurité des télécommunications
CANADIAN CENTRE FOR
CYBER SECURITY
BASELINE THREAT ASSESSMENT
CYBERCRIME
Canada



Communications security

Communications security (or COMSEC) is integral to CSE's mission. It's how we protect the Government of Canada's most sensitive data and communications from being read or modified by adversaries.

This year, CSE continued to provide the Government of Canada and industry partners with COMSEC solutions, including secure hardware, software and cryptographic keys.

CSE continued to provide advice and guidance to federal institutions and critical infrastructure organizations on secure communications solutions.

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.

This year, CSE continued to contribute to the international standardization process for quantum-safe cryptography. CSE provided public feedback on 3 draft standards led by the U.S. National Institute of Standards and Technology.

Meanwhile, CSE worked with federal partners to plan for the rollout of quantum-safe cryptography across the Government of Canada once the international standards are finalized.

CSE also provided dozens of briefings to government and critical infrastructure partners on the quantum threat and how to prepare for the quantum-safe transition. These briefings included the importance of using standardized and validated cryptography to prevent unnecessary security vulnerabilities.

Empowering Canadians

CSE and the Cyber Centre empower Canadians by sharing information and by working with partners to make Canada a safer place to live and work online.

Threat assessments

The Cyber Centre regularly publishes threat assessments to help readers understand and address the cyber threats Canada faces. The assessments also help to set CSE's mission priorities. This year, the Cyber Centre published 4 major threat assessments:

- The cyber threat to Canada's oil and gas sector[50]
- Baseline cyber threat assessment: Cybercrime[51]
- Cyber Threats to Canada's Democratic Process: 2023 update[52]
- The threat from large language model text generators[53]

In addition, the Cyber Centre published 2 profiles of specific cybercrime groups (see Cybercrime publications).

Guidance publications

The Cyber Centre issues guidance publications for a variety of audiences, from general readers to managers, executives and IT practitioners.

This year, the Cyber Centre published 34 new guidance publications and updated 14. High priority topics included:

- emerging technology, like AI
- social engineering tactics, like phishing
- authentication and administrative privileges
- mitigation measures for advanced threat actor tactics and techniques

Browse the Cyber Centre's full catalogue of cyber security guidance.[54]

Get Cyber Safe

CSE shares cyber security advice directly with Canadians through the 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.

This year, Get Cyber Safe produced over 40 new resources on a wide range of topics from securing personal devices to avoiding cyber scams.

Browse the full range of Get Cyber Safe resources.[55]

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.

To help fill this gap, in early 2024, Get Cyber Safe produced a series of resources for small business owners and an updated Quick Guide to Cyber Security for Small Business.

Browse Get Cyber Safe resources for small businesses.[56]

Get Cyber Safe also launched an advertising campaign about ransomware with small businesses as the main target audience. From February to March 2024, the ads were displayed over 49 million times, generating 3.8 million video views and almost 49,000 visits to the Get Cyber Safe website.

Get Cyber Safe for Indigenous audiences

All Get Cyber Safe resources are available in both English and French. This year, to better reach Indigenous communities, Get Cyber Safe began translating its most downloaded resources into various Indigenous languages. The following infographics are now available in Ojibwe, Cree, Inuktitut and Mi'kmaq:

- The 7 red flags of phishing[57]
- Multi-factor authentication makes cyber security all about you[58]
- Does your data have a backup plan?[59]

ᖃᐅᔨᓇᖅᑐᖅ 7
ᖁᒍᕙᑦ ᖃᐅᔾᔪᑎᒋᔪᓐᓇᖅᑕᑎᑦ
ᖃᓇᓴᐅᔭᒃᑯᑦ ᐱᕋᔭᒃᑕᐅᓇᓱᒃᑯᕕᑦ

ᐅᓇ ᖃᓇᓴᐅᔭᒃᑯᑦ ᐱᕋᔭᒃᑕᐅᓇᓱᖕᓂᖅ ᐅᓗᓇᐊᖅᑳᓴᓇᔾᔪᑕᐅᒐᔪᖕᓂᖅᐸᐅᔪᖅ ᖃᐅᔨᓇᖅᓯᓲᑦ ᐃᑭᐊᕿᕕᒃᑯᑦ. ᐊᓕᐊᓇᐃᑦ, ᖃᓇᓴᐅᔭᒃᑯᑦ ᐱᕋᔭᒃᑕᐅᓇᓱᓕᕈᕕᑦ ᕿᓚᒥ ᖃᐅᔨᓇᖅᑐᑎᑦ - ᖃᐅᔨᒪᒍᕕᑦ ᖃᓄᐃᓕᖓᒐᖕᒪᖔᑕ ᖃᐅᔨᓇᓱᒍᓐᓇᖅᑐᑎᑦ. ᑕᕝᕙ 7-ᖑᔪᑦ ᖃᐅᔾᔪᑎᒋᔪᓐᓇᖅᑐᑦ ᖃᐅᔨᒋᐊᕐᓗᒋᑦ ᖃᓇᓴᐅᔭᒃᑯᑦ ᑎᑎᕋᖃᐅᓯᐊᕈᕕᑦ ᐅᑯᐊᓗᓐᓂᑦ ᐅᖃᓘᑎᕋᕐᓂᑦ ᑎᑎᕋᕕᐅᒍᕕᑦ.

Cyber Security Awareness Month

Every October, the Get Cyber Safe campaign leads Cyber Security Awareness Month (Cyber Month) in Canada. This year's theme was "Step up your cyber fitness," with dozens of resources to help Canadians build up their cyber muscles. These included downloadable social media graphics, virtual meeting backgrounds, an interactive quiz[60] and a cyber security workout video.[61] Sample lyric: "Next do the move that's sweeping the nation. Enabling multi-factor authentication."

National partners such as Media Smarts and the Canadian Bankers Association helped to co-create and share Cyber Month content. Meanwhile, over 360 organizations shared our Cyber Month content with their audiences. Over the course of Cyber Month, Get Cyber Safe's content was seen over 293,000 times.

Learn more about Cyber Security Awareness Month.[62]

Social media

CSE's social media team shares content with Canadians on 5 platforms: X (Twitter), Facebook, LinkedIn, YouTube and Instagram. In total there are 17 accounts for different audiences. This includes channels in English and French for CSE, the Cyber Centre and Get Cyber Safe.

This year, the number of followers across those accounts increased from 184,000 to 198,000. The total number of posts was 5,580. This content was seen over 4 million times.

Social media by the numbers

17 Accounts

5 Platforms

198,000 Followers

5,580 Posts

4 Million + Impressions

Mitigations

Threat actors use malicious domains to host spoof websites and send fraudulent emails. The domain names often closely resemble those of legitimate organizations to fool you into giving up personal information or downloading malware. This year the Cyber Centre worked with trusted industry partners to block or take down almost 300,000 malicious domains. This included over 10,000 websites impersonating Government of Canada institutions.

- 2023 to 2024
  - → Government of Canada spoofs: 10,700
  - → Other malicious domains: 284,000
- 2022 to 2023
  - → Government of Canada spoofs: 3,167
  - → Other malicious domains: 306,000

Smishing scams

Smishing refers to scam messages sent by SMS (text). Smishing messages often contain links to spoof websites imitating trusted sources like government agencies, banks, delivery companies or online stores.

You can report smishing messages[63] by forwarding the text to 7726 (spells out SPAM on the keypad). This helps telecommunications service providers (TSPs) identify and block smishing attacks for all users. Several TSPs have also partnered with the Cyber Centre to share anonymized spam content. The Cyber Centre works with trusted industry partners to find and mitigate new malicious URLs (web links) contained in the content.

This year, the Cyber Centre received over 1.6 million smishing messages from TSPs and mitigated over 37,000 new phishing URLs.

CIRA Canadian Shield

Cybercriminals often try to trick you into clicking on links that will infect your device with malware or connect you to a malicious website. CIRA Canadian Shield[64] is a free service for Canadians to protect themselves using threat data from the Cyber Centre combined with commercial cyber security feeds.

To date, over 278,000 users have subscribed to CIRA Canadian Shield's threat blocking services. The service recorded over 500 million blocks over the course of the year. That's around 5 malicious connections prevented per user per day.

Growing the cyber workforce

There is a global shortage of skilled cyber professionals. Tackling this problem requires collaboration between government, industry and academia. As Canada's national centre for cyber expertise, the Cyber Centre plays a coordinating role to support and guide these efforts.

In April 2023, in consultation with partners in industry and academia, the Cyber Centre published the Canadian Cyber Security Skills Framework.[65] The framework highlights current gaps in Canada's labour market and the skills needed to fill different cyber security roles.

The Cyber Centre continued to produce resources for teachers and students to promote cyber security skills. This included the new Learning Hub course for educators (see Cyber security training) and a gamified course, Keep Canada Safe! Discover Careers in Cyber Security,[66] about cyber security careers on the digital learning platform, ChatterHigh.

Community outreach

CSE conducts a range of outreach activities to help inspire the next generation of cyber defenders. We have a particular focus on reaching groups that are currently underrepresented in the field.

This year, CSE continued to support the following partners to get more young Canadians interested in tech careers:

- Actua
- Black Boys Code
- Black Diplomats Academy
- CyberSci
- Cyber Titan
- Hackergal

CSE volunteers participated in:

- 7 coding workshops in 3 Ottawa schools
- hackathons and career workshops with Hackergal and Cyber Titan
- a career day at CSE with Black Boys Code

> **“I really liked it because it felt like it connected me to people like me. It gave me an opportunity to learn about jobs after high school that I would have never thought about.”**
>
> - Participant in the Black Boys Code career day at CSE

Innovation

At CSE, the work we do has a significant impact on Canada and Canadians. Because of this, we strive to be at the forefront of innovation and research, continuously investigating new threats, exploring new capabilities and collaborating with new partners. This ensures that we continue to be successful in carrying out our mission, both now and in the future.

Launch of new Innovative Business Strategy and Research Development branch

In September 2023, CSE created a new branch to promote innovation through collaboration with internal and external partners. Among other priorities, the Innovative Business Strategy and Research Development branch will:

- support the development of CSE's new strategic vision and plan
- foster engagement with industry, academia, and provincial and territorial partners
- acquire outside innovation, capabilities and talent to support CSE goals

The creation of this branch demonstrates the importance of research and innovation in the delivery of CSE's mission.

Research

CSE researchers explore a wide range of topics in support of our mandate. From cryptography and cyber security to data science and vulnerability research, they ensure that we have the expertise to tackle current and emerging challenges.

CSE-NSERC Research Communities grants

This year, CSE and the Natural Sciences and Engineering Research Council of Canada (NSERC) partnered to establish the CSE-NSERC Research Communities grants.

This program is a first of its kind. It provides multi-year funding opportunities to conduct research on cutting-edge technologies in alignment with CSE and Government of Canada priorities. Over a 10-year period, CSE and NSERC will fund 4 research communities, each with a distinct research topic.

The program was launched as part of the CSE Research Initiative, a funding commitment to research investment announced in Budget 2022. This initiative aims to support both classified and unclassified research at CSE.

Learn more about the CSE-NSERC Research Communities grants.[67]

Robust, secure and safe artificial intelligence

In August 2023, CSE and NSERC announced the first call for proposals for the Research Communities grants: Robust, secure and safe artificial intelligence (RSS AI). This first grant aims to:

- generate new knowledge in RSS AI
- enhance the capacities of Canadian universities to undertake research related to RSS AI
- help produce a new generation of data scientists and engineers sensitive to the issues around RSS AI

CSE encouraged proposals that explored **data-centric approaches** to RSS AI. This means research projects that focused on the early stages of the AI process, such as improving data quality.

We received 22 letters of intent from 16 different Canadian universities. The recipient of the grant will be announced in summer 2024.

Academic research

Over the past year, CSE's academic research has not only led to innovation at CSE and within Canada's research community, but it has also had global implications.

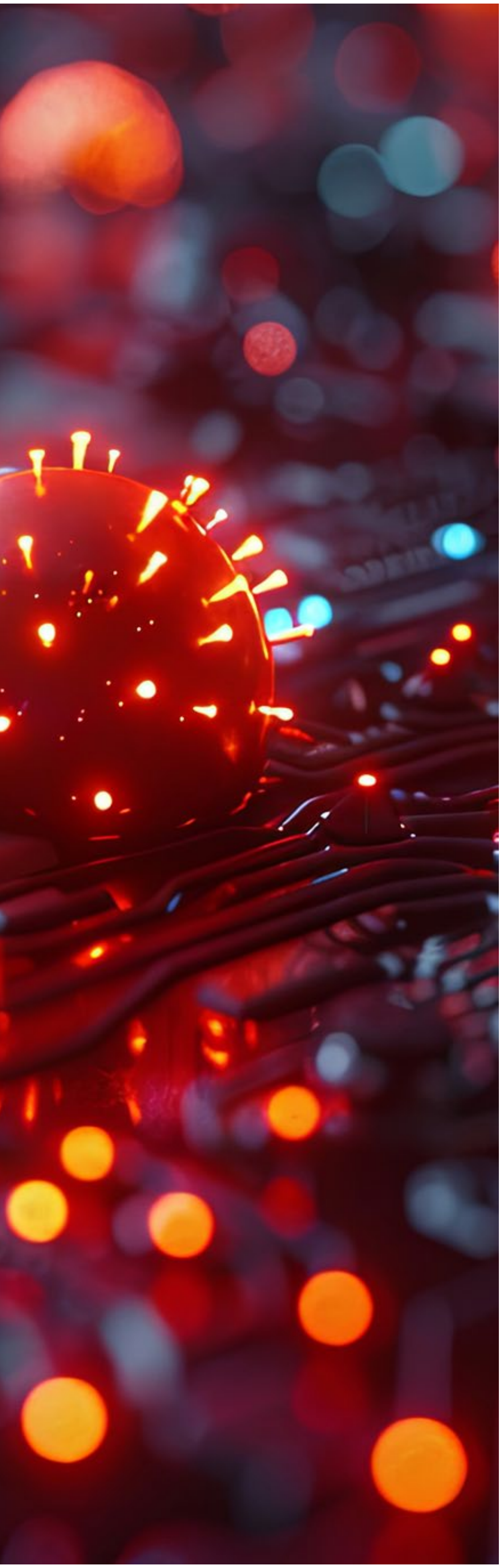
CSE's Tutte Institute for Mathematics and Computing[68] (TIMC) has continued to position itself as a global leader in relational and hypergraph research, which aims to understand and represent the complex structures and relationships of data. Their work in exploratory vector analysis continues to provide broad benefits across a wide range of research within the Canadian security and intelligence community, the Five Eyes and the global scientific community.

TIMC's unclassified external research has had a significant impact on various areas of study, including cancer research, astronomy, neuroscience and social media analysis.

This year, TIMC contributed to the academic community by:

- publishing 14 journal articles
- producing 5 software releases of new or significantly updated code
- releasing 1 book and editing 2 others
- giving 5 invited talks and 7 presentations at external conferences
- organizing 3 special conference sessions
- holding positions on the Canadian Mathematical Society Board and chairing its nominating committee

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



Applied research

This year, the Applied Research[69] team focused on operationalizing new tools and building up internal and external partnerships.

Internally, our researchers worked closely with CSE analysts to support their work and enhance their capabilities. Notably, they transitioned 2 services from research to operations. One is a tool that uses data science techniques to help analysts automate their workflow and analyze data more efficiently. The other is a tool that uses ML to translate classified content into over 100 languages (see AI-powered translation tool). Our researchers continue to support the improvement of our translation tool, working to make it quicker and more accurate.

Externally, our researchers contributed 7 presentations to Five Eyes data science conferences. They also released a technical report in support of the INfluence Campaigns Awareness and Sensemaking (INCAS) program. The goal of INCAS is to develop techniques and tools to help analysts detect, characterize and track geopolitical influence campaigns.

Vulnerability research and management

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 8 vulnerabilities to the affected vendors.

We also expanded our connections into academia by engaging with 2 new universities. For example, in summer 2023, CSE partnered with Concordia University to improve vulnerability research tooling. The work we conducted together led to the discovery of 5 zero-day vulnerabilities which were disclosed to the vendor, Netgear. In February 2024, Netgear published security advisories acknowledging CSE's contributions in finding the vulnerabilities.

Updates to the Equities Management Framework

CSE's vulnerability management process is outlined in our Equities Management Framework[70] (EMF). The EMF allows us to manage discovered vulnerabilities in a way that supports our mission of protecting our country.

The framework was updated this year to account for the evolving cyber landscape and to further ensure that our practices put the security interests of Canada and Canadians first.

The updated framework:

- includes support for foreign cyber operations
- highlights the role of the RCMP and CSIS as official members of the Equities Review Board
- removes a principle that excluded vulnerabilities unique to information systems and technology used exclusively by a foreign entity
- adds environmental scans as a condition for CSE to act on or postpone acting on the disclosure of a vulnerability

Collaborative events

CSE and the Cyber Centre host several events throughout the year to work intensively on problems related to our mission. These workshops are innovation incubators that bring together participants from across Canada and the Five Eyes, academia, industry and the public sector.

GeekWeek 8

GeekWeek 8[71] took place at the Cyber Centre in July 2023. Over the course of 8 days, participants worked on projects meant to tackle some of the most complex cyber security challenges we face.

Some of these projects explored the potential of AI, for example:

- using ML to identify the malicious parts of files
- leveraging AI to analyze large quantities of threat data
- developing a chatbot to help analysts manage cyber incidents

Learn more about GeekWeek.[72]

GeekWeek 8 by the numbers

220 Participants

90 Organizations

24 Projects

Big Dig 13

CSE hosted Big Dig 13 over a 2-week period from November to December 2023.

This classified event brings together participants from the Government of Canada, Canadian industry and international partners to develop new cyber security solutions and capabilities.

This year, teams explored topics such as:

- vulnerability assessments
- threat simulation
- threat intelligence
- phishing
- incident response

Large language models played a prominent role across various projects.

CSE welcomed Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency[73] (CISA), the Cyber Centre's U.S. counterpart, to provide the keynote speech.

Learn more about Big Dig.[74]

Big Dig 13 by the numbers

158 Participants

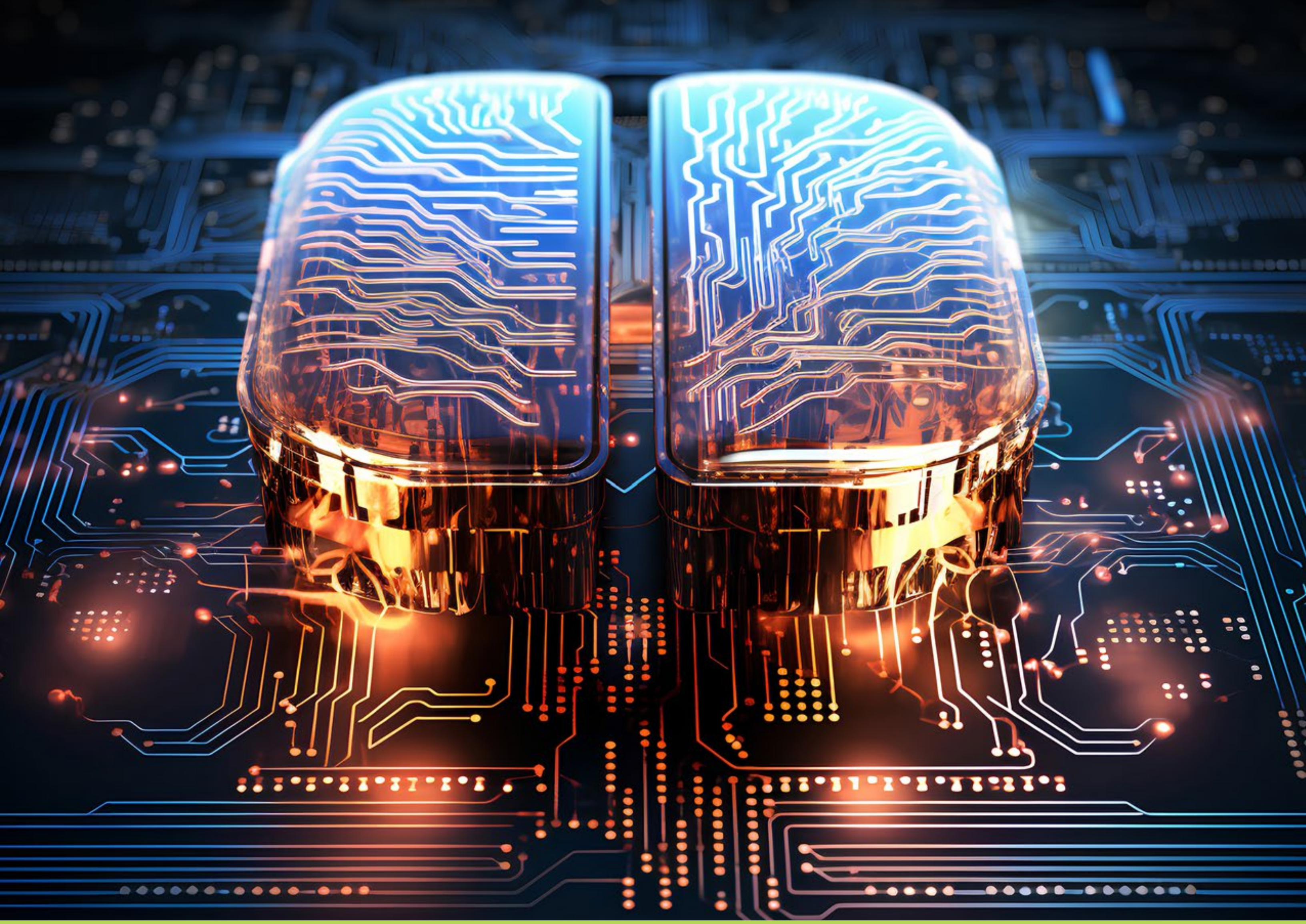
5 Countries

10 Projects

Project Kickstart

Project Kickstart is a classified CSE workshop focused on developing SIGINT tradecraft. Participants from Canada and the Five Eyes use cutting-edge tools to work on SIGINT's most complex problems in a classified environment. This year, participants from diverse areas of expertise succeeded in:

- improving SIGINT and cyber tools
- exploring data science techniques to gain new accesses
- completing big data analytics against key mission objectives



Artificial intelligence

Artificial intelligence is transforming the way Canadians work, live, and access and receive services. For organizations, it provides opportunities to increase productivity and improve services. AI is now being used in various industries across the world and national security is no exception.

At CSE, we have a long history of leading the way in using the latest technologies to support our work and our mission, including with AI. In the coming years, AI has the potential to significantly strengthen our national security by:

- enhancing and complementing our human capabilities
- improving our ability to analyze large amounts of data
- helping us identify emerging threats, allowing us to respond to them more quickly
- automating corporate processes to make them more efficient

While these opportunities will help us better defend Canada, they do present some risks. At CSE and the Cyber Centre, we are committed to building and using AI in an ethical and responsible manner while working to protect Canada from AI-enabled security threats.

Key terms

Artificial intelligence

AI refers to technologies that demonstrate behaviours normally associated with human intelligence, such as learning, reasoning and problem-solving.

Data science

Data science is the process of adapting and analyzing data to gain insights that are helpful for human (or automated) decision-making. Data science makes extensive use of ML to achieve these goals.

Machine learning

ML is a subset of AI that allows machines to learn how to complete a task from given data without explicitly programming a step-by-step solution. ML models can approach or exceed human performance for certain tasks, such as finding patterns in data.

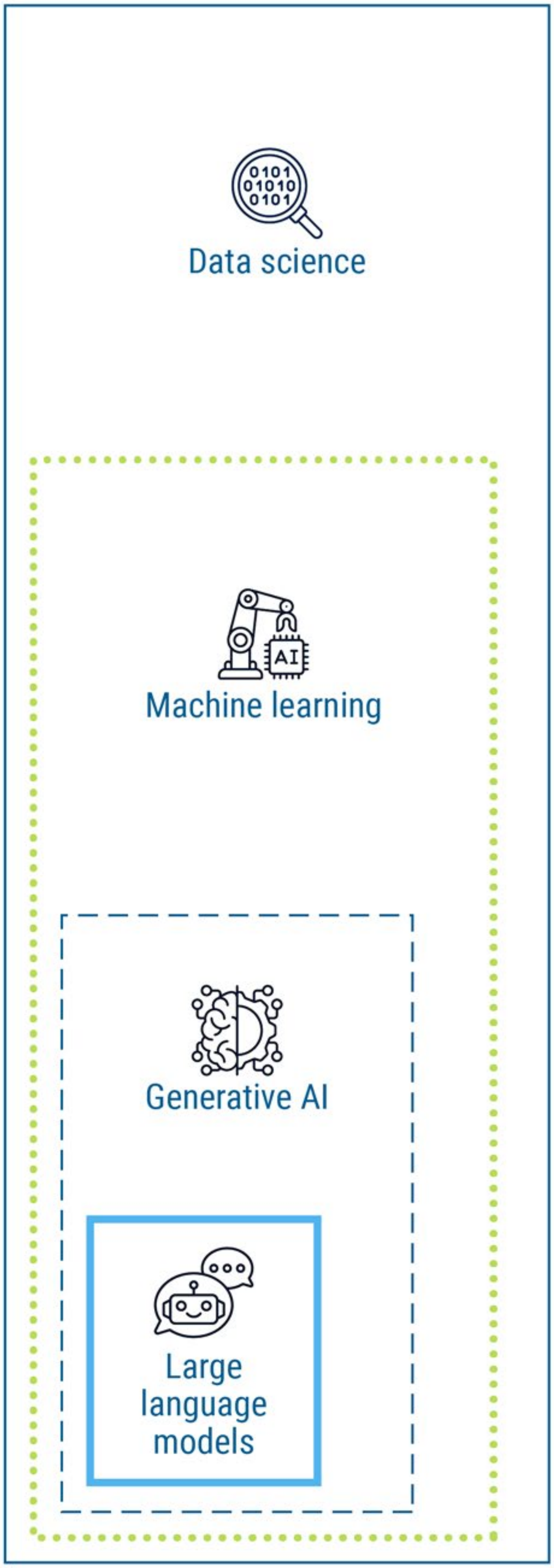
Generative AI

Generative AI is a subset of ML that can generate new content based on large datasets fed into the model. Generative AI can create many forms of content including text, images, audio, video or software code.

Large language models

Large language models (LLMs) are a type of generative AI trained on very large sets of language data that can create human-like language on a given topic from user prompts. OpenAI's ChatGPT and Google's Gemini are well-known examples of LLMs.

Key terms related to AI



Raising awareness of the threats

Over the last 2 years, generative AI has grabbed the world's attention due to its increasing accessibility and its ability to generate synthetic content that is hard to distinguish from human-made content.

This impacts the cyber threat landscape in Canada because threat actors can use generative AI to increase the effectiveness of their activities. For example, threat actors can use LLMs to craft large volumes of phishing emails that are more difficult to detect because they are more varied and more closely resemble human-written emails.

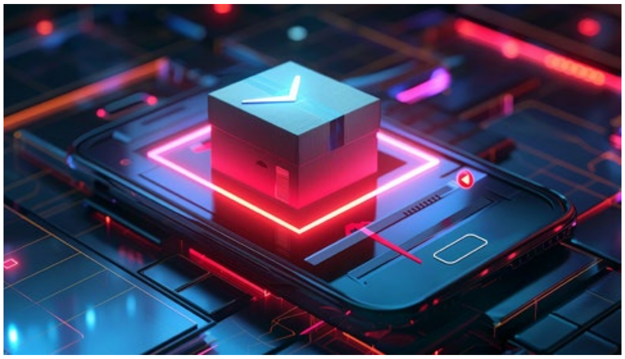
AI and threats to democracy

> **Despite the potential creative benefits of generative AI, its ability to pollute the information ecosystem with disinformation threatens democratic processes worldwide.**
>
> - Cyber Threats to Canada's Democratic Process: 2023 update

The implications of generative AI are particularly concerning when it comes to the democratic process.

The increasing use of generative AI to influence elections is one of the key trends identified in the Cyber Centre's report on Cyber Threats to Canada's Democratic Process: 2023 update.[75]

Threat actors have used generative AI to spread disinformation online by creating deepfake videos of events that never happened. The report predicts that foreign adversaries will likely use generative AI to target Canada's federal election in the next 2 years.



Threats from large language model text generators

In January 2024, the Cyber Centre published a report specifically about the threat from large language model text generators.[76]

This report identified online influence campaigns and email phishing campaigns as likely threats from this type of generative AI. It also outlined additional risks to organizations using LLM text generators, including data security and data governance risks.

Supporting the adoption of secure AI

CSE also produced an educational video on Adopting Artificial Intelligence with Security in Mind.[77] Aimed primarily at Canadian public servants, the video was published by the Canada School of Public Service in March 2024. The video features the heads of several Five Eyes agencies, as well as AI experts from the Government of Canada, industry and academia. The speakers discuss the need to act now to put in place principles-based frameworks that will maximize the potential benefits of AI while keeping safety and security top of mind.

> **AI is an opportunity and a vulnerability.**
>
> - Caroline Xavier, Chief, CSE, Adopting Artificial Intelligence with Security in Mind

Mitigating the risks

As well as raising awareness of the threats AI poses, CSE is working to mitigate them.

In July 2023, the Cyber Centre published guidance for Canadian organizations and individuals on generative artificial intelligence.[78] The document provides a checklist of actions to minimize the risk of being compromised by AI-enabled cyber attacks. An additional checklist offers security measures for organizations to consider when using generative AI tools.

We also published 2 joint endorsements with our international partners this year to provide guidance on the development and use of AI. The publication on Guidelines for secure AI system development[79] was led by our UK partners in collaboration with 17 other countries including Canada. It offers guidelines to develop, deploy and operate AI in a secure and responsible way. In January 2024, we joined Australia and 9 other countries to release Engaging with Artificial Intelligence,[80] a guide on how to use AI systems securely.

In addition to producing guidance for the public, the Cyber Centre:

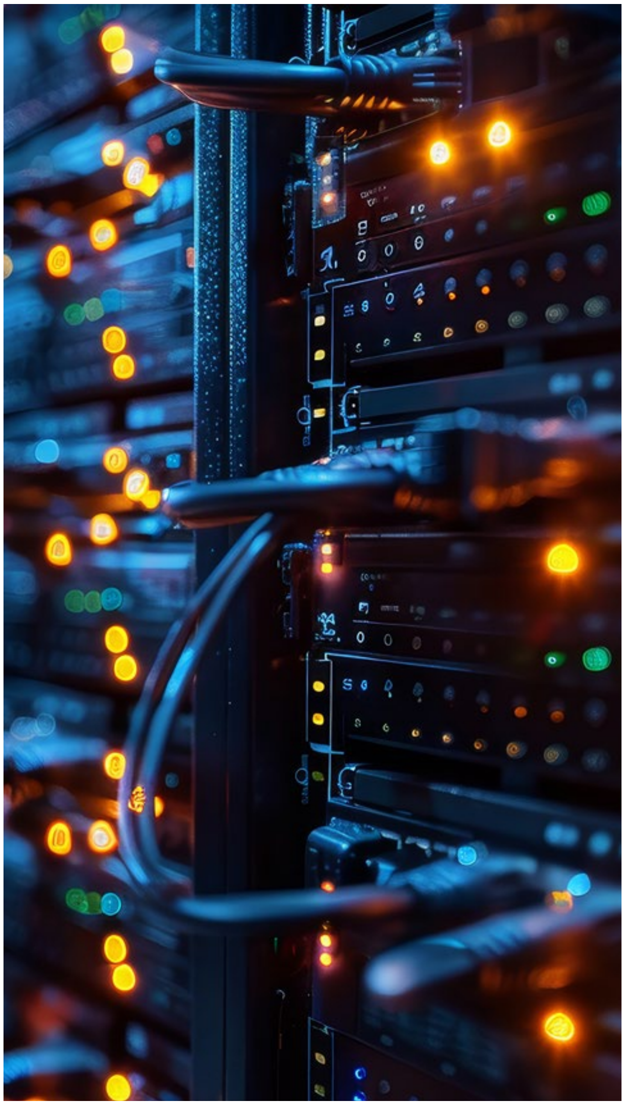
- advised federal partners on how to use AI tools safely within the Government of Canada
- advised critical infrastructure partners on the cyber security risks of AI
- engaged with partners in industry and academia on AI research
- worked with Five Eyes partners to align our activities and advice on AI
- contributed to international efforts to:
  - → develop policies on the safe and responsible use of AI
  - → develop international cyber security standards for AI
- co-hosted an onsite seminar of thought leaders in government, industry and academia to discuss AI with a focus on secure AI design

These lines of effort are not unique to AI. While the emphasis on AI has grown in the last 2 years, working with partners to improve the cyber security of digital technologies has always been a key part of the Cyber Centre's role.

Using AI in CSE's mission

Throughout our history, CSE has used advanced technology to help keep Canada and its allies safe and secure. Data science is almost CSE's core mission. In recent years, this has included the use of AI and machine learning (AI/ML) to help support mission activities.

CSE has some of the most powerful high-performance computers in the country. CSE is using these supercomputers to train new AI/ML models like our AI-powered translation tool. Harnessing the power of AI and ML does not mean removing humans from the process. Our focus is on using data science and ML to enable humans to make better decisions within our rigorous legal frameworks and accountability structures.



AI-powered translation tool

Translation software is a powerful tool, and many versions are freely available online. However, CSE cannot use those tools to translate raw signals intelligence or classified content.

To meet this need, CSE's Research Directorate developed an in-house automated translation tool using ML. Analysts can use the tool to translate content from over 100 languages. CSE SIGINT teams operationalized the tool in late 2022 and made it available to our Five Eyes partners in January 2023.

Results from the first full fiscal year show that the tool has made a valuable contribution to the Five Eyes, receiving over 1 million queries a month from CSE analysts and over 100,000 queries a month from Five Eyes partners.

AI for cyber defence

Much of the Cyber Centre's work to defend federal and critical infrastructure systems from cyber threats involves detecting patterns in vast quantities of data. This is something ML tools are ideally suited to. For example, ML enables the detection of:

- phishing campaigns targeting the Government of Canada
- suspicious cyber activity on federal networks and systems (see Sensors)

The Cyber Centre's Assemblyline[81] tool also uses ML to analyze malicious software. As of this year, this tool now incorporates optional generative AI functions (see Malware analysis).

As threat actors increasingly harness AI to help them avoid detection, ML tools will play a key role in helping our analysts identify and mitigate cyber threats to the Government of Canada and Canadian critical infrastructure.

AI research

The field of AI is evolving rapidly. CSE is conducting both fundamental and applied research to better understand and harness the potential of AI.

Researchers at CSE's TIMC are advancing the foundational data science that underpins AI/ML, including the exploration of unstructured data, and the robust, secure and safe use of AI. Meanwhile, CSE's Applied Research section is exploring applied uses more specific to CSE's mission, such as:

- data triage
- semantic search (finding relevant information based on meaning rather than exact words)

CSE researchers are also working on integrating AI research projects into operational use.

This year, CSE researchers led an exercise to manually evaluate the safety of select open-source LLMs. They used handcrafted prompts to determine whether models would generate malicious responses that could cause harm to individuals. This helped our researchers better understand the baseline safety requirements of these models.

Research partnerships

In addition to conducting our own research, CSE works with federal, academic and industry partners to foster AI innovation and to build our own capabilities.

For example, CSE is currently partnering with industry experts in the field of LLMs to explore ways of using LLM to address CSE's operational needs.

CSE and the NSERC are working together to foster the development of robust, secure and safe AI technologies. Consult the Innovation chapter for more information on the CSE-NSERC Research Communities grants.

To ensure our use of AI remains ethical, we are developing comprehensive approaches to govern, manage and monitor AI and we will continue to draw on best practices and dialogue to ensure our guidance reflects current thinking.

Accountability

CSE's mandate is defined in the *CSE Act*, with clear limits to protect Canadian privacy. CSE monitors its activities internally, while external bodies oversee and review our activities on behalf of Canadians.

External reviews

Like any Government of Canada 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 ensure, 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.

In addition, as part of Canada's national security community, CSE is subject to external review by:

- The National Security and Intelligence Review Agency[82] (NSIRA)
- The National Security and Intelligence Committee of Parliamentarians[83] (NSICOP)

These bodies publish unclassified reports of their reviews online to promote public transparency. They also submit classified reports to Ministers and the Prime Minister to ensure they have a full picture of what the reviews unveiled.

CSE actively supports external reviews by briefing review staff, answering questions and providing access to classified and unclassified materials. Beginning in March 2023, CSE and NSIRA piloted a new solution that grants NSIRA independent direct access to CSE's official classified corporate repository. The pilot was renewed in September 2023 and is ongoing.

External review statistics

This fiscal year, CSE:

- contributed to 26 external reviews and reports
- gave 31 briefings to review bodies
- answered 317 questions

CSE answered 96% of questions by the requested due date, a significant increase from last year.

Reviews into foreign interference

Of the 26 external reviews CSE supported this fiscal year, 4 were reviews into foreign interference in Canada's federal elections. These reviews were conducted by NSIRA, NSICOP, the Independent Special Rapporteur[84] (ISR) and the Foreign Interference Commission.[85]

The Foreign Interference Commission was appointed in September 2023 to conduct a Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (PIFI). CSE provided Commission staff with briefings, access to all requested documents and secure office space to examine and discuss classified material. In addition, CSE provided technical support including secure phones, desktops and videoconferencing as well as access to the CTSN. CSE representatives testified before the Commission in both *in camera* and public hearings from January to April 2024.

CSE provided the Commission with 2 Institutional Reports (1 classified, 1 unclassified) summarizing CSE's mandate and activities to combat foreign interference. The unclassified version of CSE's Institutional Report[86] is available on the Commission's website.

CSE recognizes the important role that external reviews play in ensuring accountability and promoting transparency with respect to foreign interference. As stated in our threat reporting, foreign states increasingly use cyber tools to interfere in democratic processes around the world, with over a quarter of national elections targeted worldwide.[87] Canada must have a clear view of the realities of foreign interference and must ensure its democratic processes are as resilient as they can be. CSE's mandate is key to both those needs, and we are working hard to meet them (see the chapter on Hostile state activity and foreign interference).

As always, CSE welcomes external review and advice on how we can carry out our mandate more effectively. CSE will give thoughtful consideration to any recommendations and take action as appropriate.

Ministerial Authorizations

Under the *CSE Act*,[88] certain activities must be authorized by the Minister of National Defence. There are different authorizations for the different aspects of CSE's mandate.

Foreign Intelligence and Cybersecurity Authorizations

Before conducting any activities under a Foreign Intelligence Authorization or Cybersecurity Authorization, CSE must receive approval from the Intelligence Commissioner, who performs an independent, quasi-judicial oversight function.

In 2023, CSE submitted 6 authorizations to the Intelligence Commissioner,[89] 3 of which were fully approved and 3 of which were partially approved:

- Cybersecurity Authorizations to help protect federal institutions
  → Submitted: 1
  → Fully approved: 1
- Cybersecurity Authorizations to help protect non-federal institutions
  → Submitted: 2
  → Fully approved: 2
- Foreign Intelligence Authorizations
  → Submitted: 3
  → Partially approved: 3

For the partial approvals, the Intelligence Commissioner removed one clause meant to cover enabling activities for foreign intelligence activities. The Intelligence Commissioner concluded there were not enough details to explain what would be covered by the clause.

Foreign cyber operations authorizations

The number of authorizations for foreign cyber operations in 2023 remained the same as the previous year.

- Active Cyber Operations Authorizations: 3
- Defensive Cyber Operations Authorizations: 1

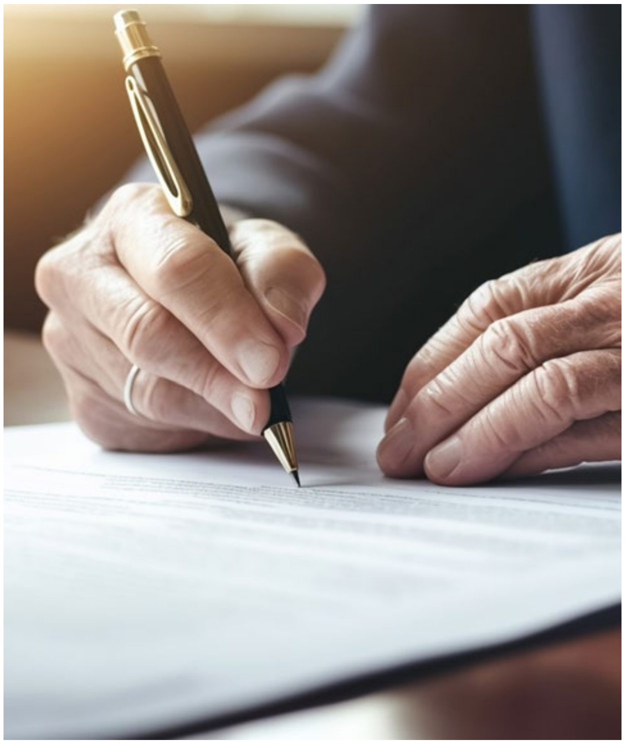
Authorizations are valid for 1 year and may include multiple operations or none. The chapter on foreign cyber operations contains more information on the types of operations CSE has conducted.

Ministerial Orders

The Minister of National Defence signs Ministerial Orders (MOs) to designate people or organizations with whom CSE can work or share information. As of March 31, 2024, CSE had 5 MOs in effect:

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

The only MO signed this year was the order designating recipients of information under CSE's cyber security mandate. Signed in June 2023, it replaced a previous MO serving the same purpose.



Disclosures of Canadian identifying information*

CSE is prohibited from directing its activities at Canadians or persons in Canada. However, it may incidentally acquire information related to Canadians or persons in Canada in the course of legitimate foreign intelligence activities. CSE obfuscates or removes all Canadian identifying information (CII) from its intelligence reports. However, agencies and departments designated by MO may request a disclosure of CII under certain conditions.[90] CSE reviews each request on a case-by-case basis.

In 2023, CSE received 1,087 disclosure requests, just over 1.5 times as many as in 2022. Just over 13% of requests were from Five Eyes agencies. Overall, CSE approved 69% of requests to disclose CII.

- Outcomes of CII disclosure requests in 2023
  - → Approved: 69%
  - → Denied: 16%
  - → Cancelled: 15%
  - → In progress: 0%

* The numbers in this section were corrected on January 24, 2025.

Internal compliance

CSE's compliance team is responsible for ensuring that CSE employees follow internal policies in the course of their work. All CSE's internal compliance findings are available for review by external review bodies.

This fiscal year, CSE's compliance team conducted:

- 15 assessments
- 6 studies
- 2 spot checks

In February 2024, CSE hosted a compliance conference with Five Eyes partners to exchange best practices and discuss common challenges.

Other activities included:

- revising CSE's compliance testing for employees
- holding CSE's annual Operational Compliance Week

Compliance incidents

Despite CSE's best efforts to avoid them, mistakes do happen. Any occurrence that does not comply with CSE's internal policies is considered a compliance incident. If the incident involves information relating to a Canadian or person in Canada it is logged as an "operational privacy incident." Examples include keeping data beyond its standard retention date or inadvertently sharing CII in a foreign intelligence report. If the incident involves a Five Eyes partner, it is recorded as a "second party privacy incident."

In 2023, CSE's compliance team identified:

- 104 operational privacy incidents
- 35 second party privacy incidents

In each case, CSE assesses what happened, mitigates any impacts (for example by deleting the data or recalling the report) and seeks to address the root cause.

Complaints

In January 2024, CSE updated its process to make it easier for members of the public to submit a complaint[91] directly through the CSE website. In the past, this could only be done by mail. Although that option remains, the new online submission tool is faster and more accessible. It also helps to ensure the complaint is not missing key information needed to conduct a proper investigation. This should help CSE to meet its target of responding to all complaints within 60 days.

This fiscal year, CSE received 10 external complaints directed to the Chief of CSE and responded to 5 complaints sent to NSIRA regarding CSE activities.

Transparency

This report is just one of the ways that CSE shares information with Canadians. This fiscal year, CSE continued to promote transparency about its activities through:

- speeches, conferences and public events
- 6 parliamentary appearances
- 4 public reports[92]
- 55 media interviews
- 4 news conferences
- 52 Open Government[93] releases
- 32 Access to Information[94] responses
- 12 proactive disclosures[95]
- 110 Order Paper question[96] responses
- 5,580 social media posts

Audit, evaluation and ethics

Every Government of Canada department must assess its activities to make sure they comply with policy (audit) and make responsible use of resources (evaluation).

CSE's audit and evaluation teams provide impartial, evidence-based advice directly to senior leadership to help CSE achieve its strategic objectives. This year, CSE completed 2 audits and 2 program evaluations to improve the effectiveness and efficiency of CSE's operational activities. CSE's internal audits are subject to external review to make sure they are independent and up to standard.

The ethics[97] team continued to provide training and advice on a broad range of matters from potential conflicts of interest for employees to the ethical considerations of mission activities.

In addition, CSE marked the 10th anniversary of the CSE Ethics Charter[98] with a week-long series of events including learning activities and a guest speaker on AI and ethics.

Task team on values and ethics

In September 2023, CSE Chief Caroline Xavier was one of 5 Deputy Ministers tasked with renewing the dialogue on how public servants live out their values and ethics in a rapidly changing world. The task team held around 90 conversations with individuals, groups and communities across the public service and delivered its Prologue Report[99] in December.

> **Our report to the Clerk is the beginning of the conversation, not the end.**
>
> - **Deputy Ministers' Task Team on Values and Ethics, Prologue Report**

Many CSE employees took part in these initial conversations. Their feedback included the need for scenario-based ethics training and clearer guidance on personal social media use.

Employees also raised the need for the CSE Ethics Charter to reflect more explicitly our organization's values around respect for people. These include accessibility, anti-racism, equity, inclusion and reconciliation.

In response, CSE began the process of reviewing the Ethics Charter and updating its ethics training. This work will continue into next fiscal year, in partnership with CSE employees and affinity groups.

People

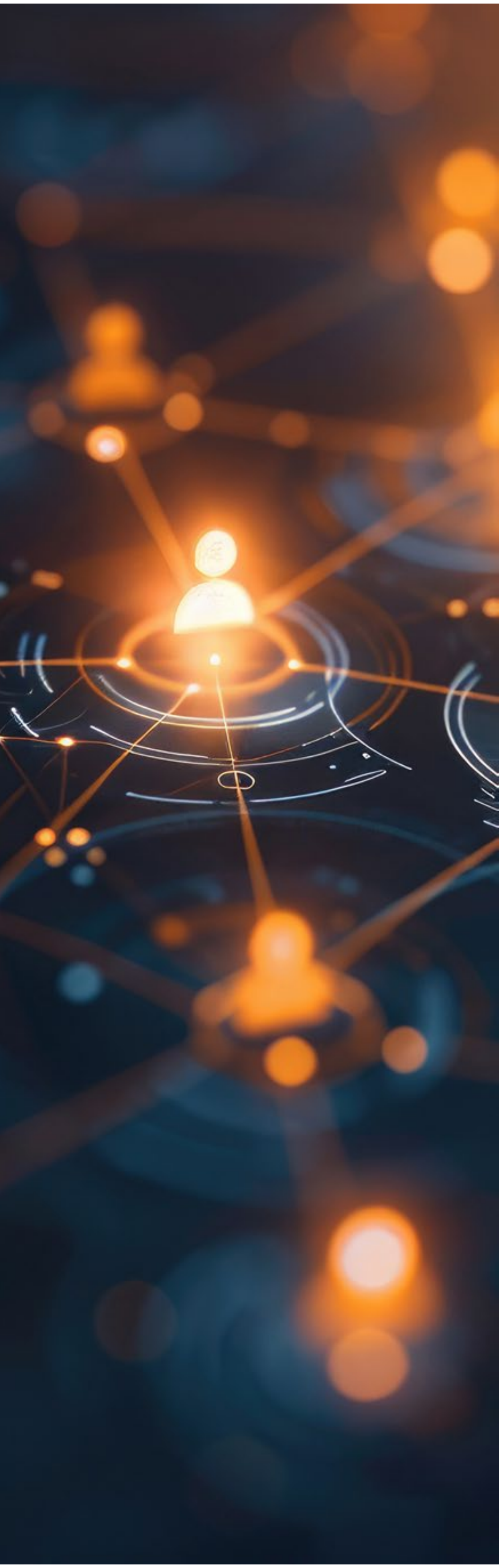
At CSE, our people are our greatest strength. Our workforce is made up of dedicated individuals who draw from their unique backgrounds and experiences to protect our country, 24/7.

Over the past year, we've engaged in various activities to reach potential candidates, bring in new employees and support our growing community.

Recruitment

This year, CSE redoubled its efforts to attract and hire the people we need to carry out our mission effectively and fulfill growing demands.

We hired approximately 465 full-time, permanent employees. CSE's total workforce is now 3,529, up by 9%.



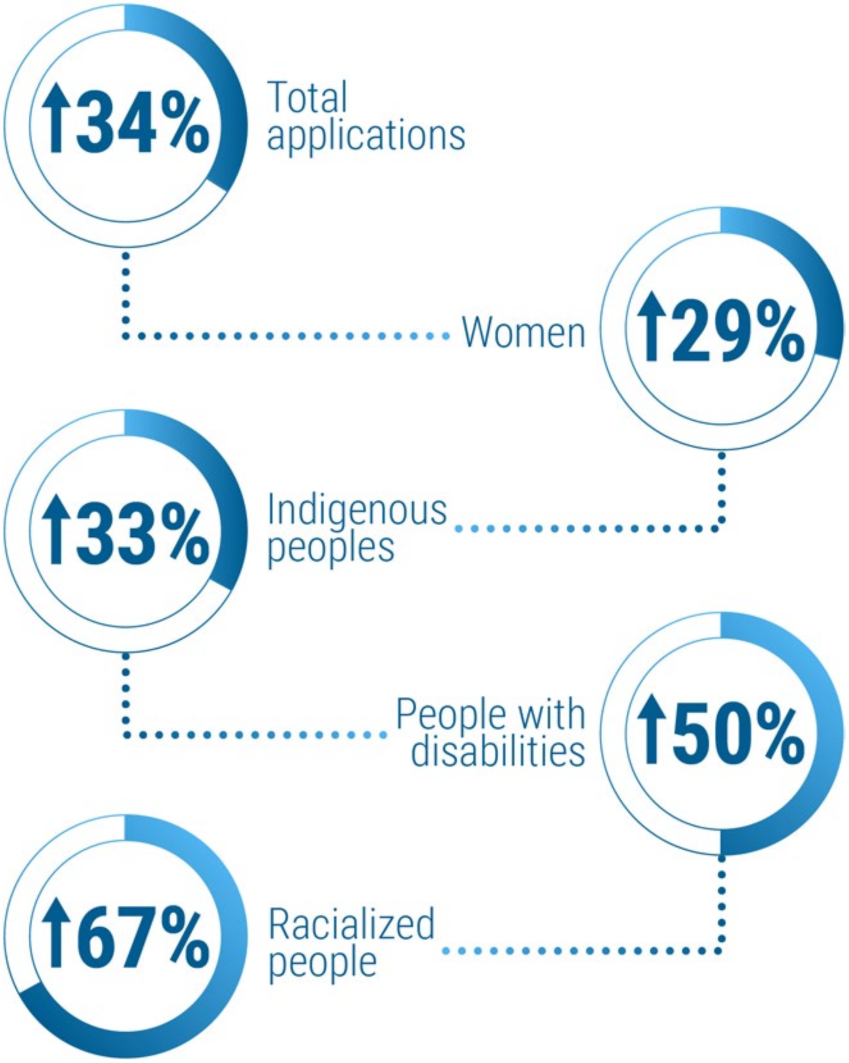
Recruitment activities

CSE’s candidate outreach team travelled across the country to participate in over 160 events, including career fairs, hackathons, information sessions and networking events. Nearly 1 in 7 events was entirely in French and one third of the events had an equity, diversity and inclusion focus, catering specifically to jobseekers from underrepresented communities.

Additionally, CSE leveraged specific job boards to further attract racialized and Indigenous applicants and ran 2 advertising campaigns to reach more potential candidates. We also conducted reviews of our job posters to ensure the use of plain, inclusive language, making them as bias-free as possible.

Our efforts have resulted in a major increase in applications across the board and particularly from many equity-seeking groups.

CSE applications 2023 to 2024[100]



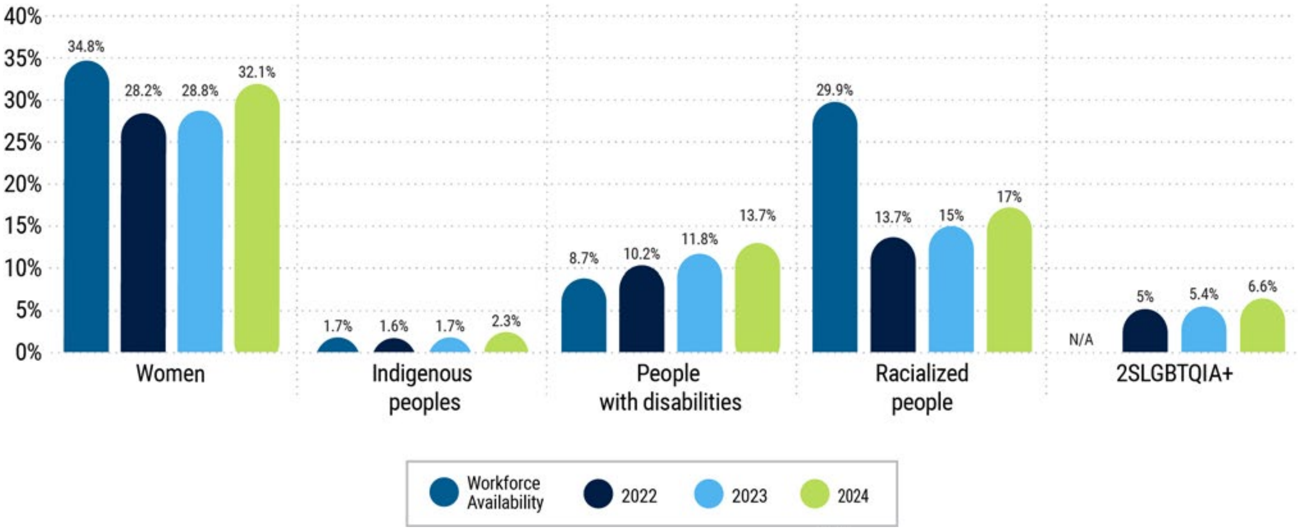
Building a representative workforce

CSE strives to build a workforce that reflects the different communities we protect. Increasing representation at all levels in the organization is a top priority.

As mentioned, we dedicated significant efforts this year towards increasing our representation of equity-seeking groups. And those efforts are having a clear impact.

Our latest numbers show that diversity continues to increase at CSE. Our representation of Indigenous employees and employees with disabilities is higher than their workforce availability. However, women and racialized employees remain underrepresented. We're committed to changing this and will continue to work towards attracting and retaining applicants from these communities through various tailored programs.

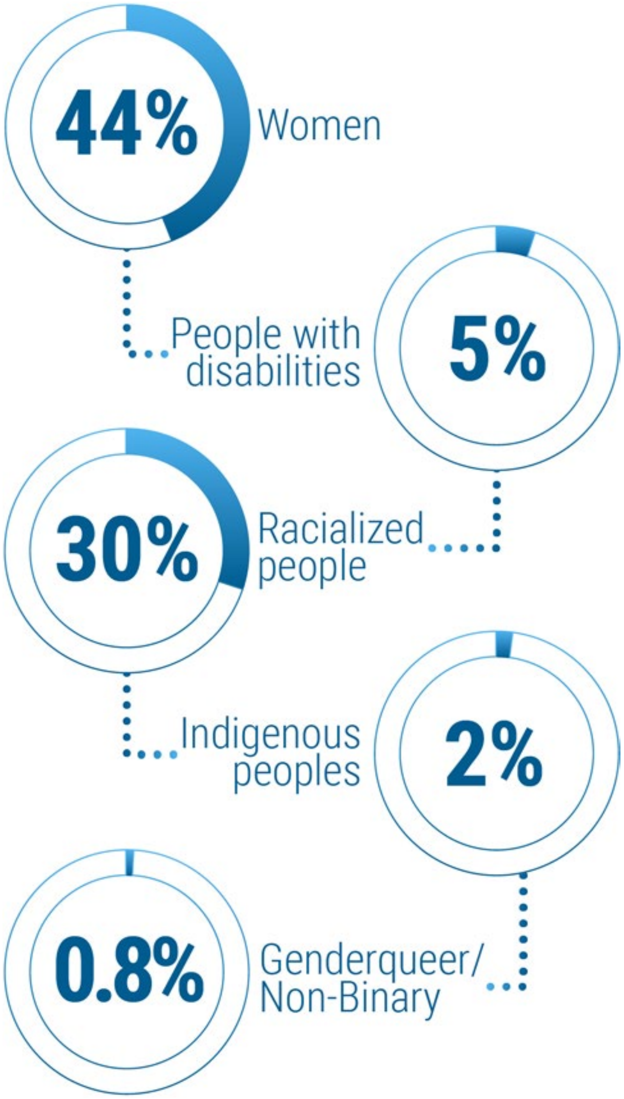
Workforce demographics at CSE from 2022 to 2024[101] [102]



Self-declaration of new hires

For the first time, CSE was able to gather significant self-declaration data from new hires, which provided us with valuable insights. The data shows that we hired women, Indigenous applicants and racialized applicants above par with workforce availability.

Rates of hire 2023 to 2024[103]



CSE recognizes the importance of data as a tool to help us grow and expand the representation of our workforce. We are making efforts to improve our external and internal data collection, allowing for disaggregated data analysis, and enhance our reporting. These initiatives will help us assess where we are today, inform our plans and track our efforts.

Hybrid workplace

Following a successful pilot, CSE officially adopted a hybrid work model in April 2023, with most of our employees working onsite at least 3 days a week. We remain committed to ensuring the success of our hybrid work model and offering flexible work arrangements to support our employees and the future growth of our workforce.

Employees whose work is classified in support of CSE's mission continue to work onsite full time.

Security process

Over the past year, CSE's Security team continued its consultations with internal partners including employee affinity groups. The purpose of these consultations is to find ways to make our security process more inclusive and transparent, while maintaining its integrity.

These efforts led to the approval of two key changes to CSE's external hiring and clearance processes in September 2023.

Exemptions to the Canadian residency requirement

Previously, CSE required all candidates to have 10 years of residency to be considered for an Enhanced Top Secret clearance. Under our new policy, CSE'S Chief Security Officer may grant exemptions for external candidates when the risk can be mitigated given other practices already in place. This change aims to break down some of the systemic barriers impacting members of underrepresented groups, facilitating the recruitment of more diverse and skilled applicants.

Formal policy concerning illegal drug use

CSE has now made it explicit (on our website and in related forms and documents) that candidates must abstain from illegal drug use or misuse of prescription drugs for at least one year ahead of applying to CSE. This should also be maintained during the assessment and clearance process. This change aims to improve the transparency of our security process by clearly outlining our expectations on this topic.

Equity, diversity and inclusion

Since the launch of One CSE: A Framework for Equity, Diversity and Inclusion (EDI),[104] CSE has continued to define what EDI means to us and has found new ways to make our workplace better for everyone.

One CSE: The Collection

On the anniversary of our EDI Framework in June 2023, we took our efforts one step further and launched One CSE: The Collection.

One CSE: The Collection is a CSE-wide initiative that encourages all employees to be active supporters of EDI in our workplace. This virtual game takes the core principles and strategic elements found in the framework and introduces them as "cards" employees can play to earn points for their business line. The cards present tangible examples of actions employees can take to integrate EDI into our organization's work and culture.

To date, nearly one quarter of CSE employees have participated in the game and all cards in the deck have been played at least once.

Examples of One CSE: The Collection cards

The Golden Bee
Creature — Industrious
Type
Standard
Effort
8
Skill
10
Impact
80
CSE | CST
One CSE — The Collection

Play this card when you have made a significant effort to support the EDI Journey of your branch.

"I have a contribution to make." — Lauren Bacall

Golden Bee

Can be played by someone who contributed to the EDI mission of their business line

Treasure Chest
Artifact — Tools
Type
Standard
Effort
8
Skill
10
Impact
80
CSE | CST
One CSE — The Collection

Play this card when you have developed a tool or resource that promotes equity, diversity, and inclusion within CSE.

Treasure Chest

Can be played by someone who developed a tool or resource that promotes equity, diversity and inclusion within CSE

Showupa, The Attender
Creature — Engaged
Type
Standard
Effort
5
Skill
2
Impact
10
CSE | CST
One CSE — The Collection

Play this card when you have attended an event hosted by an Affinity Group.

"Showing up is like 90% of the battle and just make sure your hair is really cute." — Willam Belli

Showupa, The Attender

Can be played by someone who attended an event hosted by an affinity group

Microaffirmer
Instant — Warmth
Type
Standard
Effort
3
Skill
7
Impact
21
CSE | CST
One CSE — The Collection

Play this card to recognize someone who has made one or many small or subtle gestures or acts of inclusion that indicates they value and have respect for you.

"A person's a person, no matter how small." — Dr. Seuss

Microaffirmer

Can be played to recognize someone who has made one or many small or subtle gestures or acts of inclusion

Five Eyes Equity, Diversity and Inclusion Summit

In March 2024, CSE hosted the first-ever Five Eyes EDI Summit at our headquarters in Ottawa. We welcomed 113 participants, including delegates from our partner organizations in Australia, the UK and the U.S.

The summit provided an opportunity for participants to work together on 5 main surge topics:

- building confidence and reinforcing allyship in leaders
- addressing recruitment and retention barriers
- supporting safe spaces
- promoting inclusive excellence in the mission space
- integrating EDI considerations into organizational processes

The summit also included guest speakers and panels on various themes, including Indigenous issues in Canada, accessibility, EDI and the mission, and allyship.

The outcome of the summit was a comprehensive set of recommendations, ideas, shared best practices and strategic goals that will inform our collective way forward and help us foster meaningful partnerships across the Five Eyes.

Reconciliation with Indigenous Peoples

At CSE, we have a responsibility towards reconciliation with Indigenous peoples in keeping with the Truth and Reconciliation Commission's Calls to Action.[105] It is a core principle of our EDI Framework and one we are working hard to promote.

To support our commitment, this year CSE:

- purchased 6 pieces of art from Indigenous artists and hung them prominently next to a permanent land acknowledgement at the Edward Drake Building
- hosted events to educate our workforce about the experience and culture of Indigenous peoples and the Calls to Action
- hired our first employee through the IT Apprenticeship Program for Indigenous Peoples[106]
- launched a hiring process for an Indigenous Career Navigator, in partnership with the Knowledge Circle for Indigenous Inclusion[107]
- awarded more than 5% of the total value of our procurement contracts to Indigenous businesses (exceeding the *TBS Directive on Management of Procurement* requirement)
- worked with Indigenous leaders and communities through its Cyber Centre to promote cyber resilience

Sponsorship pilot program

CSE's sponsorship pilot program concluded in March 2024. Over the past year, the 15 participants (or protégés) from Black, Indigenous or racialized communities had the opportunity to:

- build relationships with their sponsors
- receive coaching
- explore ways to advance their career goals

At the end of the pilot, more than half of the protégés met their program objectives. These included a combination of promotions, lateral moves and access to official language training that will allow them to take the next step in their careers. CSE is now exploring ways to establish sponsorship as a corporate initiative and expand the program to other communities.

> **“The Sponsorship Program came at a time where I started to lose heart. I didn't feel that I would progress in my career because, despite my competencies and work experience, I didn't have anyone with authority advocating for me. The program not only provided me with new opportunities and greater exposure, but it also introduced me to a sponsor who really cares about who I am as a person and how I want to progress in my career. This has been incredibly valuable for me as a marginalized woman and I'm grateful for the opportunity.”**
>
> \- Nora (she/her), CSE employee and sponsorship program participant

> **“People ask me why I do this and it's because other people have done so much for me in my career, I want to pay it forward. To sit across the table from people who have such compelling stories, who have faced so many barriers, and to see the ideas they have and the energy they bring… What a rewarding experience! You're giving back, but you get so much in return.”**
>
> \- Darrell Schroer (he/him), Executive Champion of CSE's sponsorship pilot and sponsor

Improving accessibility at CSE

In December 2023, we released the CSE Accessibility Plan Progress Report 2023.[108]

We published this report in line with our commitments outlined in the CSE Accessibility Plan 2022–2025.[109] It aims to highlight efforts made in the past year to identify and remove barriers to accessibility and inclusion.

This is the first of many. CSE will continue to work to design spaces, tools, systems and processes that leave no employee behind.

New affinity groups

CSE's affinity groups are critical to our EDI efforts and serve as strong advocates for our various communities. This year, we welcomed the creation of 5 new affinity groups:

- Audible Minorities Affinity Group
- Black Employee Circle (BEC)
- Code Talkers Circle (Indigenous affinity group)
- Middle East and North Africa (MENA) group
- Muslim Affinity Group

These groups provide safe spaces for employees to share their lived experiences and to be involved in shaping policies and initiatives at CSE. Throughout the year, they organized various events to raise awareness of their realities and promoted inclusion in the workplace.

Learn more about affinity groups.[110]

EDI events and commemorations

Throughout the year, CSE hosted 28 events and commemorations to raise awareness of EDI topics and recognize important days. Our affinity groups led and organized many of these events, often working with partners both here and abroad to reach a wider audience.

Types of events and commemorations hosted in 2023 to 2024

6	7	4	11
Guest speakers	Panels	Joint events	Other special events

Citizenship ceremony

In October 2023, CSE, alongside Immigration, Refugees and Citizenship Canada hosted a citizenship ceremony at our Vanier facility where 45 new Canadians, coming from 14 different countries, took the oath of citizenship. The Minister of National Defence gave a speech, officially welcoming the new citizens to Canada. This event was the first time that members of the public, not directly linked to our work, were invited onto CSE premises, and it marked an important milestone in our efforts to be a more open, inclusive and transparent organization.

New inclusive washroom

In January 2024, CSE opened its first inclusive washroom at the Edward Drake Building. The existing space was upgraded to include floor to ceiling stalls, private mirrors and inclusive signage. By implementing an inclusive washroom at its headquarters, CSE is making an important step towards creating more welcoming spaces for all employees.

> **“This impacts the transgender and non-binary community the most. From our perspective, we can freely use such washrooms without worry of being challenged, and potentially outed, as with older restroom frameworks.”**
>
> \- Member of CSE's Pride Network

Official languages

CSE continued to promote linguistic duality and official languages (OL) in the workplace through several initiatives, including:

- sharing OL best practices with employees
- providing training for new supervisors on their OL obligations
- adding OL expectations to performance agreements for all employees
- reviewing all linguistic identifications of positions for accuracy and compliance
- supporting the activities of the Réseau Franco affinity group

This year, CSE’s in-house linguistic services translated over 3.1 million words, ensuring that all our communications and reporting met OL requirements. One CSE: The Collection features 3 official languages cards to encourage employees to use their second official language day-to-day.

Employee wellbeing

CSE's Employee and Organizational Wellness program provides employees and leaders with the support and resources they need to thrive.

New mental health strategy

In 2023 to 2024, CSE created a multi-year plan focused on fostering employee mental health and organizational wellness. The plan outlines a series of objectives and activities that will continue to be refined in the coming year.

This year, CSE also implemented initiatives focused on:

- raising awareness
- supporting employees to take care of their mental health
- delivering mental health training to leaders

Our Career Services team continued to provide psychometric development and coaching programs to our employees and leaders. This included a program on emotional intelligence, which plays a crucial role in enhancing self-awareness and understanding others.

Harassment and violence prevention

This year, the Harassment and Violence Prevention Program launched several initiatives to support employee wellbeing, including:

- establishing guidelines for addressing domestic violence in the workplace
- developing a harassment and violence prevention toolkit for managers
- offering training on bystander intervention in the workplace to all employees

Grounding and processing space

The nature of the work we do at CSE exposes certain employees to material and images that can be hard to manage and process. To help these employees maintain positive mental health and performance, CSE created a grounding and processing space at its headquarters in the Edward Drake Building.

In this space, employees have access to tools, resources and activities shown to help mitigate the impacts of disturbing material. It's a safe place where employees can disconnect from their workstations, recharge and decompress.

Top Employer Awards

CSE was proud to be recognized once again as one of Canada's Top Employers for Young People[111] (2024) and named one of the National Capital Region's Top Employers[112] (2024).

NATIONAL CAPITAL REGION'S TOP EMPLOYERS
LES MEILLEURS EMPLOYEURS DE LA RÉGION DE LA CAPITALE
2024
®

Key numbers

Over the 2023 to 2024 fiscal year, CSE:

- produced 3,142 foreign intelligence reports
- disclosed 8 vulnerabilities to affected vendors
- approved 43 requests for assistance from federal partners
- contributed to 26 external reviews and reports
- responded to 96% of review questions by the due date
- translated 3 Get Cyber Safe infographics into 4 Indigenous languages
- shared 5,580 social media posts
- grew our workforce by 9%

The Cyber Centre:

- blocked 6.6 billion potentially malicious actions a day
- mitigated almost 300,000 malicious domains
- engaged with almost 1,900 Canadian critical infrastructure organizations
- analyzed over 1 billion suspicious files for malware
- shared 84 unique indicators of compromise a day
- helped respond to 2,192 cyber incidents
- used sensors to help protect the networks of 3 out of 4 federal institutions
- issued:
  - → 4 threat assessments
  - → 34 new cyber security guidance publications
  - → 40 new Get Cyber Safe resources
  - → 250 pre-ransomware notifications
  - → 779 advisories
  - → 20 alerts
  - → 10 cyber flashes

Endnotes

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

2 CSE's total authorities for 2023 to 2024 were $1,039,192,674.

3 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

4 https://www.canada.ca/en/democratic-institutions/services/reports/first-report-david-johnston-independent-special-rapporteur-foreign-interference.html

5 As defined by the National Security and Intelligence Committee of Parliamentarians (NSICOP) in its 2022 Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack. https://nsicop-cpsnr.ca/reports/rp-2022-02-14/07-en-part-5.html#nsic-s7-2

6 https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector

7 https://www.cga.ca/cyber-security/

8 https://www.cga.ca/e-stac/

9 Department of National Defence, Remarks by Minister Anand at CANSEC 2023, June 5, 2023. https://www.canada.ca/en/department-national-defence/news/2023/06/remarks-from-minister-anand-at-cansec-2023.html

10 https://cybercentrecanada.github.io/assemblyline4_docs/

11 https://www.cyber.gc.ca/en/tools-services/howler

12 https://www.cyber.gc.ca/en/glossary#c

13 https://www.cyber.gc.ca/en/news-events

14 https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-International-Partnerships.pdf

15 https://www.first.org/conference/2023/

16 https://www.cyber.gc.ca/en/education-community/learning-hub

17 https://www.cyber.gc.ca/en/education-community/learning-hub/courses/623-introduction-cyber-security-educators

18 https://www.cyber.gc.ca/en/education-community/learning-hub/courses/625-cyber-security-small-medium-organizations

19 https://www.cyber.gc.ca/en/education-community/learning-hub/courses/107-cyber-security-fundamentals

20 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

21 Democratic Institutions, Security and Intelligence Threats To Elections Task Force – Reports and publications, 2024. https://www.canada.ca/en/democratic-institutions/services/reports.html

22 CSIS, Foreign Interference Threats to Canada's Democratic Process, 2021. https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html

23 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024#a10

24 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update#generative_ai

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

26 https://www.canada.ca/en/campaign/online-disinformation.html#1

27 Canadian Centre for Cyber Security, National Cyber Threat Assessment 2023-2024, October 2023. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

28 https://www.cyber.gc.ca/en/news-events/advisory-peoples-republic-china-state-sponsored-cyber-threat

29 https://www.cyber.gc.ca/en/news-events/joint-advisory-prc-state-sponsored-actors-compromising-and-maintaining-persistent-access-us-critical-infrastructure-and-joint-guidance-identifying-and-mitigating-living-land-0

30 https://www.cyber.gc.ca/en/news-events/joint-guidance-executives-and-leaders-critical-infrastructure-organizations-protecting-infrastructure-and-essential-functions-against-prc-cyber-activity

31 https://www.canada.ca/en/communications-security/news/2023/04/statement-from-the-minister-of-national-defence--cyber-threats-to-critical-infrastructure.html

32 https://www.cse-cst.gc.ca/en/information-and-resources/announcements/cse-urging-canadian-cyber-security-community-adopt-heightened-state-vigilance

33 https://www.cyber.gc.ca/en/news-events/cse-urges-canadian-cyber-security-community-be-vigilant-two-year-mark-russias-full-scale-invasion-ukraine

34 https://www.cse-cst.gc.ca/en/information-and-resources/news/joint-cyber-security-advisory-warns-spear-phishing-campaigns-against-targets-interest-worldwide

35 https://www.cyber.gc.ca/en/news-events/joint-cyber-security-advisory-warns-russian-state-actors-are-adapting-their-tactics-access-cloud-infrastructure

36 https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/policy-sensitive-technology-research-and-affiliations-concern

37 Crown-Indigenous Relations and Norther Affairs Canada, Arctic and Northern Policy Framework: Safety, security, and defence chapter, September 2019. https://www.rcaanc-cirnac.gc.ca/eng/1562939617400/1562939658000

38 Department of National Defence, Statement from the Canadian Armed Forces Regarding Unsafe Intercept of Royal Canadian Air Force Helicopter, November 3, 2023. https://www.canada.ca/en/department-national-defence/news/2023/11/statement-from-the-canadian-armed-forces-regarding-unsafe-intercept-of-royal-canadian-air-force-helicopter.html

39 Canadian Centre for Cyber Security, Joint advisory on PRC state-sponsored actors compromising and maintaining persistent access to U.S. critical infrastructure and joint guidance on identifying and mitigating living off the land, February 7, 2024. https://www.cyber.gc.ca/en/news-events/joint-advisory-prc-state-sponsored-actors-compromising-and-maintaining-persistent-access-us-critical-infrastructure-and-joint-guidance-identifying-and-mitigating-living-land-0

40 Global Affairs Canada, Statement on actions taken by People's Republic of China against Philippines vessels in South China Sea, December 12, 2023. https://www.canada.ca/en/global-affairs/news/2023/12/statement-on-actions-taken-by-peoples-republic-of-china-against-philippines-vessels-in-south-china-sea0.html

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

42 Palo Alto Networks. "2023 Palo Alto Networks Canada Ransomware Barometer." December 7, 2023. https://www.paloaltonetworks.com/content/dam/CF/Canada%20Ransomware%20Whitepaper%202023.pdf

43 Canadian Centre for Cyber Security, Baseline cyber threat assessment: Cybercrime, August 28, 2023. https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime

44 https://www.cyber.gc.ca/en/contact-cyber-centre

45 https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime

46 https://www.cyber.gc.ca/en/guidance/profile-alphvblackcat-ransomware

47 https://www.cyber.gc.ca/en/guidance/profile-ta505-cl0p-ransomware

48 https://www.cyber.gc.ca/en/news-events/joint-cyber-security-advisory-truebot-malware

49 https://www.cyber.gc.ca/en/news-events/cse-and-international-partners-publish-cyber-security-advisory-lockbit-ransomware

50 https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector

51 https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime

52 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

53 https://www.cyber.gc.ca/en/guidance/threat-large-language-model-text-generators

54 https://www.cyber.gc.ca/en/guidance

55 https://www.getcybersafe.gc.ca/en/resources

56 http://www.getcybersafe.ca/business

57 https://www.getcybersafe.gc.ca/en/resources/7-red-flags-phishing

58 https://www.getcybersafe.gc.ca/en/resources/multi-factor-authentication

59 https://www.getcybersafe.gc.ca/en/resources/does-your-data-have-backup-plan

60 https://www.getcybersafe.gc.ca/en/resources/research/cyber-fitness-assessment-quiz

61 https://www.getcybersafe.gc.ca/en/resources/video-step-your-cyber-fitness

62 https://www.getcybersafe.gc.ca/en/cyber-security-awareness-month

63 https://www.getcybersafe.gc.ca/en/blogs/reporting-spam-text-messages-7726

64 https://www.cira.ca/en/canadian-shield/

65 https://www.cyber.gc.ca/en/education-community/academic-outreach-cyber-skills-development/canadian-cyber-security-skills-framework

66 https://resources.chatterhigh.com/discover-careers-in-cyber-security

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

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

69 https://www.cse-cst.gc.ca/en/mission/research-cse/applied-research

70 https://www.cse-cst.gc.ca/en/information-and-resources/announcements/cses-equities-management-framework

71 https://www.cyber.gc.ca/en/geekweek/geekweek-8

72 https://www.cyber.gc.ca/en/geekweek

73 https://www.cisa.gov/

74 https://www.cyber.gc.ca/en/news-events/big-dig

75 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

76 https://www.cyber.gc.ca/en/guidance/threat-large-language-model-text-generators

77 https://www.csps-efpc.gc.ca/video/ai-security-eng.aspx

78 https://www.cyber.gc.ca/en/guidance/generative-artificial-intelligence-ai-itsap00041

79 https://www.cyber.gc.ca/en/news-events/guidelines-secure-ai-system-development

80 https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/engaging-with-artificial-intelligence

81 https://www.cyber.gc.ca/en/tools-services/assemblyline

82 https://nsira-ossnr.gc.ca/

83 https://nsicop-cpsnr.ca/index-en.html

84 https://www.canada.ca/en/democratic-institutions/services/independent-special-rapporteur.html

85 https://foreigninterferencecommission.ca/

86 https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Overview_Institutional_Reports/CAN.DOC.000005.pdf

87 Canadian Centre for Cyber Security, Cyber Threats to Canada's Democratic Process, 2023 update, December 6, 2023. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

88 https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-2.html#docCont

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

90 The conditions under which CSE may disclose Canadian identifying information are explained on the Protecting Canadian identifying information in CSE's foreign intelligence mandate page on CSE's website. https://www.cse-cst.gc.ca/en/information-and-resources/fact-sheets/protecting-canadian-identifying-information-cses-foreign#DACRD

91 https://www.cse-cst.gc.ca/en/accountability/oversight#MAC

92 https://www.cse-cst.gc.ca/en/accountability/transparency/reports

93 https://open.canada.ca/en

94 https://www.cse-cst.gc.ca/en/accountability/transparency/access-information-and-privacy-atip

95 https://www.cse-cst.gc.ca/en/accountability/transparency/proactive-disclosure

96 https://www.ourcommons.ca/procedure/our-procedure/questions/c_g_questions-e.html#3

97 https://www.cse-cst.gc.ca/en/culture-and-community/ethics#disclosure

98 https://www.cse-cst.gc.ca/en/culture-and-community/ethics

99 https://www.canada.ca/en/privy-council/services/publications/deputy-ministers-task-team-values-ethics-report-clerk-privy-council.html?utm_source=message&utm_medium=Social_Media&utm_campaign=PCO_Twitter_EN&utm_id=VandE_Task_Team_Report

100 Numbers are based on voluntary self-declaration during the application process.

101 Workforce availability reference levels are based on Labour Market Availability census data (2016), factoring in additional criteria: citizenship, location and National Occupational Classification code comparisons.

102 Workforce availability data for 2SLGBTQIA+ representation is not available as this is not considered a designated employment equity group under the Employment Equity Act.

103 Numbers are based on voluntary self-declaration. 90% of 2023 to 2024 hires provided self-declaration data.

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

105 https://www.rcaanc-cirnac.gc.ca/eng/1524494530110/1557511412801

106 https://talent.canada.ca/en/indigenous-it-apprentice

107 https://www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service/knowledge-circle.html

108 https://www.cse-cst.gc.ca/en/accessibility/communications-security-establishment-accessibility-plan-progress-report-2023

109 https://www.cse-cst.gc.ca/en/accessibility/cse-accessibility-plan-2022-2025

110 https://www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/affinity-groups

111 https://reviews.canadastop100.com/top-employer-communications-security-establishment#young

112 https://reviews.canadastop100.com/top-employer-communications-security-establishment