UNCLASSIFIED

# Communications Security Establishment

# Part C
# Institutional Report to the Public Inquiry on Foreign Interference

## June 2024

## CSE and foreign interference at a glance

The Communications Security Establishment (CSE) is Canada's foreign signals intelligence agency, and technical authority for cyber security and information assurance. CSE intercepts and analyzes foreign electronic communications to provide the Government of Canada with unique information about foreign threats to Canadian security and prosperity and important insights to support the execution of foreign policy and other related decision making.

Hostile state actors are attempting to influence and interfere with Canada's society and democracy in various ways, including espionage, malicious cyber activity and online disinformation. Countering this activity requires a whole of government approach, which CSE actively supports by:

- leveraging all aspects of its mandate (foreign intelligence, cyber security, foreign cyber operations and technical and operational assistance) to counter hostile activities by state actors;
- providing foreign intelligence to Government of Canada decision makers about the intentions capabilities and activities of foreign-based threat actors;
- participating in the Security and Intelligence Threats to Elections (SITE) Task Force;
- defending Canada's federal elections infrastructure from malicious cyber activity;
- proactively helping democratic institutions improve their cyber security;
- sharing unclassified threat assessments with the public; and
- sharing information to help Canadians:
    - identify disinformation
    - protect their privacy and security online.

Since the 2015 federal election, CSE has been ensuring that strong and effective cyber defence measures are in place to protect Elections Canada's systems, and others that support Canada's democratic processes. Through its historical monitoring of foreign interference, the organization has produced multiple reports about the risks that foreign interference pose to the various parts of Canada's democratic process, including the safeguards created to protect them.

For more information, please refer to CSE's Institutional Reports from September 2023 and January 2024.

## 1. A listing and description of all major instances of suspected foreign interference targeting Canada's democratic processes, including summary, dates, target, country involved, key players, information flow and any responses taken.

Answer to be provided separately.

## 2. A listing and description of all existing means at the disposal of each government department and agency to detect, deter and counter any foreign interference activities, including any relevant changes to or evolution in these means.

### 2.1 Mandate Overview

Prior to August 2019, CSE operated under the *National Defence Act* with a three-part mandate:

A. To acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
B. To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;
C. To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Following the establishment of the *CSE Act* on August 1st, 2019, the three pre-existing aspects of CSE's mandate were expanded to five. Sections 15-20 of the *CSE Act* outline CSE's mandate:

- foreign intelligence (s.16);
- cybersecurity and information assurance (s.17);
- defensive cyber operations (s.18);
- active cyber operations (s.19);
- technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence (s.20).

CSE recognizes that foreign interference is a constant threat that Canada faces, not solely during election periods. All aspects of CSE's mandate contribute to a whole-of-government approach to detect, deter and counter activities such as foreign interference, espionage, and malicious cyber activity.

*2.1.1 Foreign Intelligence (s.16)*

The foreign intelligence aspect of the mandate enables CSE's signals intelligence (SIGINT) activities. SIGINT is the interception, decoding and analysis of communications and other electronic signals in order to collect intelligence related to foreign entities. SIGINT activities are informed by Government of Canada Intelligence Priorities established by Cabinet, and the Ministerial Directive on Intelligence Priorities, both of which include foreign interference. The foreign intelligence that CSE collects and reports upon provides insights to decision makers on the activities, intentions, and interests of various foreign entities.

CSE currently leverages three Ministerial Authorizations (MAs) to enable its foreign intelligence activities. They are distinguished from one another by the types of acquisition technique they authorize, not by the type of foreign intelligence that is sought. All three of them serve to enable CSE's ability to acquire a broad variety of foreign intelligence, including, but not limited to, foreign intelligence on foreign interference. Details of these MAs are provided in the Classified Annex to Question 5.

*2.1.2 Cybersecurity and Information Assurance (s.17)*

The cybersecurity and information assurance aspect of the mandate enables the provision of cybersecurity advice, guidance and services to help defend federal systems and non-federal systems designated by the Minister of National Defence as being of importance to the Government of Canada (systems of importance). As an example, CSE's Canadian Centre for Cyber Security (Cyber Centre) deploys sensors on endpoint devices (e.g. servers, laptops, desktops) that can automatically detect malicious activity like malware to defend against cyber threats.

CSE currently has three MAs that are used to help fulfill the cybersecurity and information assurance aspect of its mandate. One is used to protect federal systems, the other two are used to protect systems of importance. All three of these MAs authorize the conduct of certain cybersecurity services on federal systems or systems of importance to defend against cybersecurity threats of any origin. Details of these MAs are provided in the Classified Annex to Question 5.

It is under the cybersecurity aspect of its mandate that CSE provides advice and guidance to political parties, Canadians and voters during election times. In particular, CSE provided advice and assistance to Elections Canada during the 2019 and 2021 elections (please see Question 4 for additional details). CSE also provided advice and guidance, as well as a support hotline, to political parties during the elections. Additional information can be found in Section 2.3.3 of CSE's January 2024 Institutional Report, and in response to Question 7 of this Institutional Report.

*2.1.3 Defensive Cyber Operations (s.18)*

Defensive cyber operations (DCOs) allow CSE to take online actions to defend Canadian infrastructure from foreign cyber threats by disrupting their activities. During the 2019 and 2021 elections, CSE was prepared to conduct defensive cyber operations to protect Election Canada's systems, if it became necessary.

CSE currently leverages one MA to enable its DCO activities. Details of this MA are provided in the Classified Annex to Question 5.

*2.1.4 Active Cyber Operations (s.19)*

Active cyber operations (ACOs) allow CSE to take online action to disrupt the capabilities of foreign threats to Canada.

CSE currently leverages three MAs to enable its ACO activities. Details of these MAs are provided in the Classified Annex to Question 5.

*2.1.5 Technical and Operational Assistance (s.20)*

Under the technical and operational assistance aspect of its mandate, CSE provides assistance to federal law enforcement or security partners, the Canadian Forces, and the Department of National Defence. While operating under a Request for Assistance, CSE acts under the legal authorities and restrictions of the requesting agency, such as a court-issued warrant. Under this aspect of the mandate, CSE may help its domestic partners counter or identify foreign interference.

## 3. A listing and description of all policy proposals, legislative plans and resource requests related to foreign interference, including but not limited to memos to the Deputy Minister (or equivalent) or Assistant Deputy Minister (or equivalent). At a minimum, this should include the date of the request, date of decision (where applicable), a summary of the proposed changes and the outcome of the request.

In the period of September 2018 to present, CSE has participated or led the development of Memoranda to Cabinet, Treasury Board Submissions and official Budget Proposals with a nexus to foreign interference in the context of protecting Canada's democratic processes and

institutions. However, this content and related details cannot be provided as such information would disclose Cabinet Confidences.

Recent federal budgets have allocated resources to CSE in support of its broad mandate, which include activities that directly or indirectly support the goal of mitigating, disrupting, or preventing foreign interference and/or protecting democracy. For example:

**Budget 2018, announced an investment of $507.7 million over five years, and $108.8 million per year thereafter, to fund a new National Cyber Security Strategy focused on three goals**:

1. Ensure secure and resilient Canadian cyber systems by enhancing the Government of Canada's ability to investigate cybercrime, developing threat assessments, keeping critical infrastructure safe, and work in collaboration with the financial and energy sectors on bolstering their cyber security;
2. Invest in an innovative and adaptive cyber ecosystem by supporting work-integrated cyber learning placements for students and helping businesses improve their cyber security posture through the creation of a voluntary cyber certification program; and,
3. Strengthen leadership, governance and collaboration by taking the lead, both at home and abroad, to advance cyber security in Canada, working closely with provincial, territorial, private sector and trusted international partner.

- This investment **included $155.2 million over five years, and $44.5 million per year ongoing, to CSE to create a new Canadian Centre for Cyber Security (CCCS)**, a single, unified Government of Canada source of expert advice, guidance, services and support on cyber security operational matters, providing Canadian citizens and businesses with a clear and trusted place to turn to for cyber security advice.
- These investments have a nexus to the issue of foreign interference because foreign states seek to use the global information infrastructure to advance their own strategic objectives to the detriment of Canada's national interests and security. Foreign adversaries are increasingly using cyber tools to target democratic processes around the world. Disinformation has become ubiquitous in national elections, and adversaries are using generative artificial intelligence to create and spread fake content, posing threats to democratic processes.
- This is why secure and reliable connectivity is a necessity, as it underpins the delivery of critical services and systems such as health care, financial transactions, safe transportation, emergency communications, and democracy. CSE's CCCS supports a cyber resilient Canada, which bolsters our capacity to withstand and counter foreign interference.
- The CCCS was subsequently launched on October 1, 2018, and today is a trusted source of expertise on cyber security matters, including foreign interference. Of note, the CCCS leads the publication of a biannual assessment of cyber threats to Canada's democratic process, helping to inform Canadians and build resilience to counter such malign activity.

**Budget 2018 also announced $225M over four years and $62.1M ongoing to preserve Canada's Foreign Signals Intelligence Capability**

- CSE's authority to collect foreign signals intelligence helps inform the Government of Canada on matters of security, national defence and international affairs, reflecting the priorities set by the Government.
- These priorities include combatting foreign interference and protecting Canada's democracy.
- Foreign signals intelligence provides the Government of Canada with insight into the plans, intentions and capabilities of state actors (or their proxies) to conduct interference or influence activities against Canadian interests.

**Budget 2019 announced an investment of $4.2 million over three years, starting in 2019–20, to provide cyber security advice and guidance to Canadian political parties and election**

**administrators,** as part of broader measures to further strengthen and safeguard Canada's democratic institutions.

- The compromise of cyber systems used by political parties, or the cyber systems that support the work of elections administrators, has the risk of disrupting or undermining public confidence in electoral processes.
- To help increase the security of cyber systems used by Canadian political parties and elections administrators, CSE provides technical advice, guidance, and services. This includes:
  - network architecture review and advice;
  - security review of IT requests for proposals; and,
  - guidance on, and assessment of, third party cyber security service providers that meet a key list of IT security standards.
- CSE also works closely with Elections Canada to protect its infrastructure, as well as with major political parties to increase their cyber security awareness. This includes offering briefings, training resources, consultations, and tailored advice.

**Budget 2022 announced $875.2 million over five years, beginning in 2022-23, and $238.2 million ongoing** for additional measures to address the rapidly evolving cyber threat landscape. These measures include:

- $263.9 million over five years, starting in 2022-23, and $96.5 million ongoing to enhance CSE's abilities to launch cyber operations to prevent and defend against cyber attacks;
- $180.3 million over five years, starting in 2022-23, and $40.6 million ongoing to enhance CSE's abilities to prevent and respond to cyber attacks on critical infrastructure;
- $178.7 million over five years, starting in 2022-23, and $39.5 million ongoing to expand cyber security protection for small departments, agencies, and Crown corporations; and,
- $252.3 million over five years, starting in 2022-23, and $61.7 million ongoing for CSE to make critical government systems more resilient to cyber incidents.

Canadian academics are some of the leading researchers in important emerging and disruptive technologies, including quantum computing and artificial intelligence. This expertise can be leveraged to ensure Canada's security and intelligence community stay one step ahead of our adversaries.

- Budget 2022 also announced $17.7 million over five years, starting in 2022-23, and $5.5 million thereafter until 2031-32 for CSE to establish a unique research chair program to fund academics to conduct research on cutting-edge technologies relevant to CSE's activities. Researchers awarded the grants will split their time between peer-reviewed publishable research and classified research at CSE.

**Budget 2024 announced $917.4 million over five years, and $145.8 million per year ongoing**, for CSE and Global Affairs Canada (GAC) to enhance their intelligence and cyber operations programs to protect Canada's economic security and respond to evolving national security threats.

## 4. A listing and description of all existing arrangements and undertakings (including Memoranda of Understanding) between government departments and agencies, and with international partners, aimed at detecting, deterring, and countering foreign interference activities, including the dates that the arrangements have been in place.

CSE's closest intelligence-sharing arrangements are with other intelligence agencies that are part of the "Five Eyes" (FVEY) group of countries – namely the United States, the United Kingdom, Australia and New Zealand. While CSE has not identified any specific agreements with its FVEY partners regarding foreign interference, it continues to collaborate with its partners to

identify and defend against common threats such as foreign interference in democratic processes and institutions.

CSE's country-to-country international Memoranda of Understanding (MoUs) do not reference detecting, deterring, or countering foreign interference activities, instead focusing on enabling the sharing of information, tradecraft, and technologies in general terms. Thus, there are no formal arrangements or undertakings between CSE and international partners that specifically focus on foreign interference, however it is a common priority where CSE and its partners benefit from collaboration.

CSE continues to participate in the SITE Task Force to identify foreign threats that aim to interfere with Canada's democratic processes and institutions. Additional information regarding CSE's participation on the SITE Task Force was provided in Section 2.3.1 of CSE's Institutional Report from January 2024.

The Cyber Centre has identified one arrangement or undertaking between CSE and Elections Canada that is relevant to this request.

### 4.1 Arrangements or undertakings with Elections Canada

In support of the 43rd and 44th General Elections, CSE stood up operations to formally coordinate and engage Cyber Centre resources to provide Elections Canada advice, guidance, and cyber defence tools. Additional information regarding these operations was provided in Section 2.3.3 of CSE's Institutional Report from January 2024.

The Cyber Defence Operations Working Group (CDOWG) is a partnership between the Cyber Centre and Elections Canada. The purpose of the CDOWG is to provide an operational framework for cybersecurity information sharing and for the management of cyber security events (including cyber threats, vulnerabilities, or security incidents) that impact or threaten to impact general elections (GE).

Following the 44th General Election (GE44), Elections Canada (EC) and the Cyber Centre initiated a dedicated series of bi-monthly CDOWG touchpoints to support Elections Canada's inter-GE operational posture, implement lessons learned from GE44, and provide advice and guidance on major, long-term, and emerging Elections Canada cybersecurity issues and initiatives.

Compared to CDOWG meetings held during general elections that are by necessity more operational and tactical in nature, the current CDOWG forum permits Elections Canada and the Cyber Centre to collaborate at the strategic level well in advance of the next GE.

### 4.2 Additional activities

The Cyber Centre supports ongoing efforts to enable cyber resilience in Canadian research, economic, and investment activities. Although these activities are not explicitly designed to deter, detect, or counter foreign interference activities, they (like all of the Cyber Centre's overall cybersecurity activities) indirectly support that objective by improving the overall cybersecurity posture of systems of importance.

## 5. A listing and description of all warrant applications related to foreign interference submitted to the Minister of Public Safety, and ministerial authorizations submitted to the Minister of National Defence, including date submitted to the Minister, date approved by the Minister, date of decision by the Federal Court and, if applicable, the reasons for decision.

### 5.1 Evolution of Ministerial Authorizations from *NDA* to *CSE Act*

The ministerial authorization (MA) regime has existed since 2001 with the enactment of Part V.1 of the *National Defence Act* (NDA), and was continued in the *Communications Security Establishment Act* (*CSE Act*) in 2019. The NDA scheme provided for the issuance of

authorizations by the Minister of National Defence when CSE's foreign intelligence and cybersecurity activities risked intercepting private communications.

The *CSE Act* scheme modernized the authorization regime. While the previous regime focused on the interception of private communications, the *CSE Act* regime requires that CSE obtain authorizations for foreign intelligence and cybersecurity activities when these activities risk contravening any Act of Parliament or involve the acquisition of information from or through the global information infrastructure that interferes with the reasonable expectation of privacy of a Canadian or a person in Canada. Furthermore, it set outs the standard that must be met in order for the Minister to issue an authorization, i.e. reasonable grounds to believe that it would be reasonable and proportionate to do so having regard to the nature of the activities and their objectives. The *CSE Act* also added another key element to the regime, that foreign intelligence and cybersecurity authorizations issued by the Minister are not valid until they are approved by the independent and quasi-judicial Intelligence Commissioner (IC).

**5.2 Ministerial Authorization Approval Process**

MAs are instruments issued by the Minister of National Defence (MND) that provide CSE with the authority to conduct activities in support of its mandate that could risk contravening an Act of Parliament, or that may interfere with a reasonable expectation of privacy of a Canadian or person in Canada.

MAs are valid for up to one year. MAs must demonstrate that:

- the objective of activities are reasonable and proportionate;
- information acquired could not be reasonably obtained by other means (i.e., the activity is necessary);
- information is retained for no longer than necessary; and
- measures are in place to protect the privacy of Canadians and persons in Canada.

MAs under section 16 (foreign intelligence) and section 17 (cybersecurity) of CSE's mandate must be reviewed by the IC. Once an MA package is approved by the MND these documents are sent to the IC for consideration. The IC reviews whether MND's conclusions are reasonable and issues a decision to either approve, not approve, or partially approve the activities described in the MA.

All foreign cyber operations activities require an MA. MAs under section 18 (defensive cyber operations) of CSE's mandate must be consulted with the Minister of Foreign Affairs. MAs under section 19 (active cyber operations) of CSE's mandate require the consent of the Minister of Foreign Affairs.

Additional information regarding the MA process was provided in Section 1.3.1 of CSE's Institutional Report from January 2024.

CSE's detailed list of MAs is available in A5: Classified Annex to Question 5.

## 6. A listing and description of the date, venue, participants and summary of discussion for all engagements by senior executives (ADM and above, including Ministers) with representatives of foreign governments (especially China, Russia and India) where the subject of foreign interference was raised.

CSE's closest intelligence-sharing relationships are with the Five Eyes (FVEY): the United States, the United Kingdom, Australia and New Zealand. CSE leverages the collective community expertise of the FVEY to satisfy Canada's foreign intelligence requirements, to protect our shared national interests, and to keep Canadians safe.

Further information is available in A6: Classified Annex to Question 6.

## 7. A listing and description of all education campaigns aimed at Parliamentarians and their staff, political parties, government employees at federal, provincial or municipal levels, diaspora groups, or the general public related to foreign interference.

As Canada's technical authority on cyber security, the Canadian Centre for Cyber Security (CCCS or Cyber Centre) is the single unified source of expert advice, guidance, services and support for Canadians and Canadian organizations. The following educational resources can help to reduce the risks associated with cyber threats to elections and contribute to the protection of Canada's democratic processes and institutions.

For additional information, please visit the Cyber Threats to Elections[1] web page.

### 7.1 Reports on Cyber Threats to Canada's Democratic Process

The Cyber Centre's reports on cyber threats to Canada's democratic process aim to inform Canadians about the global trends in cyber threat activity targeting national elections and their potential impacts on Canada.

*Cyber Threats to Canada's Democratic Process: 2023 Update*

> **Description:** The most recent iteration of CSE's Cyber Threats to Canada's Democratic Process, which provides an update to the 2021 and 2019 reports. Specifically, this report addresses cyber threat activity targeting elections, and the growing threat that generative AI poses to democratic processes globally and in Canada.
>
> **Target Audience:** General Public
>
> **URL:** https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

*Cyber Threats to Canada's Democratic Processes: July 2021 Update*

> **Description:** The third iteration of CSE's Cyber Threats to Canada's Democratic Process. This document reviews global trends in cyber threat activity against democratic processes (which is defined as including voters, political parties, and elections) and evaluates the threat to Canada, with special focus on the impacts of the COVID-19 pandemic.
>
> **Target Audience:** General Public
>
> **URL:** https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

*Cyber Threats to Canada's Democratic Processes: 2019 update*

> **Description:** The second iteration of CSE's Cyber Threats to Canada's Democratic process. This iteration focuses on cyber threat activity undertaken by foreign adversaries with the intention of interfering with democratic processes.
>
> **Target Audience:** General Public
>
> **URL:** https://www.cyber.gc.ca/en/guidance/2019-update-cyber-threats-canadas-democratic-process

### 7. 2 Published Guidance and Training - Cyber Threats to Elections

The Cyber Centre is committed to raising awareness of cyber threats to Canada and protecting the integrity of Canadian elections. The following is a list of select guidance and training

[1] https://www.cyber.gc.ca/en/guidance/cyber-threats-elections

materials designed to mitigate the impacts of cyber threats to elections, including with respect to members of political parties, voters and election authorities.

7.2.1 Published Guidance and Training for Political Parties

*Cyber security guide for campaign teams*

**Description:** This guide offers practical advice and guidance about cyber security that is applicable to all campaigns.

**Target Audience:** Political Parties

**URL:** https://www.cyber.gc.ca/en/guidance/cyber-security-guide-campaign-teams

*Security considerations when using social media in your organization*

**Description:** This document speaks to how the rapidly changing social media environment reveals new risks and challenges. It notes that all stakeholders should be informed of the changing threat environment and the security measures required to safeguard their social media activities.

**Target Audience:** Political Parties

**URL:** https://www.cyber.gc.ca/en/guidance/security-considerations-when-using-social-media-your-organization-itsm10066

7.2.2 Published Guidance and Training for Voters

*How to identify misinformation, disinformation and malinformation*

**Description:** This document offers consumers and organizations information on identifying misinformation, disinformation and malinformation (MDM) as well as implementing the appropriate security measures to counter it. Specifically, highlighted is how Artificial Intelligence (AI) may be used during elections to spread MDM aimed at damaging public trust in institutions and discrediting public figures

**Target Audience:** General Public – Voters

**URL:** https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300

*Social engineering*

**Description:** This document speaks to how social engineering attacks are also referred to as "human hacking" since threat actors leverage information they've found on the Internet and social media platforms to target individuals and organizations. These threat actors may try to influence users into doing something which gives them access to your environment, such as changing an account password.

**Target Audience:** General Public – Voters

**URL:** https://www.cyber.gc.ca/en/guidance/social-engineering-itsap00166

7.2.3 Published Guidance and Training for Election Authorities

*Cyber Security Guidance for Election Authorities*

**Description:** Introduces common threats to Canada’s electoral processes and provides guidance on protecting the systems and the people involved in these processes.

**Target Audience:** General Public – Election Authorities

**URL:** https://www.cyber.gc.ca/en/guidance/cyber-security-guidance-elections-authorities-itsm10020

*Cyber Security Playbook for Election Authorities*

**Description:** This cyber security playbook guides election authorities on anticipating, mitigating, and responding to threats that are specific to Canada's democratic processes. This playbook introduces baseline cyber security measures and best practices that you can implement to improve your organization's security profile. This playbook also provides a set of standards to reference as elections authorities continue to improve current systems and implement new ones.

**Target Audience:** General Public – Election Authorities

**URL:** https://www.cyber.gc.ca/en/guidance/cyber-security-playbook-elections-authorities-itsm10021

*Distributed denial of service attacks - Prevention and preparation*

**Description:** Distributed denial of service (DDoS) is a type of cyber attack in which threat actors aim to disrupt and prevent legitimate users from accessing a networked system, service, website, or application. This publication provides guidance on the actions you can take when a DDoS occurs and what you can do to mitigate the impact.

**Target Audience:** General Public – Election Authorities

**URL:** https://www.cyber.gc.ca/en/guidance/distributed-denial-service-attacks-prevention-and-preparation-itsap80110

*Security considerations for your website*

**Description:** This document introduces cyber security best practices that organizations should integrate into the design and maintenance of their website.

**Target Audience:** General Public – Election Authorities

**URL:** https://www.cyber.gc.ca/en/guidance/security-considerations-your-website-itsm60005

*Spotting malicious email messages*

**Description:** By learning about malicious emails and phishing attacks, you can help protect and secure your organization's information.

**Target Audience:** General Public – Election Authorities

**URL:** https://www.cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100

*Ransomware playbook*

**Description:** The information provided in this document is intended to inform and assist organizations with drawing down the risks, reducing the impacts, and taking preventative actions associated with ransomware attacks. This document is divided into two sections: (1) how to defend against ransomware and (2) how to recover from ransomware.

**Target Audience:** General Public – Election Authorities

**URL:** https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

*Ransomware: How to prevent and recover*

**Description:** Ransomware is a type of malware that denies user's access to files of systems until money is paid. This publication provides tips to help your organization prepare for and recover from ransomware.

**Target Audience:** General Public – Election Authorities

**URL:** https://www.cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099

7.2.4 Published Guidance and Training for Public Servants

*Counter Disinformation: A Guidebook for Public Servants*

**Description:** This guidebook (created by the Canadian School of Public Service with support from CSE and other government departments) is intended to provide an overview of disinformation, how its increasing threat is impacting our democratic institutions, and how to spot and respond to disinformation as it relates to government, programs, policies and services.

**Target Audience:** Government of Canada Employees – Public Servants

**URL:** https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions/countering-disinformation-guidebook-public-servants.html

*Cyber Threats to Canada's Democratic Processes: Presentation to the Advisory Committee for Political Parties*

**Description:** Joint presentation with CSIS on electoral security for Elections Canada's annual ACPP meeting, 8 September 2023, Palais des congrès de Gatineau, Québec.

**Target Audience:** Government of Canada Employees – Elections Canada, Political Parties Member of the ACPP

**File Names:**

- (U) "Foreign Interference: Briefing to Parliamentarians" – [PBH_CAN043117]
- (U) "Foreign Interference: A threat to Canada's National Security" – [TS_CAN014638]
- (U) "Cyber Threats to Canada's Democratic Process: Presentation to the Advisory Committee for Political Parties (ACPP)" – [PBH_CAN015062]
- (U) "Cybermenaces contre le processus démocratique du Canada : Présentation pour le Comité consultatif des partis politiques" – [PBH_CAN015006]

*Deepfakes and Generative AI: Shifting the Cyber Security Threat Landscape*

**Description:** The Cyber Centre provided an educational briefing on Generative AI and Deepfakes to employees at Global Affairs Canada (GAC) as part of their Cyber Security Awareness Week 2024. The purpose of the presentation was to inform GAC employees about cyber threats related to generative AI, such as large language models (LLMs) and deepfake technologies.

**Target Audience:** Government of Canada Employees – Public Servants

**File Name:** Deepfakes and Generative AI: Shifting the Cyber Security Threat Landscape – [Deepfakes and Generative AI_GAC Presentation_2024.pptx – PBH_CAN046669]

7.2.5 Published Guidance and Training for the General Public

*Online Disinformation*

**Description:** CSE published video and written guidance that included tips and tools for identifying and countering disinformation.

**Target Audience:** General public

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

Additional information is available in A7: Classified Annex to Question 7.

### 7. 3 Courses Provided by Cyber Centre Learning Hub

The Cyber Centre Learning Hub is available to those working within the Government of Canada (GC), other levels of governments, and with critical infrastructure organizations.

*Course ITLC 612 - Cyber Security Considerations for Election Authorities and Administrators*

**Description:** Online course to Canadian democratic institutions regarding the tools and knowledge needed to make educated decisions about securing their IT infrastructure.

**Target Audience:** Government of Canada – Public Servants

**URL**: https://lh-ca.cyber.gc.ca/course/view.php?id=172

*Course ITLC 616 - Cyber Security for Political Party IT Decision Makers and IT Staff*

**Description:** Online course which examines the specific cyber threats that political parties and decision makers face and where to start when integrating cyber security into their daily work lives.

**Target Audience:** Government of Canada – Public Servants

**URL:** https://lh-ca.cyber.gc.ca/course/view.php?id=188

*Course ITLC 618 - Cyber Security Considerations for Social Media Account Management*

**Description:** Online course highlights the cyber security threats associated with the use of social media and how to best protect your organization from these threats.

**Target Audience:** Government of Canada – Public Servants

**URL:** https://lh-ca.cyber.gc.ca/course/view.php?id=191

### 7.4 National Threat Assessments

The National Cyber Threat Assessment (NCTA) is one of the Cyber Centre's flagship cyber security reports. Its purpose is to help build Canada's resilience to cyber threats. The NCTA explains the cyber threats facing Canada, describes the likelihood that these cyber threats will occur and outlines how they may evolve in the coming years.

For additional resources from the Cyber Centre to help Canadian individuals and organizations understand the cyber threats facing Canada and learn more about how to better protect yourself visit the National Cyber Threat Assessment webpage.[2]

*National Cyber Threat Assessment 2023-2024*

**Description:** CSE observes how cyber threat actors' use of misinformation, disinformation, and mal-information (MDM) has evolved over the past two years.

[2] https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessments

Machine-learning enabled technologies are making fake content easier to manufacture and harder to detect. Further, nation states are increasingly willing and able to use MDM to advance their geopolitical interests. CSE assesses that Canadians' exposure to MDM will almost certainly increase over the next two years.

**Target Audience:** General Public

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

*National Cyber Threat Assessment 2020*

**Description:** Acting as an update to the National Cyber Threat Assessment 2018, the document notes that online foreign influence campaigns are almost certainly ongoing and not limited to key political events like elections.

**Target Audience:** General Public

**URL:** https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020

*National Cyber Threat Assessment 2018*

**Description:** In this assessment, CSE notes that Canadians are very likely to encounter malicious online influence activity in 2019. For example, CSE "anticipate(s) state-sponsored cyber threat actors will attempt to advance their national strategic objectives by targeting Canadians' opinions through malicious online influence activity."

**Target Audience:** General Public

**URL:** https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018

### 7.5 Media Interviews and Ongoing Outreach

As part of ongoing public education efforts, CSE regularly does media interviews and outreach that touch on foreign interference.

*"AI-powered disinformation is spreading – is Canada ready for the political impact?"*

**Description:** On January 17, 2024, CBC's *The National* included a report on AI and disinformation and its potential impact on elections. This report featured an interview with Chief of CSE, Caroline Xavier.

**Target Audience:** General Public

**URL:** https://www.cbc.ca/news/politics/ai-deepfake-election-canada-1.7084398

*"All it takes is one click: Chief cyberspy warns Canadians to protect themselves from online crime"*

**Description:** June 24, 2023 - CSE Chief Caroline Xavier interview with CBC Radio's *The House*.

**Target Audience:** General Public

**URL**: https://www.cbc.ca/news/politics/canada-cse-cybersecurity-caroline-xavier-1.6886253

*"Critical cyberattacks are an 'hourly' event. How can Canadians protect themselves?"*

**Description:** June 25, 2023 - Sami Khoury, head of the Canadian Centre for Cyber Security, interview with Global News the West Block.

**Target Audience:** General Public

**URL:** https://globalnews.ca/news/9790617/cybersecurity-canada-attacks-russia-energy-infrastructure/

*News Conference*

**Description:** Dec. 6, 2023 - News conferences to launch the Canada's Democratic Threats to Elections report and five follow-up interviews completed, mainly with small regional outlets.

**Target Audience:** General Public

**URL:** https://www.canada.ca/en/communications-security/news/2023/12/cyber-threats-to-canadas-democratic-process-2023-update.html

*"I Am Now More Concerned About the Formidable Threat from China"*

**Description:** Sept. 11, 2021 - Sami Khoury and Jen Easterly interview with Foreign Policy

**Target Audience:** General Public

**URL:** https://foreignpolicy.com/2023/09/11/easterly-khoury-cybersecurity-russia-ukraine-war-china-threat/

### 7.6 Other Educational Material

*Mobile Device Guidance for High Profile Travellers*

**Description:** If you're someone who is in a high-profile position, such as a politician or senior executive, you need to protect the security of your mobile devices when you travel. Mobile devices contain sensitive information and they are high-value targets for cyber security threat actors. If your device or the information on it is compromised, it could be used against you or the organization you represent.

**Target Audience:** General Public – High Profile Travellers

**URL:** https://www.cyber.gc.ca/en/guidance/mobile-device-guidance-high-profile-travellers-itsap-00088

*The Threat from Large Language Model Text Generators*

**Description:** In 2023, the Cyber Centre published a cyber threat bulletin on the threat from large language model (LLM) text generators. The brief outlines how LLMs represent a growing and evolving threat to Canada's information ecosystem, its media and telecommunication landscape, and the structures in which information is created, shared, and transformed.

**Target Audience:** General Public

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

*"If it raises your eyebrows, it should raise questions"*

**Description:** Online disinformation education campaign which ran from January to March 2024 on various digital platforms.

**Target Audience:** General Public

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

*Canada joins international security partners in release of advisory, guidance on growing cyber security threat to civil society*

**Description:** 2024 news release outlining the publication of an advisory co-authored by Canada, the United States, Estonia, Japan, Finland and the United Kingdom warning the public about a growing cyber security threat to civil society organizations and individuals.

**Target Audience:** General Public

**URL:** https://www.canada.ca/en/communications-security/news/2024/05/canada-joins-international-security-partners-in-release-of-advisory-guidance-on-growing-cyber-security-threat-to-civil-society.html

## 8. For each interdepartmental committee related to foreign interference, listing of meeting frequency (or meeting dates if *ad hoc*) and description of what documentation is routinely produced for each committee (e.g. agendas, list of participants, annotated agendas for the Chair, meeting summaries, minutes).

CSE was not requested to respond to this question.

## 9. A listing of all engagements at divisional Director level (or equivalent) or above with representatives of diaspora groups where the subject of foreign interference was discussed. Listing should include dates, names of departmental and diaspora representatives and summary of discussion.

CSE has not engaged with diaspora groups at the Director level or above to discuss foreign interference.

## 10. Any relevant updates related to the information provided in the Stage 1 Institutional Report.

### 10.1 Update to Section 2.3.1 (description of programs, policies and procedures implemented to respond to foreign interference)

The SITE Task Force has provided enhanced monitoring and assessing of foreign interference threats during four federal by-elections held in June and July of 2023 and provided the same for the by-election in Toronto at the end of June 2024, in response to the Independent Special Rapporteur's recommendations. This enhanced monitoring also includes the production of classified and unclassified reports of the Task Force's assessment of whether foreign interference occurred during the by-elections. The reports are then shared with the Prime Minister, relevant ministers, NSICOP, and identified representatives of the parties with appropriate security clearances. The reports produced during the June and July 2023 by-elections concluded that no attempts at foreign interference were observed during those votes.

### 10.2 Update to Section 8 (Security & Intelligence governance architecture)

In addition to the committees listed in the January 2024 Institutional Report, CSE has participated in the following committees:

- Deputy Minister Committee on the Indo-Pacific (DM CIP), chaired by GAC.
- Deputy Minister Foreign Interference Committee (DM FI), hosted/chaired by PCO.
- Deputy Minister Coordinating Committee on the Arctic (DM Arctic), chaired by Crown-Indigenous Relations and Canadian Northern Economic Development Agency.

### 10.3 Update to Section 9 (intelligence products produced on foreign interference)

CSE is providing an updated list of intelligence products produced on foreign interference that covers the time between when the list was created for the Phase 1 Institutional Report and present.

CSE is aware that by-elections have occurred between the timeframe of the original request and this new request, and was active in supporting SITE Task Force activities during this time. As CSE is no longer responsible for chairing the SITE Task Force, CSE does not hold the official records for by-elections that have occurred since the Stage 1 Institutional Report. Therefore, the SITE Task Force's more recent SITREPs have not been included in this list.

An updated list of intelligence products is available in A10: Classified Annex to Question 10.