Building a **safe** and **resilient Canada**

Canada's National Cyber Security Strategy

Securing Canada's Digital Future

Public Safety Canada
Sécurité publique Canada

Canada

Read this publication online at:
https://publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

Canada's new National Cyber Security Strategy articulates the Government of Canada's long-term plan to partner with provinces, territories, Indigenous communities, industry, and academia to secure Canada's digital future.

Aussi disponible en français sous le titre :
La Stratégie nationale de cybersécurité du Canada

Public Safety Canada, Communications
269 Laurier Ave. W
Ottawa Canada K1A 0P8

Communications@ps-sp.gc.ca

www.PublicSafety.gc.ca

Publication date: 2025-01
Catalogue Number: PS4-239/2025E-PDF
ISBN: 978-0-660-72268-9

Table of Contents

Minister of Public Safety Message

The Honourable David McGuinty,
Minister of Public Safety

Advancements in technology continue to evolve at an unprecedented pace. As more Canadians live and work online and as businesses and industry move to digital services, cyber threats continue to increase. This is creating real impacts for Canadians and is becoming a leading threat to Canada's national security and economy.

Canada's new National Cyber Security Strategy articulates our long-term plan to tackle those challenges, in partnership with provinces, territories, Indigenous communities, industry, and academia to secure Canada's digital future.

We have made recent investments, building upon well-established mechanisms to respond to incidents of malicious cyber activity targeting Government of Canada systems. And we will continue to use all available tools to protect Canada's critical infrastructure to better position us to adapt to and combat cyber risks, ensure the security and integrity of Canada's critical systems, and create a mechanism to enforce our 2022 statement on telecommunications security.

However, there is still more to be done. This new National Cyber Security Strategy will enable us to move forward on this important work.

We must work together and protect Canadians and Canadian businesses, and prevent critical infrastructure disruptions to services that our citizens rely on every single day.

Together, we will ensure that cyberspace is safe, open and secure for all Canadians.

Introduction

Ensuring Canada's safety and prosperity online relies on robust cyber security.

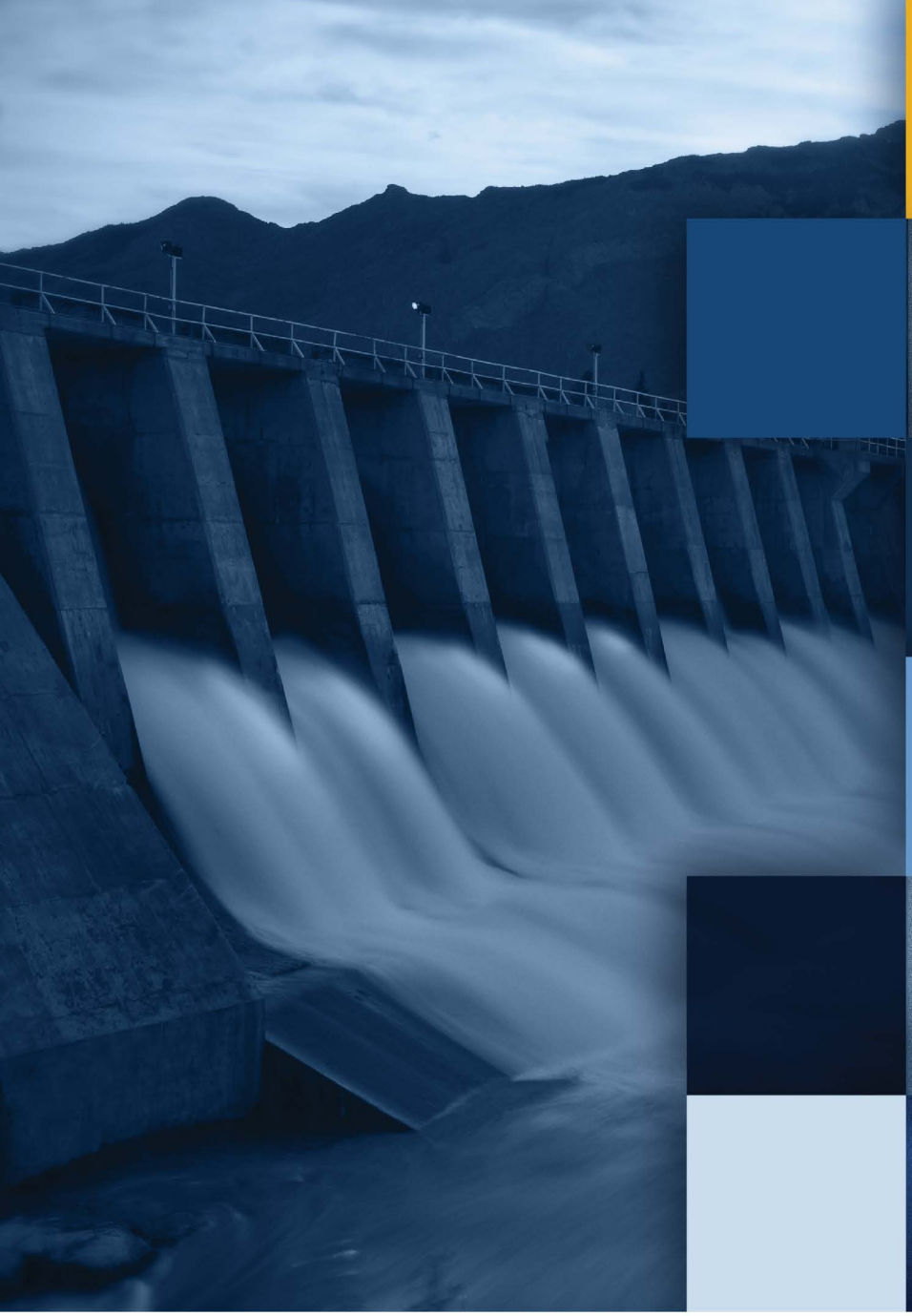
Advances in digital technologies have enriched our lives and provided enormous benefits to society. Unfortunately, the same innovations that have brought us so many benefits have also exposed us to risks that threaten not only our digital infrastructure, but also the critical services on which we rely.

Today, it is abundantly clear that to safely advance Canada's digital and clean economy, to protect our democracy and our day-to-day livelihoods, and to ensure our future economic prosperity, cyber security must be a fundamental building block of our country's national security, economic security, and public safety.

Canada's 2018 National Cyber Security Strategy[1] established the Canadian Centre for Cyber Security[2] (Cyber Centre) based within the Communications Security Establishment Canada[3] (CSE), and the National Cybercrime Coordination Centre[4] (NC3) under the stewardship of the Royal Canadian Mounted Police[5] (RCMP). These foundational changes have provided Canadians with consolidated support in responding to cyber incidents and investigations into cybercrime.

Despite these gains, the cyber threats facing Canada continue to evolve and grow. Canada must do more.

1 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf
2 https://www.cyber.gc.ca/en
3 https://www.cse-cst.gc.ca/en
4 https://www.rcmp-grc.gc.ca/en/nc3
5 https://www.rcmp-grc.gc.ca/



The Challenge: Cyber Threats Affecting Canadians Evolve Constantly

Canadians face persistent, sophisticated, daily cyber threats.

Since 2018, we have experienced enormous change. The pandemic pushed almost all aspects of Canadians' lives online at an accelerated pace, and, as a result, our critical infrastructure is becoming increasingly interconnected. State-sponsored cyber threat actors and organized cybercriminals have been quick to capitalize on these expanded opportunities and our increased reliance on online services.

Canadians continue to be affected by this increase in cyber threat activity and pay a heavy price. Malicious cyber actors detrimentally impact key services, including healthcare and education, and steal Canadians' private information and intellectual property. Revenue that should boost Canada's economy disappears into criminal hands. The financial and reputational costs of cyber breaches are felt by small, medium and large enterprises, as well as governments at all levels. And, unfortunately, many organizations do not have the resources required to defend against these sophisticated threats.

Moreover, in recent years we have seen increasingly brazen and sophisticated state-sponsored cyber actors conducting foreign interference and military action online. Canada has been targeted for our membership in the North Atlantic Treaty Organization[6] (NATO) and for our support to Ukraine.

To tackle and reduce the level of risk borne by Canadians and Canadian businesses from these cyber threats, Canada must be prepared to continuously adapt, and to foster and harness all of its collective abilities.

6 https://www.nato.int/

Addressing the Challenge: A New Approach to National Cyber Security that Engages All Canadians

Two overarching principles will serve to guide Canada's approach to cyber security:

1. **Whole-of-society engagement:** All Canadians have a role to play in improving Canada's national cyber resilience. The Government of Canada will deepen partnerships with key stakeholders to tackle key issues in the cyber security landscape. Partnerships with other levels of government, Indigenous communities, the private sector, academia, and civil society will be critical to developing the solutions that will address tomorrow's cyber security challenges. Canadians will play an important part, too, as digital citizens and business owners. Improving public awareness and cyber security know-how for all will help to ensure that Canadians are more informed of the cyber threats they face, and more resilient against malicious cyber actors.

2. **Agile Leadership:** Threats and opportunities in cyberspace continue to evolve at a rapid pace globally; it is critical for Canada to be equipped to respond to emerging risks as they occur. Therefore, rather than a single static plan, Canada's cyber security solutions will be developed in close collaboration with partners and stakeholders and set out in a series of issue-specific action plans over the coming years. These action plans will outline initiatives for Canada and Canadians with clear outcomes and a commitment to report on results achieved. They will be collaborative and holistic, and will enable Canada to be at the forefront of innovative approaches to cyber security risks and opportunities. This will ensure that our solutions remain relevant and effective as threats evolve.

The National Cyber Security Strategy will focus on using this approach to deliver results under three pillars:

Pillar 1: Work with Partners to Protect Canadians and Canadian Businesses from Cyber Threats

Canada will:

- Forge whole-of-society partnerships
- Defend and advocate for Canadian interests and values internationally
- Advance national cyber awareness and hygiene

Pillar 2: Make Canada a Global Cyber Security Industry Leader

Canada will:

- Make Canada a trusted innovator that prioritizes cyber security
- Grow the foundational workforce of the future
- Identify and support targeted areas of research to meet Canadian needs

Pillar 3: Detect and Disrupt Cyber Threat Actors

Canada will:

- Identify, deter, and defend against cyber threats
- Improve capacity to combat cybercrime
- Make critical systems more resilient

Pillar 1: **Work with Partners to Protect Canadians and Canadian Businesses from Cyber Threats**

No single institution or segment of society can address the challenges posed by cyber threats alone. As the Government of Canada, we have had success in partnering with industry and other levels of government to share information, respond to cyber incidents and to launch Canadian cyber capabilities. We will deepen those connections and do more.

The Government of Canada will lead an unprecedented level of public-private partnering on cyber issues to better tap into the expertise and capabilities of stakeholders.

We will develop action plans to identify and address barriers to collaboration between government and other segments of society including international partners, build partnerships to leverage our collective capacity to respond to cyber threats, and guide our international engagement to promote norms-based behaviour in cyberspace.

Objective 1.1: Forge Whole-of-Society Partnerships

National leadership is key to a unified, holistic, and strategic approach to cyber security.

The Government of Canada should not build its cyber security action plans alone. The Government of Canada will bring the topic of cyber security to the forefront of engagements with provinces and territories, and Indigenous communities to better represent cyber security needs. For instance, Canada's critical infrastructure—primarily owned by the private sector—is spread across a vast but unevenly populated country. Small and remote communities, including northern populations and Indigenous communities, must be protected to the same extent as those in major urban centres.

As part of the Government of Canada's shift toward whole-of-society partnership, Public Safety Canada[7] (PS) and the Canadian Centre for Cyber Security[8] (Cyber Centre) will establish the **Canadian Cyber Defence Collective (CCDC)**. The CCDC will serve as a national multi-stakeholder engagement body to advance Canada's cyber resilience through direct public-private partnership on national-level cyber security challenges, policy priorities, and defence efforts. The Government of Canada will actively leverage the CCDC to regularly engage stakeholders in the development of action plans to ensure the most current insights and experiences are informing future policy and program action.

7 https://www.publicsafety.gc.ca/index-en.aspx
8 https://www.cyber.gc.ca/en

As a first step to its commitment to developing partnerships with academia, the Government of Canada has funded a Cybersecurity Attribution Data Centre (CADC) at the Canadian Institute of Cybersecurity (CIC)[9] at the University of New Brunswick (UNB)[10]. With the ultimate goal to identify malicious cyber threat activity, the CADC will apply the latest cyber analytics to data gathered from a variety of sources. The CADC will also train and equip the next generation of artificial intelligence (AI) cyber security specialists. Overall, the CADC will address a clear workforce and training gap in the ever-evolving cyber security environment, and in the long- term, improve Canada's ability to collaborate and innovate to protect Canadians and Canadian business from cyber threats.

Objective 1.2: Defend and Advocate for Canadian Interests and Values Internationally

Canada's domestic cyber security exists in a global context.

> The Government of Canada released a Statement on International Law applicable in cyberspace[11] to contribute to ongoing international dialogue on how international law applies in cyberspace. Canada continues to advance implementation of the United Nations (UN) Norms of Responsible State Behavior in Cyberspace[12] by promoting greater understanding of, and compliance with, its norms of responsible state behaviour.

As cyber threats do not respect borders, Canada must continue to work with its allies to defend our national interests and promote global security. Canada will continue to play a significant role in bringing together like-minded international partners to champion international law and norms-based behavior and international standards in cyberspace, and will also deepen its international partnerships to deter and respond to malicious cyber activity. Canada will continue to promote its vision of an open, free, secure, and reliable Internet; call-out unacceptable behaviour; and, consider the role that sanctions and listings regimes can play in deterring online threats.

9 https://www.unb.ca/cic/
10 https://www.unb.ca/
11 https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng
12 https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

To support these actions, Global Affairs Canada[13] (GAC) has created a new role, a foreign policy **Senior Official for Cyber, Digital and Emerging Technology,** to coordinate international engagement across government and represent Canada internationally.

The Government of Canada will also support other nations' capacity building efforts to detect and address cyber threats, including through greater cooperation in the Indo-Pacific region.

Objective 1.3: Advance National Cyber Awareness and Hygiene

National cyber security depends on raising Canadian cyber awareness to reduce victimization.

> The "Get Cyber Safe"[14] program provides Canadians with free access to basic cyber hygiene tips and education. The Canadian Anti-Fraud Centre[15] (CAFC), the Competition Bureau, and the Canada Revenue Agency coordinate fraud awareness efforts.

The Government of Canada will strive to make cyber security more accessible to all Canadians. Enhancing collective cyber hygiene and awareness ensures the safety and security of more Canadians, and it reduces the risk of Canadians becoming victims of cybercrime. Cyber security considerations need to become embedded in the day-to-day operations of Canadian businesses and in Canadian innovation, particularly in sectors of national importance such as health, energy, and green technology.

Additionally, the Government of Canada will build on the success of the "Get Cyber Safe"[16] program and the Canadian Anti-Fraud Centre[17] (CAFC), and will continue to leverage the expertise of the Cyber Centre[18] through the publication of cyber-related material on topics such as artificial intelligence, the threats posed by large language models (LLMs), and how to identify misinformation, disinformation, and malinformation (MDM) to increase engagement with Canadians. As digital technologies continue to advance, their capabilities are being harnessed for malicious intent in new ways. Going forward, the Government of Canada will continue to advance cyber security awareness campaigns to enhance Canada's cyber hygiene on a national scale and strengthen Canada's national cyber resiliency.

---

13 https://www.international.gc.ca/global-affairs-affaires-mondiales/home-accueil.aspx?lang=eng
14 https://www.getcybersafe.gc.ca/en
15 https://antifraudcentre-centreantifraude.ca/index-eng.htm
16 https://www.getcybersafe.gc.ca/en
17 https://antifraudcentre-centreantifraude.ca/index-eng.htm
18 https://www.cyber.gc.ca/en

Pillar 2: **Make Canada a Global Cyber Security Industry Leader**

Canada is an innovator. We will build on our already strong cyber security industry to make Canada a global leader in innovative cyber technology. To help set the conditions for success, the Government of Canada will support the full spectrum of research and development, from basic research to product launch.

There is a global shortage of cyber security professionals. Canada is no exception. We will take steps to educate and grow cyber security talent in Canada. At the same time, there are steps we can take now to use technology—such as artificial intelligence (AI) and automation—to better meet the threats we face today.

Some notable initiatives underway include:

- Canada's Digital Charter[19] sets out how the Government of Canada ensures that Canadians can rely on the integrity and security of the services they use online, and of their information held by the private sector.
- The Cyber Security Innovation Network[20] supports the growth of Canada's cyber security ecosystem through collaboration between academia, the private sector, not-for-profit sectors and other levels of government. It funds high-impact projects to enhance research and development, commercialize products and services, and develop cyber security talent.
- The recently established Canada Innovation Corporation[21] supports the development and protection of new intellectual property in the defence sector, resulting in new, innovative, and safe Canadian cyber technology.
- Canada's Digital Technology Supercluster[22] accelerates the development and adoption of cyber technologies.
- The Digital Technologies Research Centre[23] partners with industry to research threats to supply chains, transportation, energy, and other infrastructure.
- Innovative Solutions Canada[24] helps small and medium enterprises (SMEs) bring their innovations to market.

19 https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world
20 https://ised-isde.canada.ca/site/cyber-security-innovation-network/en
21 https://www.canada.ca/en/department-finance/services/publications/canada-innovation-corporation-blueprint.html
22 https://ised-isde.canada.ca/site/global-innovation-clusters/en/canadas-digital-technology-cluster
23 https://nrc.canada.ca/en/research-development/products-services/technical-advisory-services/cybersecurity
24 https://ised-isde.canada.ca/site/innovative-solutions-canada/en/about-us

- The Accelerated Investment Incentive[25] allows SMEs to benefit from tax incentives for capital investments, including those related to cyber security.
- Procurement Assistance Canada[26] is working to simplify the procurement process for small businesses. By reducing barriers and providing Canadian companies with preferred access to government contracting opportunities, the program will help incubate and grow Canadian cyber security businesses.

To protect our industry, innovative research, and livelihood we need to ensure that cyber security is prioritized. In short, Canadians need access to secure products by default. While Canada has made significant strides in strengthening cyber security, the number of incidents Canada experiences every year continues to grow.

In response, the Government of Canada will explore legislation, regulation, and incentives to foster the adoption of secure technologies and practices. We will partner with all levels of government, industry and academia to build leading-edge cyber security into our industry, our day-to day business practices, and our products and services.

Our legislation and actions must be well-informed. We will invest in research to build a comprehensive understanding of the economics of cybercrime and cyber security in order to more effectively encourage the adoption of secure technology and combat cyber threat actors.

Objective 2.1: Make Canada a Trusted Innovator that Prioritizes Cyber Security

Promoting secure-by-design products and the adoption of secure technologies.

We all share the responsibility to use and implement cyber-secure products and practices; this burden cannot be placed solely on individual citizens. Canadian businesses of all sizes must embrace a cultural shift that prioritizes secure-by-design products, and a mindset of being “first-to-secure” rather than only being “first-to-market”. Only in this way can the security of the digital ecosystem be improved.

The Government of Canada, working with industry, will set out a strategy to facilitate a

25 https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/sole-proprietorships-partnerships/report-business-income-expenses/claiming-capital-cost-allowance/accelerated-investment-incentive.html
26 https://www.canada.ca/en/public-services-procurement/services/acquisitions/support-for-businesses.html

society-wide shift toward shared cyber responsibility. As a first step, the Government of Canada will consider ways it could incentivize organizations to place consumer safety at the core of their operations. The Government of Canada will also consider cyber security certifications and designating trusted companies with preferred Government of Canada contractor status.

In addition, the Government of Canada will explore Internet of Things (IoT) labelling to help Canadians easily identify and compare the cyber security protections built into products. This would help consumers, while also making domestic cyber products more attractive. The Government of Canada will also work with international partners to coordinate labelling efforts and obtain reciprocal recognition of Canadian standards.

The Government of Canada will continue to work with businesses that provide essential services to improve their cyber security. Notably, the Government of Canada announced the Canadian Cyber Security Certification program[27] to enhance cyber security in the defence sector. This will ensure that companies bidding for select Canadian government defence contracts maintain a high level of cyber security. The Government of Canada is collaborating with the U.S. to ensure the certification is compatible with the U.S. Cybersecurity Maturity Model Certification (CMMC), easing the burden on Canadian industry when bidding on U.S. defence contracts. The Government of Canada will consider expanding this program beyond the defence sector.

The Government of Canada is also fortifying Canada's private sector privacy regulations, and establishing new guidelines for the responsible development and deployment of artificial intelligence (AI). The Government of Canada aims to modernize the federal private sector privacy framework, and improve governance of the design, creation, and use of AI. The Government of Canada also continues to update its federal guides and directives on AI[28]. We must ensure that AI systems are developed safely and in accordance with Canadian values, thereby ensuring that Canadians can have confidence in the digital technologies they interact with daily. The Government of Canada will continue to respond to emerging technologies, including AI, to ensure their responsible and safe adoption in Canada.

27 https://www.canada.ca/en/public-services-procurement/news/2023/05/government-of-canada-helping-defence-industry-protect-itself-from-cyber-security-threats.html
28 https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html

Objective 2.2: Grow the Foundational Workforce of the Future

Cyber security talent development, attraction, retention, and education are critical to our national success.

> Already, the Upskilling for Industry Initiative[29] allows employers to identify skill requirements in rapidly growing sectors. By encouraging collaboration between employers and training providers, the program helps deliver tailored upskilling programs that meet employers' needs, particularly in high-growth industries. The initiative is anticipated to help over 15,000 Canadians, including individuals from underrepresented backgrounds, access new employment opportunities.

The demand for cyber security professionals is surging, and there is a shortage of cyber skills around the globe. As such, developing and retaining cyber talent is essential for Canadian businesses and government. Canada already has a highly skilled cyber security workforce, but, by making further investments, we can ensure that Canadian companies have access to the staff they need to continue to grow and innovate. Investing in cyber security talent also aligns with the evolving demands of the workforce and fosters a more diverse and adaptable workforce capable of navigating industry transitions.

The Government of Canada will work with partners in other orders of government, academia, and the private sector to develop a skilled and diverse cyber security talent pipeline. This will include improved educational opportunities, including expanded private sector apprenticeship and training programs. These programs will help both youth seeking to forge careers in cyber security, as well as mid-career workers looking to up-skill and re-skill. In addition, the Government of Canada will explore support for programs aimed at ensuring the participation of underrepresented groups.

In addition, through the Cyber Security Cooperation Program[30] (CSCP), Public Safety Canada[31] (PS) will provide grants and contributions to a range of initiatives aimed to reduce cybercrime against Canadians, strengthen Canada's ability to protect its critical infrastructure, increase Canadians' cyber security awareness, augment Canadians' cyber security skills, and improve Canada's competitiveness in the global economy.

29 https://ised-isde.canada.ca/site/upskilling-industry-initiative/en
30 https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-en.aspx
31 https://www.publicsafety.gc.ca/index-en.aspx

The Government of Canada will continue to increase Canada's cyber workforce through programs like Express Entry[32], which allows skilled foreign workers to come to Canada and work in their fields of expertise.

The Canadian Centre for Cyber Security[33] (Cyber Centre) provides the Government of Canada with a dedicated home for cyber expertise. The Cyber Centre's Learning Hub[34] has helped develop the Government's cyber workforce skills while also helping to shape Canadian post-secondary institutions' curricula to better meet the demands of the labour market. The Communications Security Establishment Canada[35] (CSE) and the Cyber Centre work to encourage under-represented groups to pursue education and careers in science, technology, engineering and mathematics (STEM) through community outreach.

Objective 2.3: Identify and Support Targeted Areas of Research to Meet Canadian Needs

Home-grown cyber innovation makes Canada more secure.

Canada is a world leader in emerging technologies such as quantum computing and artificial intelligence. As part of a global market, however, Canadians obtain many cyber security products from foreign vendors. To bolster Canada's global competitiveness, cyber resilience, and economic security, the Government of Canada will work with other levels of government and academia to boost research and innovation in support of Canada's cyber security industry. The Government of Canada will also continue to work with groups, like CANARIE[36], that help secure Canada's research and education ecosystems.

> The Government of Canada is taking steps to protect Canada's research ecosystem by implementing the new Policy on Sensitive Technology Research and Affiliations of Concern[37] that protects our research while ensuring that Canadian research remains open and internationally collaborative. In future, the work of Canada's new Research Security Centre[38] will guide the implementation of the National Security Guidelines for Research Partnerships[39] in order to protect Canadian innovation, including in cyber technology.

32 https://www.canada.ca/en/immigration-refugees-citizenship/services/immigrate-canada/express-entry.html
33 https://www.cyber.gc.ca/en
34 https://www.cyber.gc.ca/en/education-community/learning-hub
35 https://www.cse-cst.gc.ca/en
36 https://www.canarie.ca/
37 https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern
38 https://www.canada.ca/en/services/defence/researchsecurity/about.html
39 https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships

The Government of Canada is also investing in securing the data of Canadians by modernizing its cryptographic systems and implementing quantum-safe technologies. Canada's National Quantum Strategy[40] will help ensure the privacy and cyber security of Canadians through support for research and talent development, as well as a national secure quantum communications network and a post-quantum cryptography initiative. Building on this, the Government of Canada will develop a cryptography action plan to guide further efforts, helping to better secure communications and promote cryptographic research.

The newly funded Cybersecurity Attribution Data Centre (CADC) at the Canadian Institute of Cybersecurity (CIC)[41] at the University of New Brunswick (UNB)[42] is an excellent example of how partnerships with academia can increase Canada's research and innovation capabilities while contributing to our national and economic security.

However, defending against cyber threats requires more than just technological research. We also need to understand cyber threats in their broader criminal and economic contexts so that we can find ways to undercut the incentives that drive cyber criminals. This will require collaboration with civil society and academia to foster the research needed to inform policy.

40 https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy
41 https://www.unb.ca/cic/
42 https://www.unb.ca/

Pillar 3: **Detect and Disrupt Cyber Threat Actors**

As our lives and businesses have moved online, Canadians and Canadian industry have felt the growing impact of cyber threats. Cybercriminals have targeted our critical infrastructure, government networks, hospitals, and our industrial base. Cybercrime, and, in particular, ransomware continue to be the number one cyber issue affecting all levels of Canadian society. Preventing cybercrime is critical to Canadians' public safety, national security, and economic prosperity.

To reduce the number and impact of cyber incidents, we need to strengthen our defences and make Canada a more difficult target for hostile actors. In practice, this means improving our ability to deter, detect, identify, disrupt, and defend against the full range of cyber threats.

The Government of Canada will work with partners, including all levels of law enforcement, to better protect Canadians from cybercriminals, including critical government and private sector critical infrastructure. This will include fostering the widespread adoption of strong cyber security standards and practices, increasing Canadian threat-monitoring capabilities to better detect incursions when they occur, and encouraging the sharing of threat intelligence and information across economic sectors to ensure a better view of the threats facing Canada. The Government of Canada will also continue to foster a coordinated response to cyber incidents.

Objective 3.1: Identify, Deter, and Defend Against Cyber Threats

Cyber threats to Canada's national and economic security continue to grow every year.

The Government of Canada takes direct action in international cyberspace to counter threats to Canada and Canadians, and to impose costs on malicious cyber actors.

> Under its cyber operations mandate, the Communications Security Establishment Canada[43] (CSE) conducts cyber operations against foreign interference and the hostile activities of state actors. CSE has also countered sophisticated cybercrime operations and disrupted foreign-based extremist activity. CSE and the Canadian Armed Forces[44] (CAF) engage jointly in defensive and offensive cyber operations, often in partnership with allies. The Government of Canada is also strengthening its military-to-military relationships to build on allies' unique skills and insights.

43 https://www.cse-cst.gc.ca/en
44 https://forces.ca/en/

The Canadian Security Intelligence Service[45] (CSIS) also has a role in protecting Canada from national security cyber threats, including the hostile activities of state actors. Using its intelligence collection and threat reduction mandates, bolstered by its array of international partnerships, CSIS investigates cyber threats of national security concern, thwarts malicious cyber actors, and provides intelligence assessments and advice across the federal government.

The Royal Canadian Mounted Police's[46] (RCMP) Federal Policing Cybercrime Program investigates cyber-related criminal activity and threats to national security. This includes cybercrime directed against institutions of government, critical infrastructure of national importance, and key Canadian institutions and business assets.

To reinforce these efforts, the Government of Canada will build and strengthen partnerships beyond the federal government. For example, the Government of Canada, through the Canadian Cyber Defence Collective (CCDC), will bring together industry experts, academia, and other levels of government to examine challenges and solutions to national-level cyber security issues.

The Government of Canada recognizes that cyber security readiness varies across the country. Indigenous communities, as well as small and rural municipalities, do not always have the tools and resources needed to fully protect their systems and information. The Government of Canada will explore ways to reduce this inequality through targeted investments, using mechanisms such as Public Safety Canada's[47] Cyber Security Cooperation Program[48] (CSCP).

In addition, as threat actors become more sophisticated, it is increasingly important that we use threat intelligence to block threats before they can harm their intended targets. In 2022, the Government of Canada laid the groundwork for filtering of malicious activity at the level of Canadian internet service providers (ISPs) through initial reporting requirements. The Canadian Radio-television and Telecommunications Commission[49] (CRTC) also intends to implement mandatory rules for blocking botnets by ISPs following consultations. Further collaboration will be needed to develop and expand threat-blocking capabilities to provide automatic protection to Canadians.

45 https://www.canada.ca/en/security-intelligence-service.html
46 https://www.rcmp-grc.gc.ca/
47 https://www.publicsafety.gc.ca/index-en.aspx
48 https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-en.aspx
49 https://crtc.gc.ca/eng/home-accueil.htm

Objective 3.2: Improve Capacity to Combat Cybercrime

Canadians expect to access a safe and secure digital Canada.

Cybercrime encompasses a broad range of malicious activities, such as ransomware and cyber-enabled fraud, and uninvited interference in networks and systems belonging to organizations, including Canada's most vital cyber systems and critical infrastructure. It is perpetrated by states, organized crime groups, as well as less sophisticated cybercriminals who purchase cybercrime services to carry out their activities.

Ransomware is the most prevalent and disruptive form of cybercrime in Canada; the majority of requests for assistance received by the National Cybercrime Coordination Centre[50] (NC3) relate to ransomware. Canadians also continue to report record losses from cyber-enabled fraud, and this cost is growing. This is money taken away from fuelling Canada's economic growth. To protect Canadians and secure growth of Canada's economy, a strong response is required.

> The Royal Canadian Mounted Police's[51] (RCMP) National Cybercrime Coordination Centre[52] (NC3) coordinates and enables cybercrime investigations across jurisdictions, both within Canada and abroad; provides investigative advice and technical capabilities to other law enforcement organizations; and produces actionable cybercrime intelligence for Canadian police.
>
> The RCMP also engages with law enforcement partners to address cybercrime. This includes engagement with Europol's European Cybercrime Centre[53] (EC3), the U.S.-based National Cyber-Forensics and Training Alliance[54] (NCFTA), as well as through RCMP Liaison Officers and Analysts deployed in strategic locations. The RCMP's NC3 is also part of the International Cyber Offender Prevention Network[55]. The network includes law enforcement agencies from 26 countries and is aimed at preventing cybercrime offender activity through educational resources, social media campaigns, and other innovative measures.

50 https://www.rcmp-grc.gc.ca/en/nc3
51 https://www.rcmp-grc.gc.ca/
52 https://www.rcmp-grc.gc.ca/en/nc3
53 https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
54 https://www.ncfta.net/
55 https://www.europol.europa.eu/partners-collaboration/networks/intercop-international-cyber-offender-prevention-network

Currently, the Government of Canada conducts cyber operations to reduce the ability of foreign cybercriminals to launch ransomware incursions and profit from the sale of stolen information. The Government of Canada is also exploring additional ways to further discourage ransomware payments and impose costs on cybercriminals. This includes improving Canada's approach to cyber insurance policies to make cybercriminal business models, particularly ransomware, less profitable. The Government of Canada is also committed to working with industry to dissuade businesses from paying ransoms, in accordance with the Counter Ransomware Initiative[56] (CRI).

In addition, the Government of Canada is committed to bolstering Canada's national security and law enforcement capacity. One important means of doing so will be education. The Government of Canada will help improve the ability of law enforcement to support victims of cybercrime, using a victim-centric approach.

Cybercrime transcends borders and often involves hostile states or organized crime groups. The Government of Canada will continue to collaborate with international allies to impose costs on cybercriminals and disrupt the business model of cybercrime.

Reporting is critical to the Government of Canada's efforts to better understand the cyber threat landscape, disrupt criminal activities and prevent incursions, as well as dismantle cybercriminal infrastructure. The Government of Canada urges those who have been targets of cybercrime to contact their local police services as well as the Canadian Anti-Fraud Centre[57] (CAFC). The Government of Canada will be releasing a new cybercrime and fraud reporting system[58] so it's easier for Canadians to report cybercrime and fraud to law enforcement, and for information to be shared amongst law enforcement.

Objective 3.3: Make Critical Systems More Resilient

Critical infrastructure underpins services Canadians use every day.

Critical infrastructure owners and operators are the targets of persistent, well-funded, and sophisticated cyber activities. Malicious cyber actors can inhibit or damage Canadian critical infrastructure, such as water treatment plants, energy grids, pipelines, transportation infrastructure, and agricultural equipment. They can also disrupt essential services, such as healthcare and supply chains, putting the safety, security, and

56 https://www.canada.ca/en/public-safety-canada/news/2023/11/international-statement-counter-ransomware-initiative-joint-statement-on-ransomware-payments.html
57 https://antifraudcentre-centreantifraude.ca/index-eng.htm
58 https://www.rcmp-grc.gc.ca/en/new-cybercrime-and-fraud-reporting-system

livelihood of individual Canadians at risk. Moreover, cyber incidents erode trust in the networks and operating systems in use, as well as in the public and private institutions responsible for safeguarding personal and sensitive information. The high economic and societal costs of cyber incidents underscore the importance of securing Canada's critical infrastructure.

> The Government of Canada has two complementary procedures for when a cyber incident takes place. First, the Government of Canada Cyber Security Event Management Plan (GC CSEMP)[59] provides a framework to manage cyber security events that affect, or threaten to affect, the Government of Canada's ability to deliver programs and services to Canadians. Second, the Federal Cyber Incident Response Plan (FCIRP)[60] is a coordination plan and information-sharing framework for when the Government of Canada is responding to significant cyber incidents affecting non-Government of Canada systems that are essential to the health, safety, security, defence, or economic well-being of Canadians.

The Government of Canada recognizes the importance of working collectively to strengthen Canada's critical infrastructure to deter cyber threats. Canada's critical infrastructure is owned and managed by a variety of organizations, so all levels of government together with private industry must collaborate to ensure that information, operational technology, industrial control systems, and software supply chains are secure.

The Government of Canada will continue working with partners and industry stakeholders as part of the Global Coalition on Telecommunications[61] to foster diverse supply chains as well as secure and interoperable standards in the telecommunications sector. The Government of Canada will also support the work done by cyber security organizations and forums, such as the Canadian Internet Registration Authority (CIRA) Canadian Shield[62], Rogers Cybersecure Catalyst[63], Canadian Cyber Threat Exchange[64] (CCTX), and CANARIE[65]. In the future, the Canadian Cyber Defence Collective (CCDC) will also serve as an important forum for critical infrastructure discussions across sectors.

---

59 https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html
60 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fdrl-cbr-ncdnt-rspns-pln-2023/index-en.aspx
61 https://ised-isde.canada.ca/site/ised/en/global-coalition-telecommunications-joint-statement-intent
62 https://www.cira.ca/en/canadian-shield/
63 https://cybersecurecatalyst.ca/
64 https://cctx.ca/
65 https://www.canarie.ca/

Additionally, the Government of Canada will continue to improve its ability to defend and recover from cyber incidents. The Canadian Centre for Cyber Security[66] (Cyber Centre) is working to share many advanced cyber defence capabilities to a growing number of critical infrastructure owners and operators. In this way, the Cyber Centre will strengthen critical non-government services, like banking and telecommunications.

66 https://www.cyber.gc.ca/en

Conclusion

Canada’s 2025 National Cyber Security Strategy seeks to secure Canada’s digital future. It maps out the Government of Canada’s ongoing and future efforts to enhance cyber security through national and international efforts.

Cyber security is a whole-of-society responsibility. The Government of Canada calls on other levels of government, Indigenous communities, the private sector, and academia to be partners in the creation of a series of action plans, each of which would work to address a key challenge identified in this strategy. This broad collaboration is needed to ensure that the action plans improve Canada’s national cyber resilience at all levels, not just the Government of Canada.

This approach marks a commitment from the Government of Canada to ongoing discussions with stakeholders to help design and implement initiatives that further protect Canadians. By implementing the Strategy through a series of action plans over time, Canada will have a flexible mechanism ensuring timely responses to an ever-changing cyber environment. Together, we will ensure that cyberspace is safe, open, secure, stable, and accessible to all Canadians.

Cyber Security Roles and Responsibilities in the Government of Canada

These entities hold core public-facing cyber roles and functions, serving as the primary windows into the Government of Canada — the Canadian Centre for Cyber Security, Public Safety Canada, the Royal Canadian Mounted Police and the Canadian Security Intelligence Service. Many more have subject-specific roles that involve public engagement or partnership of different kinds.

Accompanying this Strategy is a call to partnership. For Canadians and Canadian organizations of all sizes to report cyber incidents and cybercrime — of all kinds. To leverage funding to advance cyber innovation, and to help communities and businesses become more cyber secure. To inform policy and regulation. To improve cyber hygiene, digital literacy, and public awareness. Here is where stakeholders can turn.

Core Public Facing Roles

Canadian Centre For Cyber Security (Communications Security Establishment Canada)

Report an incident (organizations)

- Incident reporting and mitigation

Public awareness

- Source of general, threat- and sector-specific cyber security advice, guidance, and services for Canadians and Canadian organizations
- Cyber security public awareness

Operations

- Canadian Cyber Defence Collective (CCDC) co-chair (Operations chair)

Public Safety Canada

Cyber funding

- Cyber security funding for small and medium enterprises

Policy

- National cyber security policy lead
- National critical infrastructure (CI) security policy lead
- Canadian Cyber Defence Collective (CCDC) co-chair (Policy chair)

Royal Canadian Mounted Police

Report an incident

- Cybercrime and fraud reporting and coordination via the National Cybercrime Coordination Centre (NC3) and Canadian Anti-Fraud Centre (CAFC)
- Suspicious incident reporting via the National Critical Infrastructure Team

Public awareness

- Cybercrime prevention and public awareness

Operations

- Investigate major cybercrime threats to Canada

Canadian Security Intelligence Service

Public awareness

- Conduct engagement with public and private sector entities on national security cyber threats

Operations

- Investigate and take measures to mitigate or reduce national security cyber threats targeting Canadian entities

Additional Public Facing Cyber Roles

Innovation, Science and Economic Development Canada

Report an incident

- Spam reporting

Policy

- National policy lead for the development and commercialization of new technologies (includes information and communications technologies [ICT] and telecommunications)

Natural Resources Canada

Operations

- Provide energy sector expertise and connect stakeholders across government, industry, academia, and others to enhance the cyber security resilience of critical energy infrastructure
- Facilitate and advance the timely sharing of information among energy sector stakeholders in an effort to strengthen the resilience of critical energy infrastructure

Policy

- Policy lead for cyber security of critical energy infrastructure, including cross-border (Canada-U.S.) energy infrastructure

Transport Canada

Report an incident

- Cyber security incident reporting via the Transport Canada Situation Centre

Policy

- National policy lead for marine, aviation, rail and road transportation system safety and security

National Research Council

Cyber funding

- Cyber security research and development funding

Public Services and Procurement Canada

Policy

- Procurement policy lead (security requirements – cyber security)

Standards Council of Canada

Policy

- Cyber security standards lead

Federal Organizations with Non-Public Facing Cyber Roles

Some of the most critical functions to Canada's national cyber defence and security occur outside of public view — on systems and networks, in coordination with critical infrastructure partners, and with allies around the world. The Government of Canada is active in offensive and defensive cyber operations against malicious threat actors — a function of growing importance to both economic and national security. Engagement in foreign cyber policy and norms development is increasing year-over-year. And a multi-departmental effort defends government networks and keeps essential services online.

- Department of National Defence
- Global Affairs Canada
- Privy Council Office
- Shared Services Canada
- Treasury Board of Canada Secretariat
- Finance Canada

Federal Critical Infrastructure Sector Regulators

- Canada Energy Regulator
- Canadian Nuclear Safety Commission
- Canadian Radio-Television and Tele-communications Commission
- Canadian Transportation Agency
- Office of the Superintendent of Financial Institutions

Glossary

Artificial Intelligence
The subfield of computer science concerned with developing intelligent computer programs that can solve problems, learn from experience, understand language, interpret visual scenes, and, in general, behave in a way that would be considered intelligent if observed in a human.

Critical Infrastructure
Processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.

Cybercrime
Any crime where a cyber element (i.e., the Internet and information technologies such as computers, tablets, or smart phones, etc.) has a substantial role in the commission of a criminal offence. In broad terms, the RCMP breaks cybercrime into two categories: technology-as-target; and technology-as-instrument. A crime committed with the aid of, or directly involving, a data processing system or computer network. The computer or its data may be the target of the crime, or the computer may be the tool with which the crime is committed.

Cyber Incident
Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete or render unavailable any computer network or system resource.

Cyber Operation
Action taken in and through cyberspace to disrupt and interfere with or defend against the ability of a threat actor to operate online.

Cyber Resilience
The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, malicious cyber activities, or compromises on systems that use or are enabled by cyber resources.

Cyber Security
The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from malicious cyber activities, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

Cyberspace
The electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 3 billion people are linked together to exchange ideas, services, and friendship.

Cyber Threat
Any circumstances or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Cryptography, including Encryption
Cryptography is a discipline that includes the principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. The conversion of the information to hide its content from unauthorized individuals is referred to as encryption. The conversion of information back to its original form is decryption.

Digital Economy
The digital economy incorporates all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services and data. It refers to all producers and consumers, including government, that are utilizing these digital inputs in their economic activities.

Industrial Control System
Industrial Control System (ICS) is a general term that encompasses several types of control systems that are often found in the industrial sectors and critical infrastructures. ICS are the automated systems used to deliver essential services to Canadians and consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). ICS are responsible for everything from the electrical current that powers our computers, to the water that flows through our buildings, to the traffic lights that manage our daily commute.

Internet of Things
The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Quantum Computing
Quantum computers are experimental devices that are designed to process certain calculations very quickly. Whereas a classical computer works with ones and zeros, a quantum computer will have the advantage of using ones, zeros and “superpositions” of ones and zeros. Certain difficult tasks that have long been thought impossible for classical computers will be achieved quickly and efficiently by a quantum computer.

Ransomware
Malicious software that denies an individual or organization access to key files and systems until a ransom is paid to the cybercriminal. Ransomware involves encryption, locked screens and/or other methods to prevent file access and extort victims, such as leaking sensitive data online, and ransomware payments often involve cryptocurrency.

Secure-by-Design
Secure-by-Design means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure.