Government of Canada / Gouvernement du Canada

Communications Security Establishment Annual Report 2019-20

ISSN 2564-047X

Table of contents

MESSAGE FROM THE CHIEF

We are one CSE, known and trusted.

Our inspired workforce and thought leading innovation help secure a digital Canada, provide a Canadian information advantage, and achieve strategic impact through cyber operations.

It may seem remarkable that the Communications Security Establishment is issuing our first public report at the same time as we begin preparations to celebrate our 75th anniversary. CSE's journey between these two points in time is worth telling.

Our mandate has always been important, but has quietly and incrementally gained relevance over nearly three-quarters of a century collecting foreign intelligence and protecting information systems. Government of Canada priorities have changed over those decades, of course, as has the global technical landscape. Today, in 2020, the world is more polarized and geopolitically complex. And advanced, interconnected and disruptive technologies are emerging at unprecedented rates.

At the intersection of these two trends lies CSE's modern-day cyber mandate.

While we have always found ways to adapt to our dynamic operating environment, two recent developments have been significant in positioning CSE for the next decade's challenges. First, the *CSE Act* came into force in mid-2019, recognizing the growing relevance of CSE's mandate, skills and capabilities. The Act enhances CSE's current authorities and adds mandates for CSE to use our expertise with non-Government of Canada cyber victims, to take cyber action outside Canada when necessary, as well as assist the Canadian Armed Forces in delivering their mandate, when requested. This Act—which will be reviewed in three years—provides CSE with a modern set of authorities, and also enhances the accountability framework with new oversight and review functions.

Second was the creation of the Canadian Centre for Cyber Security. This CSE branch is built on the foundations of our longstanding Information Technology Security mission and bolstered by cyber security expertise from other Government of Canada departments. The Cyber Centre's outward

facing role is as Canada's single unified source of expert advice, guidance, services and support on cyber security. Within CSE, cyber defence and foreign intelligence teams bring the right information and expertise together to mitigate national cyber risks. This reporting period marks the Cyber Centre's first full year of operation.

Nowhere has this powerful collaboration of CSE's two missions been more evident than in our work to help protect the 2019 Canadian general election. CSE's mandate put us at the nexus of monitoring foreign threats directed at Canada in the lead up to the election and ensuring our Canadian infrastructure was positioned to withstand them. Together with partners, CSE played an important role, notably by leaning forward and sharing our unique insights more broadly with Canadians and Canadian political parties in the form of threat assessments and tailored advice and guidance.

A more recent example has been our support for the Government's COVID-19 response efforts. To date in 2020, CSE has provided valued intelligence for Government clients, alerted Canadians to the sharp increase in COVID-19-related on-line schemes and advised Canada's health and medical research sector of varied, determined cyber threat actors. Tailored advice, guidance and services have been designed to help protect Canadians and those researching solutions for the pandemic.

In this modern world, cyber security must be taken seriously and baked into every stage of Canada's digital evolution-for critical infrastructure owners and operators, for small and medium enterprises, for research organizations and for Canadians. Digital networks underpin every aspect of Canadian society, economy, and security. By embracing even basic cyber security practices, every Canadian and every Canadian organization can play a part in Canada's national cyber security. It is our job to provide the

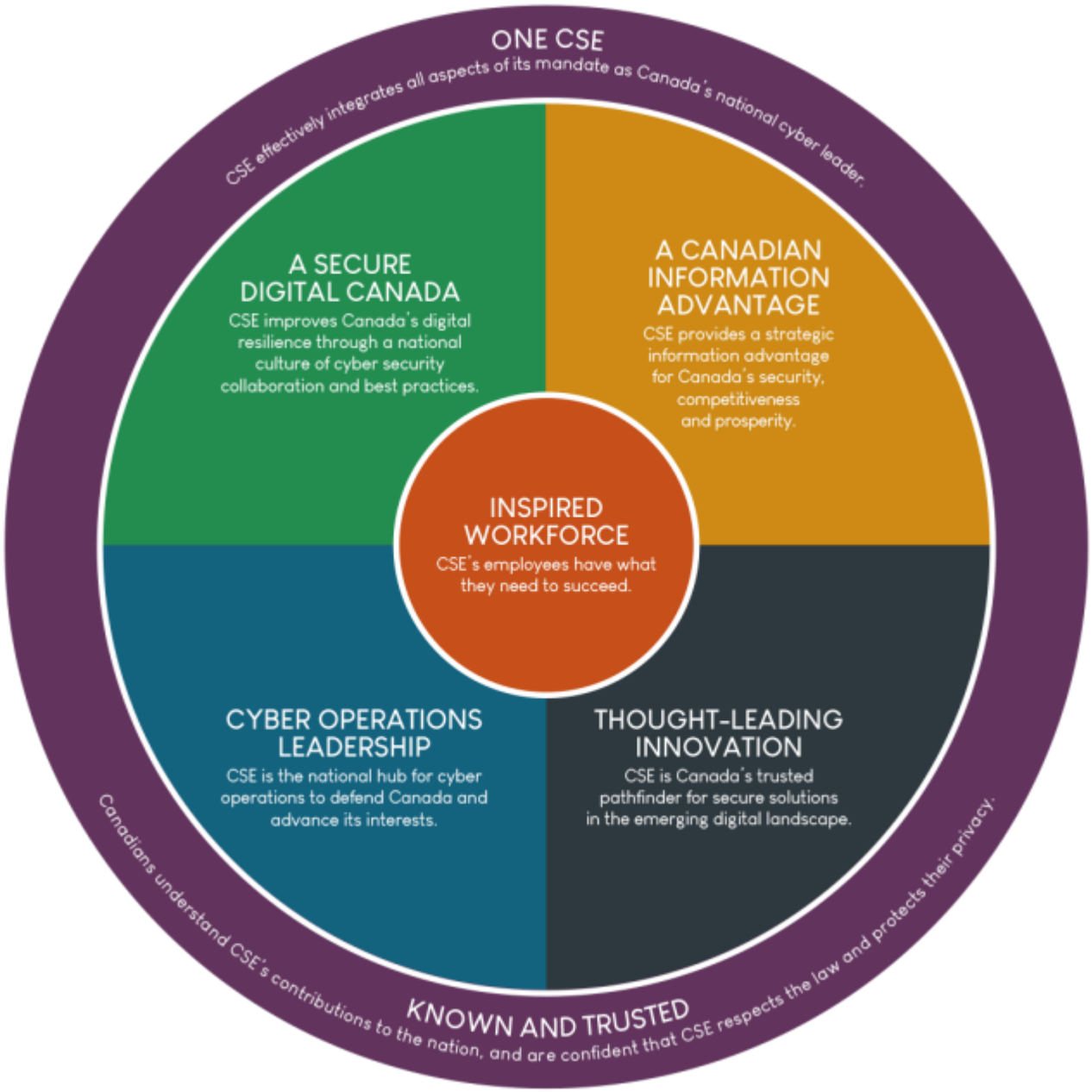
right information and tools to help them take their position as Canada's front-line cyber defenders. We have invested a great deal of effort over 2019-2020 to raise public awareness, and this work must continue.

Since our wartime beginnings, CSE has nurtured a culture of innovation that is both natural and necessary, and that has been supported by our exceptional workforce and their unique technical expertise, commitment to collaboration and strong set of shared values. While some may still think of CSE as a secret organization, it is more accurate to think of us as an organization with secrets. Some of our work must necessarily remain out of the public domain and that, of course, has had an impact on what can be included in this report. All of our activities, however, are subject to review, and those independent bodies act as proxies for the public by letting Canadians know that we have done our job very well, and where there may be room for improvement.

It is my hope that, with the publication of this and future public reports, CSE can be better known and understood for our national roles and valued contributions in protecting Canada and Canadians from those who would seek to undermine our security, our prosperity and our competitiveness.

Please watch for our 75th anniversary celebrations in the coming year as another way to understand how our history forms the foundations for our future.

Shelly Bruce
Chief, CSE

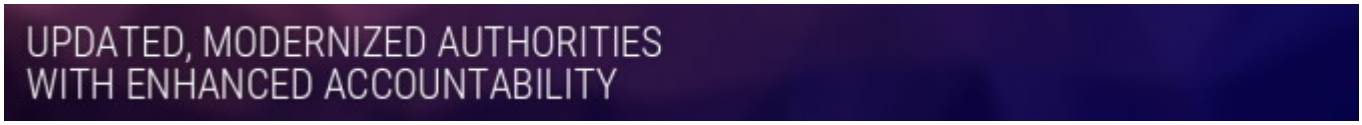


CSE 2025 lays out CSE's five-year strategic horizon to guide investments and operations in a way that directs our focus on delivering national-level results and mitigating national-level risks. In early 2020, we set our sights on delivering:

- **A secure digital Canada:** CSE improves Canada's digital resilience through a national culture of cyber security collaboration and best

practices.

- **Information advantage to Canadian decision makers:** CSE provides a strategic information advantage for Canada's security, prosperity and competitiveness.
- **Cyber operations leadership:** CSE is the national hub for cyber operations to defend Canada and advance national interests.
- **Thought-leading innovation:** CSE is Canada's trusted pathfinder for secure solutions in the emerging digital landscape.



Milestone legislation for the Communications Security Establishment, the *CSE Act*, came into force in August 2019. The new Act outlines CSE's lead roles as the national authority for foreign intelligence (for signals intelligence or SIGINT) and as the national technical authority for cyber security and information assurance. The Act expresses in detail CSE's enhanced mandate to:

- Help protect and defend information infrastructures of importance to Canada;
- Acquire foreign intelligence in support of the Canadian intelligence priorities;
- Conduct foreign cyber operations—both active and defensive—in Canada's interests; and,
- Use our expertise to assist federal law enforcement and security agencies, the Canadian Armed Forces and the Department of National Defence to carry out their lawful mandates

▶ Long description - Accountability measures

The *CSE Act* also describes how CSE fits into Canada's new security and intelligence accountability framework. While CSE's operations are conducted under a series of authorizations from the Minister of National Defence, the *CSE Act* added the role of the Intelligence Commissioner to provide quasi-judicial oversight of CSE's foreign intelligence and cyber security authorizations.

In mid-2019, the National Security and Intelligence Review Agency (NSIRA) was created to review activities in Canada's security and intelligence community, including CSE. At the same time, the Office of the CSE Commissioner, in place since 1996, was disestablished, and ongoing reviews were transferred to NSIRA. CSE is also subject to the review of the National Security and Intelligence Committee of Parliamentarians (NSICOP), and other Agents of Parliament, including the Auditor General, the Information and Privacy Commissioners.

CANADA'S SECURITY, PROSPERITY AND COMPETITIVENESS

The following highlight some of CSE's key activities in 2019-2020. They illustrate how our people, our plans, our expertise and our partnerships combine to deliver mission impact in support of Canada's security, prosperity and competitiveness.

Protecting the .gc.ca

In 2019-2020, CSE's Cyber Centre continued to deliver world-class dynamic defence of Canadian government networks, by now routinely blocking well over a billion malicious actions aimed every day at federal systems, databases and websites. As the Government of Canada has rapidly transitioned its systems and information to cloud environments, CSE has been at the forefront of designing security solutions to protect them. Federal departments and agencies within the secure perimeter operated by CSE and Shared Services Canada benefit from sophisticated cyber defences,

informed by threat intelligence gleaned from CSE's mandate and trusted partners. This bolsters protection for Canadian federal programs and networks, as well as Canadians' personal information.

Some cyber actors set up malicious websites or use email addresses that impersonate Government of Canada entities. When discovered, the Cyber Centre worked with trusted commercial and international partners directly involved in taking them down. In 2019-2020, the most frequently impersonated government sites were Canada Revenue Agency, Public Health Agency of Canada, and Canada Border Services Agency. This has helped reduce the risk that Canadians will be defrauded of their money or lose their information to malicious actors.

Protecting the .ca

Phishing attempts are the work of cyber threat actors, often criminal networks, to defraud Canadians, steal their information or gain further access to networks of interest. In keeping with CSE's national lead role for cyber security, the Cyber Centre partnered with the Canadian Internet Registration Authority (CIRA), a not-for-profit agency that manages the .ca internet domain. Under this partnership, the Cyber

Centre shares unique and timely threat intelligence into a free service for protected DNS—or Domain Name System (the phone book of the Internet)—called *Canadian Shield*. The service prevents users from connecting to malicious websites that might infect their devices or steal their personal information.

Security through collaboration with Canadian industry

In 2019-2020, the Cyber Centre's efforts were focused on increasing awareness and knowledge of cyber-security issues and concerns among private sector critical infrastructure providers. The Cyber Centre shared available cyber threat information with businesses including information learned from defending the government of Canada and that from our foreign intelligence program. This information was included in automated threat feeds, cyber alerts (security notifications requiring attention within 24 hours) and flashes (security notifications requiring immediate solution) as well as other advice and guidance products.

The Cyber Centre worked with the Canadian financial sector, including banks, regulators, and financial institutions, helping to prevent potential losses from fraud, and support to the energy industry was provided by helping utilities companies monitor for cyber threats. These are just a few examples of the broad range of partnership activities underway in the review period and which will continue to grow with a view to bolstering the cyber security of critical systems across Canadian sectors.

That's important. A 2017 StatsCan survey found that at least one in five Canadian companies believed their systems had been targeted by cyber actors. To help protect those systems, the Cyber Centre developed baseline security controls for small and medium-sized enterprises (SMEs),

recognizing that they have operating environments and resources which set them apart from larger corporate entities, but are equally at risk in the current environment.

Publishing second election-related cyber threat report

In 2019, CSE released an updated assessment on Cyber Threats to Canada's Democratic Process, building on our first-of-its-kind public examination in 2017. The pre-election report informed Canadians about the upward trend of cyber threat activity against democratic processes globally, especially against OECD nations, and noted that the Canadian electorate, information systems and political parties would not be immune. The report, combined with CSE's real-time operational

perspectives, helped shape the Cyber Centre's advice and guidance for those involved in the democratic process, from Elections Canada and political parties to Canadian voters.

Monitoring for foreign threats to the 2019 election

In the lead up to and during the 2019 Federal Election, CSE worked with partners at the Canadian Security Intelligence Service (CSIS), Global Affairs Canada (GAC), and the RCMP as the Security and Intelligence Threats to Elections Task Force (SITE). CSE's role in SITE was to monitor for foreign threats and interference with electoral processes in Canada. Along with SITE officials, CSE provided regular briefings to the members of the Government of Canada's Critical Election Incident Public Protocol (CEIPP), who did not observe any activities that met the threshold for public announcement or affected Canada's ability to have a free and fair election. CSE also participated with other SITE members in briefings to political party representatives and the media.

Securing Canadian election infrastructure

Drawing on CSE's experience from the 2015 election, the Cyber Centre ensured strong and effective cyber defence measures were in place to protect Elections Canada's systems and networks. Advice and guidance was also provided to provincial and other institutions involved in democratic processes.

Providing cyber security advice to political parties and candidates

CSE provided a series of briefings and published a range of tailored products outlining specific actions, tips and best practices that could be taken by political parties, candidates, and their staff to protect themselves

against malicious cyber activity during the 2019 Federal Election, and established protocols to use should cyber security assistance be required.

Providing foreign intelligence insights to Canadian decision-makers

CSE's foreign intelligence work extended far beyond helping protect Canada's democratic processes. In the past year, CSE provided foreign intelligence reports to more than 2100 clients in over 25 departments and agencies within the Government of Canada in response to a range of priorities related to international affairs, defence, and security. As examples, CSE's intelligence reporting helped thwart or respond to foreign cyber threats, supported Canada's military operations and protected deployed forces, identified hostile state activities and provided insight into global events and crises to help inform Government policies and decision making.

Protecting Canada's research and innovation edge

CSE's Cyber Centre engaged directly with several Canadian universities and academic communities in 2019-2020 and has begun sharing some of our tools and services to enhance their cyber security efforts. CSE is also working with Canada's academic sector to raise awareness and establish protocols to best support them. Early in the COVID-19 pandemic, CSE alerted Canada's health and medical research sector regarding rapidly emerging cyber threats and provided advice and guidance about how to bolster their network security.

Protecting Canada's sensitive communications

CSE continued to operate Canada's Top Secret Network (CTSN) for the Government of Canada, onboarding new departments and agencies, and increasing communications capacity and functionality, as well as delivering other secure communications solutions. CSE also assisted the House of Commons in developing options for holding virtual Parliament and committee sessions.

Developing Canada's quantum edge

CSE's research leads in partnership with other government departments and academic leaders continued work on a national quantum-safe cryptographic solution. The results of this work will help secure the Government of Canada's most sensitive information before a sufficiently powerful quantum computer—one that can break today's cryptography—is produced. Actively in development, deployment of the solution to some Government of Canada departments is expected as early as 2021.

Promoting experimentation and innovation in cyber security

Cyber Security is a team imperative. In spring 2019, CSE hosted the "Big Dig," our 10th annual, week-long classified collaboration event bringing government, industry, academia and allied partners together to take on specific cyber challenges. Later in the year, CSE also hosted the sixth "Geek Week", a similar but unclassified annual workshop that brings together cyber security practitioners from around the world to address vital problems facing the cyber security industry. These experimentation sessions have led to the development of important new tradecraft to better secure networks against common threats and to identify novel ways to mitigate risks.

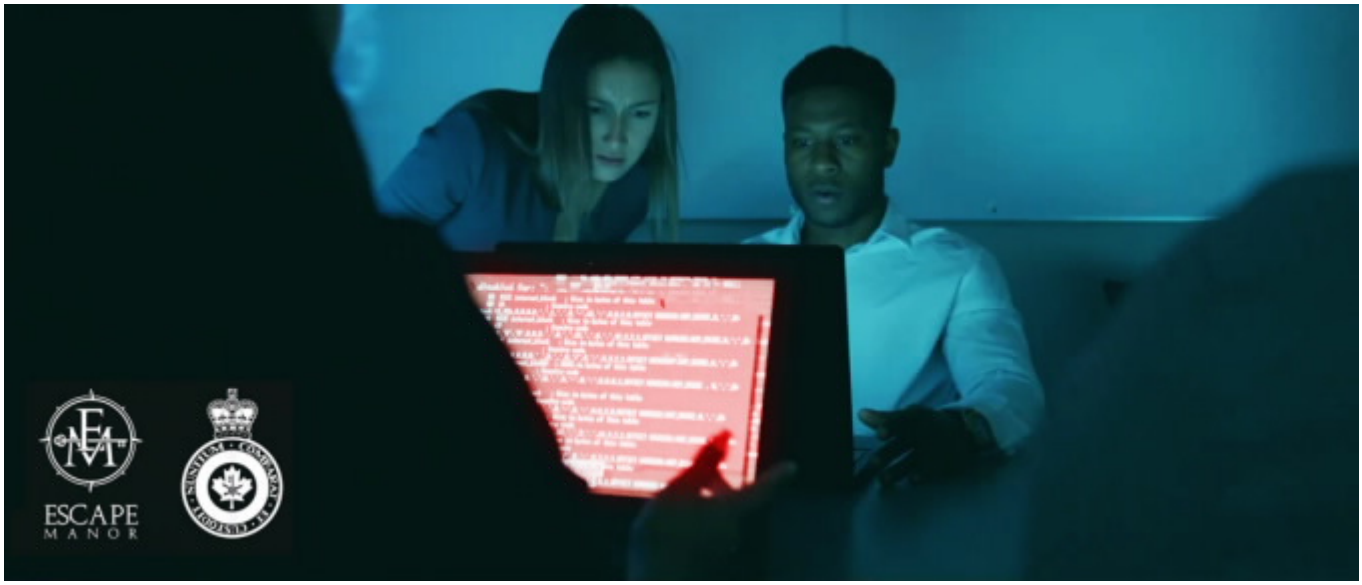
Promoting STEM among Canada's youth

CSE has a growing outreach program, including support and mentoring for national-level, not-for-profit programs, such as Hackergal and CyberTitan. These partnerships promote the development of STEM skills among Canada's youth and stoke interest in STEM educational paths and careers. They also motivate and engage CSE's workforce, who are always keen to share their passion for STEM with national and community organizations and local schools.

Introducing cyber security concepts to Canadian children

To plant seeds today that will help meet future needs of the Government of Canada's in cyber security, CSE partnered with Ingenium, Canada's Museums of Science and Innovation, to create Cipher | Decipher, a travelling exhibition that explores concepts of encryption and cyber security, specifically designed for school-age children. Cipher | Decipher proved to be a popular exhibit at host venues, attracting 22,000 at the Canadian Science and Technology Museum. Cipher | Decipher will continue to travel in Canada into 2021.

Finding new ways to recruit top talent



In 2019-2020, CSE forged new partnerships aimed both at promoting our organization and aiding with critical recruitment efforts, ensuring that CSE can recruit the best and brightest. One of these was "The Recruit", an immersive, cyber-themed "escape-room" experience created through a partnership between CSE and Escape Manor. Participants successful in the challenge had an opportunity to talk with a CSE recruiter and be invited to apply for a position at CSE.

OUR PEOPLE: A CULTURE OF COMMUNITY

CSE's accomplishments in 2019-2020 were made possible by our very clever and dedicated people. CSE's values, ethics and culture combine to create an environment that promotes diversity, inclusion and community. This sets the scene for innovation and trusted experimentation across the whole organization and has contributed to our recognition as a "Top Employer" in both 2019 and 2020.

CSE's 2019 Public Service Employee Survey results highlighted that:

▶ Long description - PSES results for CSE

While the PSES results for CSE have been positive for the past several years, we know there is always more that can be done. CSE takes continuous improvement to heart, communicating with employees regularly on how to enhance their experience in the workplace, and ensure CSE's workforce remains inspired and armed with what they need to succeed as individuals and as a community delivering an important mission for Canada and Canadians. Our Beyond 2020 report to the Clerk shows how our people get and stay engaged in serving their country.

CSE BY THE NUMBERS

A quick catch up of key dates and figures in CSE's history...

▶ Long description - Dates and figures in CSE's history

- Today, CSE is a stand-alone agency, running 24/7 operations to collect vital foreign intelligence (signals intelligence), protect Canadian systems of importance, conduct cyber operations and assist our federal partners deliver their mandates.
- The Chief of CSE, Shelly Bruce, reports to the Minister of National Defence, the Honourable Harjit S. Sajjan.

- CSE’s budget is $786.6 million and our workforce is 2,900 strong.

Search our events, information and resources

Mission

Discover CSE's impactful mission

Careers

Join our team and help keep Canadians safe

Culture and community

Learn how we support our employees and our community

Date modified:
2021-06-04