Communications Security Establishment

Institutional Report

1 OVERVIEW AND MANDATE

1.1 CSE History

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 foreign policy and decision making.

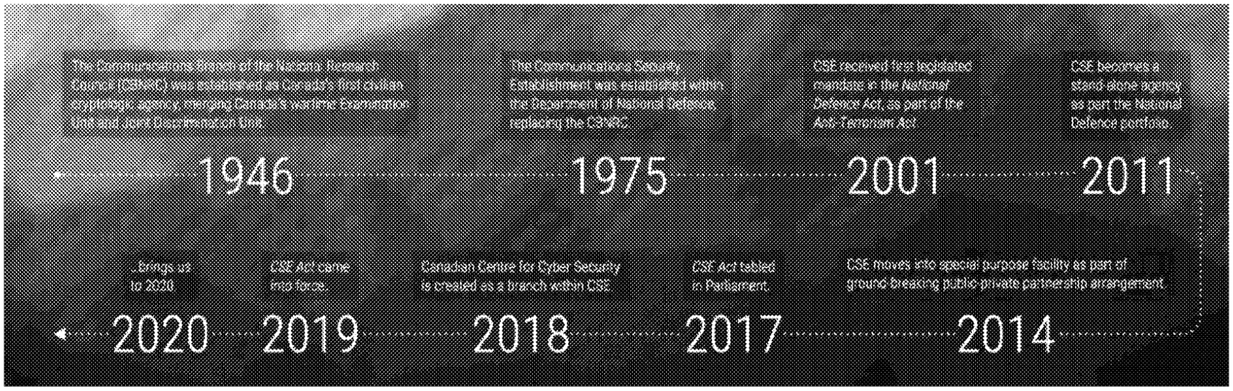
CSE's foreign intelligence collection is bound by the Government of Canada's intelligence priorities established by Cabinet.

CSE has a rich history of foreign signals intelligence (SIGINT) and communications security (COMSEC) going back to the Second World War and the very beginning of Canadian SIGINT (see Image 1). What began as a military signals corps in support of the British War effort quickly became a joint military and civilian operation. Established in 1946, the Communications Branch of the National Research Council (CBNRC), became Canada's national cryptologic agency. In 1975, the CBNRC was renamed the Communications Security Establishment, under the Department of National Defence.

For over 75 years, CSE has proved a valuable asset to the Government of Canada and to its allied partners, remaining committed to its primary mission: providing the federal government with SIGINT vital to Canada's national security and protecting Government of Canada communications.

Milestone legislation for CSE, the *CSE Act*, came into force in August 2019. Today, CSE is a stand-alone agency, running 24/7 operations to collect vital foreign intelligence, protect Canadian systems of importance, conduct cyber operations and assist our federal partners deliver their mandates.

Image 1: Dates and Figures in CSE's History



The Communications Branch of the National Research Council (CBNRC) was established as Canada's first civilian cryptologic agency, merging Canada's wartime Examination Unit and Joint Discrimination Unit.

1946

The Communications Security Establishment was established within the Department of National Defence, replacing the CBNRC.

1975

CSE received first legislated mandate in the *National Defence Act*, as part of the *Anti-Terrorism Act*

2001

CSE becomes a stand-alone agency as part the National Defence portfolio.

2011

CSE moves into special purpose facility as part of ground-breaking public-private partnership arrangement.

2014

CSE Act tabled in Parliament.

2017

Canadian Centre for Cyber Security is created as a branch within CSE.

2018

CSE Act came into force.

2019

...brings us to 2020

2020

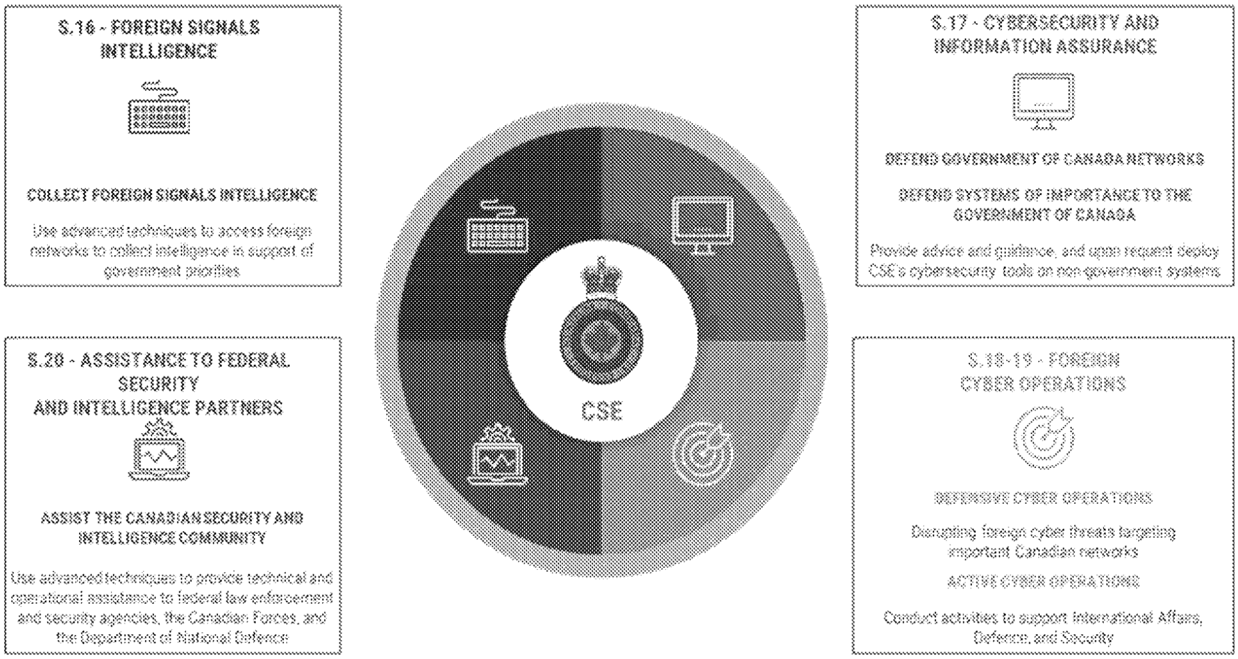
1.2 CSE Mandate

Section 15 of the *CSE Act* sets out CSE's mandate as the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance.

CSE is explicitly prohibited by law from directing its activities at Canadians or any person in Canada and CSE activities must not infringe on the *Canadian Charter of Rights and Freedoms*[1]. CSE also cannot ask allies to do anything on the behalf of CSE that it is otherwise not authorized to do.

See *Annex 1* for more information on the *CSE Act* at a Glance.

Image 3: CSE Mandate at a Glance



S.16 - FOREIGN SIGNALS INTELLIGENCE

COLLECT FOREIGN SIGNALS INTELLIGENCE

Use advanced techniques to access foreign networks to collect intelligence in support of government priorities

S.17 - CYBERSECURITY AND INFORMATION ASSURANCE

DEFEND GOVERNMENT OF CANADA NETWORKS

DEFEND SYSTEMS OF IMPORTANCE TO THE GOVERNMENT OF CANADA

Provide advice and guidance, and upon request deploy CSE's cybersecurity tools on non-government systems

S.20 - ASSISTANCE TO FEDERAL SECURITY AND INTELLIGENCE PARTNERS

ASSIST THE CANADIAN SECURITY AND INTELLIGENCE COMMUNITY

Use advanced techniques to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces, and the Department of National Defence

S.18-19 - FOREIGN CYBER OPERATIONS

DEFENSIVE CYBER OPERATIONS

Disrupting foreign cyber threats targeting important Canadian networks

ACTIVE CYBER OPERATIONS

Conduct activities to support International Affairs, Defence, and Security

MANDATE (S.15) : National signals intelligence agency for foreign intelligence and technical authority for cybersecurity and information assurance

1.3 CSE Authorities

The Minister of National Defence (MND) guides and authorizes activities using the following mechanisms that establish operating parameters and expectations for CSE:

- Ministerial Authorizations (MA)
- Ministerial Orders (MO)

[1] As per Section 22 (1) of the *CSE Act*: Activities carried out by the Establishment in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations aspects of its mandate must not be directed at a Canadian or at any person in Canada and must not infringe the Canadian Charter of Rights and Freedoms.

- Ministerial Directives (MD)

1.3.1 Ministerial Authorizations

As per the *CSE Act*, the MND must authorize CSE to carry out classes of activities in support of the foreign intelligence or cybersecurity aspects of its mandate if those activities would:

- risk contravening any other act of Parliament (or of any foreign state for s.16 and s.18-19 only), or
- may interfere with a reasonable expectation of privacy of a Canadian or Person in Canada

Foreign intelligence and cybersecurity MAs must demonstrate that:

- the authorization is necessary and that the activities being authorized 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

There are four (4) types of MA that correspond to aspects of CSE's mandate: foreign intelligence (s.16), cybersecurity and information assurance (s.17), and active and defensive cyber operations (s.18 and 19).

The Intelligence Commissioner[2] must approve foreign intelligence authorizations and cybersecurity authorizations before the activities can begin. Each authorization is valid for up to a year.

Unlike foreign intelligence and cybersecurity authorizations, the Intelligence Commissioner does not approve active cyber operations (ACO) or defensive cyber operations (DCO (collectively known as foreign cyber operations (FCO)), in accordance with the *CSE Act*. FCO authorizations are also approved in a 'two-key system,' whereby the MND must either consult or obtain the consent of the Minister of Foreign Affairs prior to issuing the authorization. Applications to MND for FCO authorizations must also demonstrate that the authorization is necessary and that the activities being authorized are reasonable and proportionate.

MAs are not required for the assistance aspect of CSE's mandate, as in the course of providing the assistance, CSE has the same authority to carry out any activity as would have the federal law enforcement or security agency, the Canadian Forces or the Department of National Defence, as the case may be, if it were carrying out the activity, and is subject to any limitations imposed by law on these organizations.

Each time an MA is repealed or expires, CSE must provide MND an End of Authorization report that described the outcome of the activities conducted. End of Authorization Reports for foreign

[2] The Intelligence Commissioner is responsible for performing quasi-judicial reviews of the conclusions on the basis of which certain authorizations are issued or amended, and certain determinations are made, under the *Communications Security Establishment Act* and the *Canadian Security Intelligence Service Act*.

intelligence and cybersecurity authorizations are also shared with the Intelligence Commissioner. In the case of FCO authorizations, both MND and the Minister of Foreign Affairs receive the End-of-Authorization report.

Finally, the MND cannot authorize any activities that are not included in the *CSE Act* or grant CSE any powers that are not included in the *CSE Act*.

1.3.2 Ministerial Orders

Under the *CSE Act*, the MND may use a Ministerial Order (MO) to designate people or organizations with whom CSE can share information or to whom CSE can provide cybersecurity services. For example, for CSE to provide cybersecurity services to a non-federal institution, the Minister would have to designate that organization's cyber systems as being "of importance to the Government of Canada." CSE's MOs are used to:

- Designate non-federal cyber systems as being of importance to the Government of Canada;
- Designate entities with whom CSE may share information relating to a Canadian or person in Canada if it is necessary to protect the information or systems of federal institutions or critical infrastructure;
- Designate entities with whom CSE may share Canadian identifying information, if it is essential for international affairs, defence or security.

1.3.3 Ministerial Directives

The Chief, CSE receives instructions from the MND through Ministerial Directives (MDs). These Directives set out direction and guidance, operating parameters, or the Minister's expectations for CSE on a range of issues. CSE's activities must be consistent with those Directives and must always fall within its mandate and authorities.

CSE currently has only one Directive in force: the MD on Government of Canada Intelligence Priorities. CSE's acquisition of foreign intelligence is legislatively bound to Government of Canada Intelligence Priorities, which are officially promulgated to CSE by the MND through a MD, meaning CSE can only collect intelligence as it relates to intelligence priorities as established by Cabinet.

Resulting from a PCO-led interdepartmental process which translates Intelligence Priorities into more detailed intelligence requirements, CSE's MD outlines the requirements which are then further refined into internal priorities and plans.

An MD cannot grant CSE any power that is not included in the *CSE Act*.

2 DESCRIPTION OF PROGRAMS, POLICIES AND PROCEDURES IMPLEMENTED TO RESPOND TO BOTH THE GENERAL THREAT AND THE ACTUAL INCIDENTS OF FOREIGN INTERFERENCE ASSOCIATED WITH THE 43RD AND 44TH GENERAL ELECTIONS

2.1 CSE's response to the general threat of foreign interference

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. As foreign interference is a threat at all times, not just during election periods, countering this activity requires a whole of government approach, which CSE actively supports by:

- providing SIGINT to Government of Canada decision makers about the intentions, capabilities and activities of foreign-based threat actors
- 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
- 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 Election Canada's systems, network and our various democratic processes. Through its historical monitoring of foreign interference, the organization has produced multiple reports about the risks the interference poses to various parts of Canada's democratic process and the safeguards created against them.

2.2 Countering hostile state activity and foreign interference

CSE leverages all aspects of its mandate (foreign intelligence, cyber security, foreign cyber operations and technical and operational assistance) to counter hostile state activities. These threats include espionage, malicious cyber activity and foreign interference.

2.2.1 State backed cyber actors

State-backed cyber actors pose the greatest strategic threat to Canada and Canada's critical infrastructure. These adversaries use highly sophisticated and covert techniques against Canada and allied countries with ambitions ranging from intelligence collection to destructive acts.

CSE signals intelligence continues to provide unique and timely insight into the tactics, techniques and procedures used by a broad spectrum of state-backed cyber actors. This in turn informs the advice and guidance generated by the Canadian Centre for Cyber Security (CCCS, or Cyber Centre).

2.2.2 Transnational repression

Authoritarian states use a variety of means to monitor and intimidate diaspora populations around the world, including in Canada. An example of this is the issue of the People's Republic of China operating "police service stations" in Canada.

CSE works with global and federal partners to mitigate the risks posed by these transnational repression activities. CSE does this by gathering SIGINT and by supporting Canada's security and intelligence community.

2.2.3 Disinformation and democracy

Disinformation is false information that is deliberately created to cause harm. Often designed to provoke an emotional response, disinformation spreads very quickly on social media. This makes it harder for Canadians to know what is true or who to trust. CSE judges that it is highly probable that cyber threat activity against democratic processes worldwide will increase in quantity and sophistication over the next year, and perhaps beyond that.

Foreign states use online disinformation to destabilize Canada's democracy by:

- spreading false information
- influencing voter decisions
- polarizing opinions
- discrediting people and institutions
- undermining trust in the democratic process

CSE contributes to a government-wide online disinformation awareness campaigns, which includes:

- tools to help Canadians identify and fact-check disinformation
- content and videos from external partners like MediaSmarts and CIVIX: CTRL-F
- information from Cyber Centre threat reports including:
  - the National Cyber Threat Assessment
  - Cyber Threats to Canada's Democratic Process
- Cyber Centre guidance on how to identify misinformation, disinformation and malinformation

2.2.4 Public attributions

Canada supports and advocates for responsible state behaviour in cyberspace.

In 2017, CSE assessed actors in Russia were responsible for developing *NotPetya*, a destructive malware which indiscriminately attacked critical financial, energy, government and infrastructure sectors around the world.

CSE joined its allies and partners in attributing WannaCry to North Korea, a malware which extorted ransoms and disrupted services globally, in December 2017.

In April 2022, Global Affairs Canada (GAC) set out Canada's position on International Law applicable in cyberspace. GAC works with international allies to call out state behaviour that violates these norms.

CSE intelligence reporting and cyber security analysis contributed to public attributions of:

- Russia's malicious cyber activity affecting Europe and Ukraine (May 2022)
- Iran's malicious cyber activity affecting Albania (September 2022)

The Cyber Centre has also issued three (3) additional joint cyber security advisories with Five Eyes partners to warn about cyber techniques associated with Russian-backed actors and the following public reports, alerts and guidance documents:

- Joint cyber security advisory on Russian state-sponsored and criminal cyber threats to critical infrastructure (April 2022)
- Cyber threat activity related to the Russian invasion of Ukraine (July 2022)
- Cyber security for heightened threat levels (July 2022)
- Risk of malicious cyber activity against Ukraine-aligned nations (February 2023)

2.2.5 Other reports and guidance to Canadians

CSE's Cyber Centre publishes threat reports and guidance resources online so that all Canadians and Canadian organizations can access high-quality cyber security information. These reports and resources have been produced since 2017.

In 2018, the Cyber Centre published the first installment of the *National Cyber Threat Assessment 2018* (NCTA).

This flagship report is published every two (2) years. It draws on classified and unclassified sources to identify key trends in the cyber threat landscape. This edition of the report focused on five (5) trends:

- Ransomware
- Threats to critical infrastructure
- State-sponsored cyber activity
- Online disinformation
- Disruptive technologies

To accompany the NCTA, CSE publishes guidance to address those five (5) trends regularly.

Additionally, as democratic processes around the world continue to be targeted by cyber threat actors, CSE's Cyber Centre also published in 2017, 2019, 2021, and 2023 the *Cyber Threats to Canada's Democratic Process*. In these reports CSE reviews global trends in cyber threat activity against democratic processes (which we define as including voters, political parties, and elections) and evaluate the threat to Canada.

2.3 CSE's response to the threat of foreign interference associated with Canadian elections

Around the world, democratic processes continue to be affected by cyber threat activity. Cyber threat activity is carried out against these participants and events by state-sponsored actors, cybercriminals, politically motivated actors, hacktivists, and thrill-seekers. Targeting democratic processes largely remains a strategic activity. State-sponsored cyber threat actors with links to Russia, China, and Iran have conducted most of the observed cyber threat activity against democratic processes worldwide.

While there are many opportunities for threat actors to target Canadian democratic processes, it is important to note that, in the past few years, there have also been significant strides towards protecting these processes over the last two general elections (General Elections 43 and 44 in 2019 and 2021 respectively).

2.3.1 The Security and Intelligence Threats to Elections (SITE) Task Force

SITE Task Force is an interdepartmental working group where member organizations CSE, Canadian Security and Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP) and Global Affairs Canada (GAC):

- Review and share intelligence collection, assessment, and open-source analysis related to foreign interference in Canada's democratic process in a coordinated manner.
- Provide situational awareness for government partners, senior public servants, and other relevant partners.
- Promote protection of electoral processes through sharing with partners or, when respective mandates permit, take action to mitigate the threat.

Additionally, throughout the 2019 and 2021 elections, SITE Task Force disseminated daily SITREPs by email to its distribution list, which includes Canada's Critical Election Incident Public Protocol (CEIPP).

CSE's role on SITE is to monitor SIGINT and cyber activity for signs of foreign interference in the electoral process. CSE chaired SITE from its inception in 2018 until 2022, when the role passed to CSIS.

Throughout the election periods, SITE partners briefed a panel of senior public officials under CEIPP. The CEIPP lays out a simple, clear and impartial process by which Canadians would be notified of an incident or series of incidents that threatened Canada's ability to have a free and fair election. More information on the CEIPP panel is contained in the Institutional Report of the Privy Council Office. The SITE Task Force continues to meet to remain connected as a community and to continue to monitor ongoing foreign interference activities.

2.3.2 Defending elections infrastructure

CSE's mandate includes conducting defensive cyber operations (DCO) to respond to cyber attacks on critical systems.

In the run-up to both the 2019 and 2021 federal elections, the MND issued an authorization for DCO which included protecting the electronic infrastructure of Elections Canada. This was a precaution in case of malicious cyber activity during the election period. For example, if a foreign threat actor had compromised Elections Canada's website, CSE could have used its cyber operations capabilities to impact the server being used for the attack. In the event, no activities took place that would have required a DCO response. However, DCOs are an important tool for countering cyber threats to Canada's democratic processes.

CSE planned two DCOs to prevent threats of foreign interference in Canadian democratic processes and institutions. The DCO for the 2019 federal election was planned and approved but not conducted as the threat did not manifest. The recreated DCO for the 2021 federal election was planned but approval was not sought nor was it conducted, as the threat did not manifest.

Although these two operations are related to threats of foreign interference in Canadian democratic processes and institutions, it should be noted that CSE's focus for these DCOs was to disrupt cyber threats against Elections Canada infrastructure specifically, and only if one of the three conditions of the DCO MA were met. The objectives of the operations were to disrupt or interfere with foreign elements on the global information infrastructure (GII) being used to conduct malicious cyber activity against Elections Canada's infrastructure in order to protect that infrastructure.

2.3.3 Cyber security for democratic institutions

Democratic institutions are an essential part of Canada's critical infrastructure. The Cyber Centre works with election authorities and federal political parties to help them strengthen their cyber security, in addition to working with Elections Canada and their provincial and territorial counterparts to help ensure their networks are protected.

In the run-up to both the 2019 and 2021 federal elections, the Cyber Centre worked with federal political parties to brief them on cyber threats and advise them on cyber security best practices. In both cases, the Cyber Centre set up a 24/7 hotline that candidates could call if they had any cyber security concerns. Outside election periods, the Cyber Centre has a dedicated point of contact that political parties can reach out to on cyber security matters, including providing tailored advice and guidance to candidates which is available on the Cyber Centre's website.

During both elections, CSE stood up efforts to monitor for, prevent or mitigate hostile foreign activity related to the election.

During GE43 and GE44, as part of its regular activities, the Cyber Centre also:

- supported elections authorities ahead of provincial elections throughout the country
- shared guidance resources with municipalities
- provided election authorities with:
  - briefings on the National Cyber Threat Assessment
  - technical advice
  - guidance resources
  - cyber security services

2.3.4 Information on cyber threats to elections

In May 2022, as part of its response to the 43rd and 44th General Elections, CSE created a dedicated web page on cyber threats to elections. The page provided an overview of ways in which threat actors can disrupt democratic processes, such as:

- disrupting election infrastructure using distributed denial of service (DDoS) attacks
- mimicking user identities to spread false information on social media
- compromising political parties' IT systems
- launching online foreign influence campaigns to discredit the democratic process
- using ransomware to disrupt access to election data

The web page contains links to Cyber Centre reporting on cyber threats to Canada's democratic process. It also provides up to date cyber security advice and guidance resources for political parties, elections authorities, and voters.

2.3.5 September 2023 Chief, CSE directive on threats to democracy

In early September 2023, the Chief, CSE issued a directive to the Deputy Chief, SIGINT and the Head, Cyber Centre outlining expectations on how CSE will contribute to broader Government of Canada efforts to protect Canada's democracy. Specifically, the directive outlines the Chief's direction for CSE to continue operations to ensure foreign intelligence on threats to Parliament, Parliamentarians, their families and staff, (as well as cyber security threats linked to specific Parliamentarians) is provided at the right time to inform decision making.

See *Annex 2* for the full *September 2023 Chief, CSE directive on threats to democracy.*

3 KEY EXECUTIVES

3.1 Chief, CSE

Executive Name(s)

- Caroline Xavier (31 August, 2022 – present)
- Shelly Bruce (June 27, 2018 – August 30, 2022)

Roles and Responsibilities

Manages and controls the Establishment and all matters relating to it.

3.2 Associate Chief, CSE

Executive Name(s)

- Daniel Rogers (January 2022 – February 2023)
- Daniel Rogers was the only Associate Chief, CSE within the requested timeframe, and the position ceased to exist after their departure.

Roles and Responsibilities

Assists in overseeing and managing efforts at CSE.

3.3 Head, Cyber Centre, CSE

Executive Name(s)

- Sami Khoury (September 2021 – present)
- Scott Jones (October 2018-August 2021)

Roles and Responsibilities

Oversees the Cyber Centre which is the single unified source of expert advice, guidance, services and support on cyber security for Canadians.

3.4 Associate Head, Cyber Centre, CSE

Executive Name(s)

- Rajiv Gupta (2021 – present)
- André Boucher (2018-2021)

Roles and Responsibilities

Responsible for helping to advance the Cyber Centre's operations and management.

3.5 Deputy Chief, Signals Intelligence (SIGINT), CSE

Executive Name(s)

- Alia Tayyeb (2022 – present)
- Daniel Rogers (2018 – 2022)

Roles and Responsibilities

Oversees and manages the foreign signals intelligence and foreign cyber operations aspects of the CSE mandate. Also responsible for responding to requests for assistance from federal partners pursuant to section 20 of the *CSE Act*.

3.6 Associate Deputy Chief, Signals Intelligence (SIGINT), CSE

Executive Name(s)

- Artur Wilczynski (2020 – 2022)
- Artur Wilczynski was the only Associate Deputy Chief, SIGINT within the requested timeframe, and the position ceased to exist after their departure.

Roles and Responsibilities

Assists with the oversight and management of the foreign signals intelligence and foreign cyber operations aspects of the CSE mandate, and with responses to requests for assistance from federal partners pursuant to section 20 of the *CSE Act*.

3.7 Deputy Chief, Authorities, Compliance and Transparency (ACT), CSE

Executive Name(s)

- Christopher Williams (A/) (December 2023 – present)
- Nabih Eldebs (2021 – December 2023)
- Position did not exist prior to 2021. Was formerly DG Policy, Disclosures and Review. Nabih Eldebs was in that position from 2019-2021.

Roles and Responsibilities

Delivers and supports the Ministerial Authorizations approval process, governance framework, and the policy requirements that enable mission operations as well as complementary activities to enable and sustain CSE's operational activities (Operational Policy, Program for Operational Compliance, Transparency and Information Sharing and External Review and Complaints). DC ACT also serves as the Chief Privacy Officer for CSE.

3.8 Chair, Security and Intelligence Threats to Elections (SITE) Task Force

Executive Name(s)

- Lyall King (2018 - 2022)
- Position no longer at CSE.

Roles and Responsibilities

The SITE Task Force brought together operational leads and experts from CSE, CSIS, GAC, and the RCMP with the aim of improving awareness, collection, coordination, and action in countering foreign interference in Canada's federal elections. The Chair of SITE was responsible for overall administration and coordination of the SITE Task Force which included administration of meetings, organizing and preparing SITE Task Force work for upcoming elections, delivering briefings and drafting reports.

4 INFORMATION CHANNELS TO THE MINISTER'S OFFICE AND THE MND

CSE's policy requirements for how its intelligence products are permitted to be disseminated are laid out in the Mission Policy Suite (MPS). Specifically, section 26.2 of the Foreign Intelligence MPS identifies the requirements for all Releasable SIGINT Products (RSPs):

"All RSPs must be shared using approved systems and/or processes, and must adhere to the following six requirements.

- *Include information that has been assessed to be of FI [Foreign Intelligence] value in support of GC intelligence priorities;*
- *Be altered to protect the privacy of Canadians and persons in Canada;*
    - *RSPs must also comply with privacy protection rules for second party nationals and persons in second party territory, in accordance with the relevant second party policies;*
- *Be sanitized to protect SIGINT equities, methods, and techniques (in accordance with the classification);*
- *Be serialized and traceable;*
- *Be caveated as appropriate; and*

- *Be approved for release by the appropriate Release Authority."*

Due to these requirements, CSE's intelligence products may only be shared via certain systems/ mechanisms, regardless of recipient.

4.1 Information Produced by CSE/2P Partners

CSE disseminates collected intelligence to Canada's Security and Intelligence Community through intelligence products, which are published through CSE's reporting applications on the Canadian Top Secret Network.

In the regular course of business, the MND's Office (MNDO) is made aware of relevant CSE/partner reports by CSE's Client Relations Officers (CROs). CROs may provide relevant reports through secure electronic solutions or in hard copy. Further information about the CRO program can be found in section 5.

The MND also may be made aware of relevant CSE reports by the Chief, CSE, during scheduled or *ad-hoc* meetings or calls. However, as needed and depending on the urgency, CSE's Chief of Staff, or Ministerial Liaison Officer may alert MNDO of important relevant reports by phone or email.

4.2 Information Produced by Other Departments

When information on possible foreign interference is produced by other departments, the information may be provided through various means:

1. Producing departments push soft-copies of relevant reports to a specific distribution list;
2. Producing departments may provide soft or hard copies of the information for awareness and discussion at weekly/*ad hoc* DM, Cabinet Committee, or ministerial-level meetings.

As needed, CSE's Chief of Staff may flag this information for MNDO awareness by phone or email as part of regularly scheduled or ad-hoc meetings. CSE's Ministerial Liaison Officer or CSE's Chief may also flag this information directly to the MND or their office during regular weekly meetings or on an ad hoc basis, as appropriate.

If necessary CSE officials can meet a Minister to share intelligence in an accredited secure location.

5 INFORMATION CHANNELS TO THE PCO AND PMO

CSE foreign intelligence reporting, unlike that of other Government of Canada security and law enforcement agencies, consists purely of factual representations of electronic communications data. CSE does not use the information it collects to conduct assessments of or present conclusions about the foreign intelligence it reports. CSE may include analytic comments in its RSPs, which is used to provide additional context to the specifics of that report. It is left to those receiving CSE's intelligence reporting to assess the overall relevance and significance of the information reported. The assessment of the information by partners and clients, or the context in which they assess that information, is entirely dependant on those clients and partners. The Cyber Centre uses CSE's foreign intelligence, in conjunction with other information sources, to inform its assessments related to cyber threats.

As indicated in section 4, CSE's intelligence products may only be shared via certain systems/ mechanisms, regardless of recipient. CSE's reporting tools are used for the dissemination, management, and tracking of information produced by CSE or shared with CSE for further dissemination.

Government of Canada clients who have been authorized to have an account to CSE's reporting tool can directly access the intelligence products contained in the reporting tool commensurate with their security clearance and indoctrinations. These clients, including PCO officials, may then leverage this intelligence in their own decision-making, analysis, and derivative reporting.

Government of Canada clients who are authorized through their security clearance and indoctrinations to access intelligence products but who do not have CSE reporting tools accounts may still receive relevant intelligence products via CSE's CROs. CROs facilitate access to intelligence products for these clients by providing them with hard copy or soft copy (through a secure solution) products. CROs use CSE's reporting tool to then track readership and feedback on the products they have shown or provided to the GC clients. Senior PCO officials, the Prime Minister and PMO staff have access to intelligence products commensurate with their security clearance and indoctrinations via the services of CSE's CROs.

CSE also provides access to intelligence products to other GC departments through their SIGINT Dissemination Officer (SDO) program. SDOs are Government of Canada employees with CSE reporting tool accounts who have been empowered to perform a function similar to CROs within their own departments only. SDOs track when they have disseminated CSE reports to their internal clients or received feedback on those reports.

5.1 Typical CRO Dissemination Workflow

CROs build and maintain knowledge of their clients' requirements through engagement with their clients. Clients can also request to be briefed on specific topics on an *ad-hoc* basis.

Once a product of interest to a client has been identified, CROs will print the product package and, if the client has access to a TS//SI accredited safe, will leave the package with them. The CRO will indicate that the client has been provided with access to the product in the reporting tool. While access will have been provided to the client, it does not definitively mean that the client has read the intelligence product. If the client does not have access to an appropriate safe, the CRO will sit with the client while they read the intelligence product package and then take the package back. In addition, any feedback provided by the client, in terms of value and use of the intelligence product, will be captured by the CRO and entered into CSE's reporting tool.

CROs always maintain positive control of any printed copies and log the destruction of these. Logs are audited on a regular basis to ensure the integrity of the information.

CSE may also flag reporting for awareness and discussion at weekly/ad hoc DM, Cabinet Committee, or ministerial-level meetings.

6 ORAL OR WRITTEN BRIEFINGS RELATED TO THE MATTERS COVERED BY THE COMMISION'S TERMS OF REFERENCE (A)(I)(A) AND (A)(I)(B) TO THE SITE TASK FORCE, THE CEIPP PANEL, A DEPUTY MINISTER, THE NSIA, THE CLERK OF THE PRIVY COUNCIL, PMO, OR THE PRIME MINISTER SINCE SEPTEMBER 2018

During the 43rd (2019) and 44th (2021) general elections, CSE chaired the SITE Task Force (please see section 2.3.1 for more information about SITE TF). SITE Task Force conducted briefings in the lead up to and throughout both elections.

Additionally, throughout the 2019 election, the 2021 election, and in response to these, actions taken in 2023 by-elections, SITE Task Force disseminated regular situation reports to its distribution list, which includes CEIPP.

Please see the classified version of this report for a full listing of these briefings.

7 ADVICE AND RECOMMENDATIONS PROVIDED TO MINISTERS OR MINISTER'S OFFICES

CSE did not provide advice and/or a recommendation to a Minister or a Minister's office in response to specific intelligence on foreign interference in democratic processes and institutions, including interference in parliamentary business, since January 2019.

8 SECURITY & INTELLIGENCE GOVERNANCE ARCHITECTURE

Hosted/Chaired by CSE:

Canadian Committee on National Security Systems (CCNSS): The Secretariat Unit acts on behalf of the CCNSS in providing operational management, guidance, and oversight to Canada's National Security Systems community. The Secretariat develops, on behalf of the CCNSS, the strategic roadmap of activities which includes the development of policy instruments and compliance monitoring. The goal of these activities is to ensure a consistent and appropriate application of protection across all national security assets, establish acceptable risk levels and ensure continued trust and interoperability with allies.

Director General Cyber Operations Committee: In support of the implementation of Canada's National Cyber Security Strategy, and in conformity with the applicable national policies, the Government, through the Directors General Cyber Operations (DG Cyber Ops) committee, helps ensure that key operational federal cyber security departments and agencies are working together to protect Canada. The DG Cyber Ops committee exists to ensure that the federal response to cyber threats and incidents of national interest is coordinated and that national operational policy issues are advanced.

- DG Cyber Ops is the operational sub-group of the DG Cyber Committee. The DG Cyber Operations group is differentiated from that group by its operational focus and reduced membership. Participation in DG Cyber Ops is limited to those organizations with mandated operational cyber security functions.
- DG Cyber Ops primary focus is cyber events of national interest, or those events which impact non-federal systems. Cyber events affecting Government of Canada systems and infrastructure will be responded to in accordance with the Government of Canada Cyber Security Event Management Plan (CSEMP).

While CSE hosts the CCNSS, officials from PCO would be best placed to provide a full description of the national security and intelligence governance inter-departmental architecture.

9 INTELLIGENCE PRODUCTS PRODUCED ON FOREIGN INTERFERENCE

CSE has produced a number of types of intelligence products since January 2019. Further information about the programs that produced these products can be found in section 2.

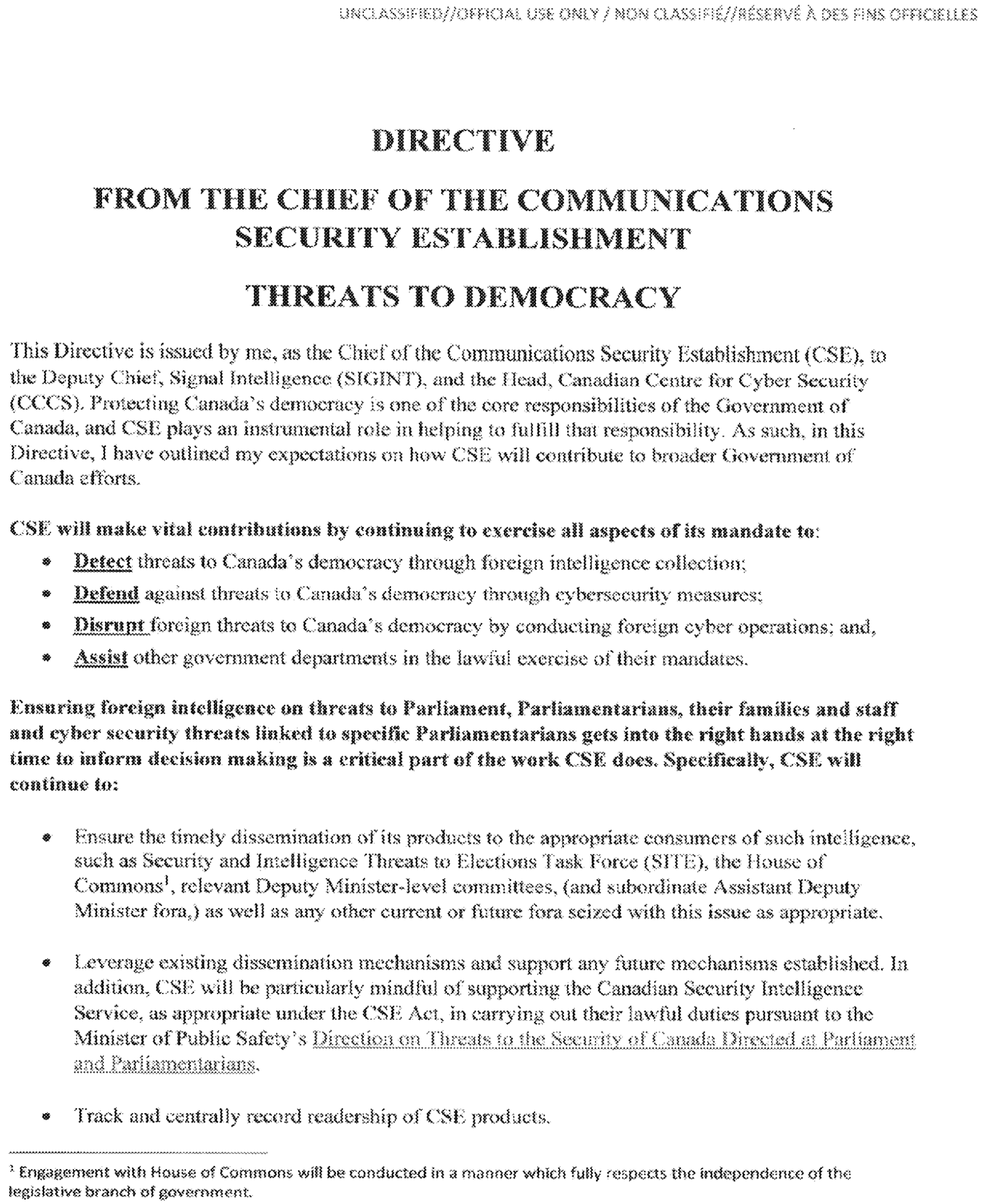
Please see the Classified version of this report for a list and description of intelligence products produced on foreign interference.

10 THREAT REDUCTION MEASURES

CSE has a NIL response, as CSE does not have the legislated authority to conduct TRMs. CSE's defensive cyber operations (DCO) efforts were described above.

Annex 1: Quick Guide to the *CSE Act*

Annex 2: Directive from the Chief, CSE on Threats to Democracy



UNCLASSIFIED//OFFICIAL USE ONLY / NON CLASSIFIÉ//RÉSERVÉ À DES FINS OFFICIELLES

DIRECTIVE

FROM THE CHIEF OF THE COMMUNICATIONS SECURITY ESTABLISHMENT

THREATS TO DEMOCRACY

This Directive is issued by me, as the Chief of the Communications Security Establishment (CSE), to the Deputy Chief, Signal Intelligence (SIGINT), and the Head, Canadian Centre for Cyber Security (CCCS). Protecting Canada's democracy is one of the core responsibilities of the Government of Canada, and CSE plays an instrumental role in helping to fulfill that responsibility. As such, in this Directive, I have outlined my expectations on how CSE will contribute to broader Government of Canada efforts.

CSE will make vital contributions by continuing to exercise all aspects of its mandate to:

- **Detect** threats to Canada's democracy through foreign intelligence collection;
- **Defend** against threats to Canada's democracy through cybersecurity measures;
- **Disrupt** foreign threats to Canada's democracy by conducting foreign cyber operations; and,
- **Assist** other government departments in the lawful exercise of their mandates.

Ensuring foreign intelligence on threats to Parliament, Parliamentarians, their families and staff and cyber security threats linked to specific Parliamentarians gets into the right hands at the right time to inform decision making is a critical part of the work CSE does. Specifically, CSE will continue to:

- Ensure the timely dissemination of its products to the appropriate consumers of such intelligence, such as Security and Intelligence Threats to Elections Task Force (SITE), the House of Commons[1], relevant Deputy Minister-level committees, (and subordinate Assistant Deputy Minister fora,) as well as any other current or future fora seized with this issue as appropriate.

- Leverage existing dissemination mechanisms and support any future mechanisms established. In addition, CSE will be particularly mindful of supporting the Canadian Security Intelligence Service, as appropriate under the CSE Act, in carrying out their lawful duties pursuant to the Minister of Public Safety's Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians.

- Track and centrally record readership of CSE products.

[1] Engagement with House of Commons will be conducted in a manner which fully respects the independence of the legislative branch of government.

All CSE activities will be conducted in accordance with the *Communications Security Establishment Act* and in a manner consistent with the following principles:

- **Lawfulness** – CSE will apply the principles and requirements of the Canadian laws, legislation, and policies that drive us, including respecting and protecting the privacy of Canadians.
- **Transparency** – CSE will recognize that it is essential to democracy that Canadians understand what the Government does to protect national security, how the Government does it, and why such work is important.
- **Accountability** – CSE will support accountability measures, which are fundamental to Canada's system of government and maintaining the confidence of Canadians. CSE's accountability extends to the Minister of National Defence and to Cabinet, Parliament, and Canadians.

EFFECTIVE DATE: The Directive will take effect on the date of the signature.

Issued at OTTAWA this 8 day of September 2023.

Caroline Xavier
Chief

DIRECTIVE DE LA CHEF DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

MENACES CONTRE LA DÉMOCRATIE

En tant que chef du Centre de la sécurité des télécommunications (CST), je suis l'auteure de la présente directive, à l'intention de la chef adjointe, Renseignement électromagnétique (SIGINT) et du dirigeant principal du Centre canadien pour la cybersécurité (CCC). Protéger la démocratie du Canada est l'une des principales responsabilités du gouvernement du Canada et le CST joue un rôle clé pour aider à assumer cette responsabilité. Par conséquent, dans cette directive, je présente mes attentes sur la façon dont le CST contribuera aux efforts du gouvernement du Canada.

Le CST apportera une contribution essentielle en continuant d'exercer tous les volets de son mandat visant à :

- **Détecter** les menaces contre la démocratie du Canada en recueillant du renseignement étranger;
- **Défendre** la démocratie du Canada contre les cybermenaces grâce à des mesures de cybersécurité;
- **Contrer** les menaces étrangères contre la démocratie du Canada en menant des cyberopérations étrangères; et
- **Assister** les autres ministères dans l'exercice des mandats que la loi leur confère.

S'assurer que le renseignement étranger sur les menaces contre le Parlement, les députés, leurs familles, leur personnel, et les cybermenaces contre des députés en particulier, soit transmis aux bonnes personnes, en temps opportun, pour éclairer la prise de décisions est un élément essentiel du travail effectué par le CST. Plus précisément, le CST continuera de faire ce qui suit :

- Assurer la diffusion en temps opportun de ses produits aux clients qui ont besoin du renseignement, comme le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (GT MSRE), la Chambre des communes[1], les comités pertinents au niveau des sous-ministres (et les forums des sous-ministres adjoints subordonnés) ainsi que tout autre forum actuel ou futur saisi de cette question, le cas échéant.

- Tirer parti des mécanismes de diffusion et soutenir les mécanismes qui seront mis en place à l'avenir. De plus, le CST soutiendra particulièrement le Service canadien du renseignement de sécurité, conformément à la *Loi sur le CST*, dans l'exercice de ses fonctions conférées par la loi, à l'appui des Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires du ministre de la Sécurité publique.

[1] La collaboration avec la Chambre des communes se fera d'une manière qui respecte pleinement l'indépendance du pouvoir législatif du gouvernement.

- Faire le suivi et consigner de manière centralisée le lectorat des produits du CST.

Toutes les activités du CST seront menées conformément à la *Loi sur le Centre de la sécurité des télécommunications* et de manière à respecter les principes suivants :

- **Respect de la loi** – Le CST applique les principes et les exigences qui découlent des lois canadiennes, du cadre législatif et des politiques régissant nos activités, y compris le respect et la protection de la vie privée des Canadiennes et Canadiens.
- **Transparence** – Le CST reconnait qu'il est essentiel à la démocratie que les Canadiennes et Canadiens comprennent ce que le gouvernement fait pour protéger la sécurité nationale, comment il le fait et pourquoi un tel travail est important.
- **Reddition de comptes** – Le CST appuie les mesures de reddition de comptes qui sont essentielles au système de gouvernement du Canada et au maintien de la confiance des Canadiennes et Canadiens. Le CST rendra des comptes au ministre de la Défense nationale, au Cabinet, au Parlement et aux Canadiennes et Canadiens.

DATE D'ENTRÉE EN VIGUEUR : La présente directive entrera en vigueur à la date de la signature.

Publié à Ottawa, en ce 8 Septembre 2023.

Caroline Xavier
Chef

Annex 3: CSE Briefings

Please see the Classified version of this report for more information.

Annex 4: Intelligence products related to the threat or incidence of foreign interference in Canadian democratic processes and institutions since January 2019

Please see the Classified version of this report for more information.