Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Public Summary of the Classified Interview of: Shelly Bruce, Alia Tayyeb, Dan Rogers

Senior officials from the **Communications Security Establishment ("CSE")** were interviewed in a panel format by Commission counsel on February 8, 2024. The interview was held in a secure environment and included references to classified information. This is the public version of the classified interview summary that was entered into evidence in the course of the Commission's in camera hearings held in February and March 2024.

Notes to Reader:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.
- This summary has been produced in reliance on subclause (a)(iii)(C)(II) of the Commission's Terms of Reference. It discloses the evidence pertinent to clauses (a)(i)(A) and (B) of the Commission's Terms of Reference that, in the opinion of the Commissioner, would not be injurious to the critical interests of Canada or its allies, national defence or national security.
- This summary contains information that relates to the Commission's mandate under clauses (a)(i)(A) and (B) of its Terms of Reference. Information provided during the interview that relates to other aspects of the Commission's Terms of Reference has been omitted from this summary, but may be adduced by the Commission at a later stage of its proceedings.
- This summary should be read in with the unclassified CSE Institutional Report.

Background and Mandate

CSE is Canada's national cryptologic and signals intelligence agency. Its core mandate is defined by the provisions of the *Communications Security Establishment Act.* CSE collects foreign intelligence from the global information infrastructure primarily through electronic signals / information, referred to as signals intelligence ("**SIGINT**"). CSE uses SIGINT to produce intelligence reports.

Shelly Bruce was appointed Chief of CSE in June of 2018, and served in this role until August of 2022. As Chief, she was the senior executive of CSE, with responsibility for the management and operation of CSE. She retired in 2022.

Alia Tayyeb was appointed Deputy Chief, SIGINT at CSE in 2022. She is also responsible for foreign cyber operations as they relate to CSE's mandate.

Dan Rogers was appointed Deputy Chief, SIGINT at CSE in 2018. He was then appointed Associate Chief of CSE in January of 2022. He served in this role until May of 2023.

CSE's Definition of Foreign Interference

Ms. Bruce explained that pursuant to the *CSE Act*, CSE foreign signals intelligence collection is dictated by the Government of Canada's Intelligence Priorities, which includes foreign interference ("FI"). Ms. Tayyeb elaborated that while CSE is familiar with and accepts the definition of FI used by the **Canadian Security Intelligence Service ("CSIS")**, CSE is guided by the Intelligence Priorities which includes both foreign influence as well as foreign interference. Influence is broader than interference and encompasses the intentions, activities and capabilities of foreign states.

Ms. Bruce discussed CSE's mandate as it relates to FI. She identified five aspects of the CSE mandate:

1) The foreign intelligence mandate;
2) The cyber security and information assurance mandate;
3) The foreign cyber operations mandate;
4) The defensive cyber operations mandate; and
5) The assistance mandate.

She explained that all five aspects of CSE's mandate are relevant to the investigation of FI. For example, CSE's foreign intelligence mandate involves the collection of intelligence to determine the motivations, intentions, and capabilities of foreign entities, based on Canada's intelligence priorities. CSE may provide this intelligence to partners through Section 16 of the CSE Act. Clients who receive that intelligence may use it to take action. If the client determines that action is required, they must request permission from CSE to ensure the intelligence is used in a way that safeguards national security and does not compromise CSE equities.

Ms. Bruce noted that CSE also engages with FI-related matters through its cybersecurity and information assurance mandate. For example, CSE works with partners to help protect the electronic components of infrastructure, such as those required to organize and administer general elections.

Ms. Bruce explained that CSE, through the Canadian Centre for Cyber Security (the "**Cyber Centre**"), also conducts outreach to political parties, and provides advice and guidance to IT [information technology] managers of election campaigns to promote the security of these campaigns. The Cyber Centre has also set up a "hotline" for questions, conducts threat assessments for the public, and produces a bi-annual national cybersecurity threat assessment. The Cyber Centre has also reached out to Canada Post, for example, regarding the security of systems supporting mail-in ballots during the 2021 election.

Ms. Tayyeb added that in relation to threats to democratic institutions and elections security, it was useful to conceptualize CSE's cybersecurity and information assurance mandate as aimed at protecting three entities: voters, political parties, and electoral infrastructure. To protect voters, CSE, though the Cyber Centre, issues public advisories, promotes awareness of cyber hygiene, and updates the public on what threat actors are doing. To protect political parties, the Cyber Centre provides advice and guidance about security best practices. To protect electoral infrastructure, the Cyber Centre works with Elections Canada, and helps protect electronic voting infrastructure from cyber attacks.

Ms. Bruce discussed CSE's foreign cyber operations mandate. She explained that during the 2019 and 2021 elections, a Ministerial Authorization was in place to permit CSE to take action, if necessary, to disrupt attacks against electoral infrastructure.

Finally, Ms. Bruce touched on the assistance aspect of CSE's mandate. She noted that CSE can provide operational and technical assistance to other agencies as requested. These agencies include CSIS, the **Royal Canadian Mounted Police** (**"RCMP**"), **the Department of National Defense/Canadian Armed Forces** (**"DND/CAF"**), and the Canadian Border Services Agency. When providing assistance to these departments and agencies, CSE acts under the requestor's mandate and policies, and the results of this assistance are owned exclusively by the requesting department and agency.

When operating pursuant to its own mandate, CSE is forbidden from conducting activities directed at Canadians or persons in Canada. CSE's mandate is focused on activity or information that is foreign in nature.

Aspects of CSE Mandate

Mr. Rogers pointed out that some aspects of CSE's mandate work together. For example, the information gathered through CSE's foreign signals intelligence mandate is used to inform the reporting issued through CSE's cybersecurity and information assurance mandate.

Ms. Bruce echoed that all aspects of CSE's mandate inform one another. CSE's foreign signals intelligence mission feeds into the cybersecurity and information assurance mission, and also supports CSE's foreign cyber operations. Likewise, the information garnered from the cybersecurity mission feeds back into the foreign signals intelligence mission. Information is shared organically and dynamically through established information-sharing mechanisms within CSE.

Mr. Rogers used the example of a **distributed denial of service attack ("DDOS")** [a type of cyber operation that temporarily disables a website by flooding it with such high levels of internet traffic that it is unable to respond to normal requests] to explain how this information sharing would work in practice. In the event of such an attack, the Cyber Centre might find indicators that the operation was conducted by foreign actors. Then,

those involved in the foreign signals intelligence mandate could investigate. Finally, in certain circumstances, those involved in the foreign cyber operations mandate might take action to disrupt the operation.

Ms. Tayyeb flagged that CSE investigates foreign actors to determine their intentions. If CSE's foreign signals intelligence team finds information that suggests an actor will launch a cyber attack, they advise those responsible for foreign cyber operations. At that stage, those involved in foreign cyber operations could take appropriate measures to disrupt the attack.

Ms. Tayyeb also underscored the difference between active and defensive cyber operations, pursuant to sections 18 and 19 of the *CSE Act*. A defensive cyber operation occurs when a cyber attack is underway against Government of Canada systems or designated systems of importance, and CSE must defend against it. An active cyber operation is where CSE takes online action to disrupt the capabilities of foreign threat actors and to degrade their ability to target Canada.

Coordination Between Groups

Ms. Tayyeb noted there are many procedures in place to facilitate cooperation and coordination among the various groups and sections within CSE. Everyone knows their roles well. These procedures are both formal and informal in nature. For example, those involved in SIGINT might share SIGINT with cyber security and cyber operations colleagues via formal reports, and follow up with meetings/emails/phone calls. These teams are co-located and have a robust and collaborative working relationship. This ensures information is shared dynamically and all team members are well-connected.

Mr. Rogers noted that in some cases, it is not always necessary to have a formal procedure for coordination within the agency because of these collaborative working relationships. In certain circumstances, however, there must be controls to ensure legal and policy compliance, such as when intelligence may be used for advisories or in operations. Doing so ensures proper information handling.

Ms. Tayyeb added that there is a robust framework for operational approvals relating to cyber operations. There is an escalating governance system in place, and plans to govern any foreign cyber operations that arise. Ms. Tayyeb added that such operations also have

an escalating requirement for input from and collaboration with **Global Affairs Canada** (**"GAC"**).

CSE's Assistance Mandate

Explanation of Assistance Mandate

Mr. Rogers explained that CSE's assistance mandate allows CSE to act on behalf of federal law enforcement or national security agencies and on behalf of DND/CAF. When CSE is engaged in assistance, it operates under the authority of the agency it assists, and takes on the authorities and limits of that agency. For example, if CSE were to assist CSIS, it would be bound by the same conditions as those that bind CSIS.

Typically, Mr. Rogers explained, a federal law enforcement or security agency will make a request for CSE's technical assistance. Upon receipt of a request for assistance, CSE engages a formal process to evaluate the request. This process involves a legal assessment and a plan of operations to understand the request. The plan of operations may set out parameters for data retention, or assess how CSE will create the technical capabilities requested, or any applicable reporting requirements.

Mr. Rogers stated requests often involve technical assistance to collect or analyze intelligence. A CSIS request, for example, might ask for CSE's help intercepting communications pursuant to a warrant.

Ms. Tayyeb underscored that it was important to note that for every request, CSE ensures itself that the requesting agency has the legal authority to do what it is requesting CSE to assist with. Mr. Rogers added that these requests are typically very specific and may be related to Canadians. If that is the case, CSE takes special measures to ensure that any information collected under these requests is treated with the appropriate conditions which apply to the requesting agency (e.g. retention periods) and is appropriately limited in distribution within CSE. In part, this is because CSE's own mandate does not permit CSE to direct activities at Canadians or anyone in Canada.

He went on to note that the information collected pursuant to a request for assistance belongs to the requesting agency. For example, information that CSE collects pursuant to a request from CSIS belongs to CSIS. CSIS decides what to do with the information,

and who can receive it. If the information collected is also relevant to CSE's mandate, then CSIS can decide whether to disclose that information back to CSE for CSE's use.

Assistance Mandate During the 2019 and 2021 Elections

Mr. Rogers explained that CSE provided assistance to CSIS in relation to CSIS's foreign intelligence mandate. This work helped to inform SITE's strategy and interests during the 2019 and 2021 elections. However, he was not aware of any other specific requests for assistance related to FI made to CSE during either election period.

Information Sharing

Central Database

Ms. Bruce explained that CSE-produced intelligence is uploaded onto a central database. Clients can then go onto the database and search for information pertinent to their intelligence priorities. CSE decides who can access what information. The database ensures that CSE's clients can access information and intelligence relative to their priorities. CSE serves many clients, and sometimes information or intelligence is relevant to more than one client.

Ms. Tayyeb described two products that go onto this database: end product reports, and summary products. An end product report is a specific detailed intelligence report. Summary products are less detailed, may sum up several reports and are crafted for specific audiences.

Mr. Rogers noted that CSE will flag intelligence reports for specific clients. He also noted that analytic exchanges, discussions, and other exchanges occur between CSE and their CSIS counterparts. For example, the CSE team dedicated to intelligence related to a given state will frequently exchange information with the CSIS desk for that state. If CSE discovers information that is important to CSIS, CSE employees may call or alert relevant CSIS employees that information would be forthcoming before it is published in a report, and provide any appropriate context. Outside of the context relating to a request for assistance, CSE will not suggest investigative actions in Canada, as this falls outside CSE's mandate.

Mr. Rogers also noted that CSE suppresses the identities of Canadians that incidentally show up in CSE's foreign intelligence reporting. If the recipient of the report needs to know the identities of those Canadians, and has a valid authority to receive it, then there are formal processes in place to release that information to a limited number of people in appropriate cases.

Dissemination and Tracking of Compartmentalized Information

Ms. Tayyeb explained that access to compartmentalized information is controlled primarily by technological access controls. These controls are based on the need-to-know principle and dissemination policies. Mr. Rogers added that, in addition to these formal controls, there is a culture and systems in place (e.g. the government's standing intelligence requirements) within CSE and the intelligence community that ensures that CSE employees assigned to a specific topic are aware of (i) where the intelligence that they need to access is located and the various teams with whom they should interact on a regular basis to discuss it and (ii) what intelligence needs to be shared with external partners. All witnesses underscored that these practices were long-embedded in CSE's culture.

Outside of CSE, Mr. Rogers explained that **Client Relation Officers** ("**CROs**") [employees of CSE housed within other departments or agencies such as CSIS, DND or the Privy Council Office] cooperate with senior government officials to ensure that the officials have access to relevant information in the database. CROs are also typically responsible for providing information to senior government officials and ministerial offices.

Mr. Rogers explained that, since most ministers do not work in a sensitive compartmented information facility, a CRO would typically bring a physical binder to a Minister for them to read its contents. The CRO would take the binder when the Minister had finished reading and would record that the report was provided. Ms. Tayyeb specified that this was the most reliable way CSE has at the moment of tracking whether a senior official had read a CSE intelligence product. She added that the database used by CSE also has a tracking system that allows CSE to see who has opened a given report directly, or has been provided a copy by a CRO. Mr. Rogers further indicated that, to evaluate the usefulness of its intelligence products, CSE monitors this tracking system for feedback

(which can be provided electronically or through CROs) and conducts surveys with its intelligence clients.

Ms. Tayyeb also added that, in addition to CROs, CSE trains SIGINT Dissemination Officers, who are employees of the relevant department or agency, but essentially perform the same functions as CROS.

CSE Activity During the 2019 and 2021 Election Periods

Ms. Bruce stated that CSE identified various attempts to scan, probe or exploit Canadian electoral infrastructure during the 2019 elections. However, none of these attempts compromised Canada's electoral infrastructure.

Mr. Rogers noted that CSE monitored cyber attacks and intrusions during the elections, and this was relevant given cyber attacks could be used as a component of FI activity. Ms. Bruce added that CSE has focused on cybersecurity during elections since 2017, when then-Minister of Democratic Institutions Gould's mandate letter was issued directing CSE to focus on this area. Ms. Bruce explained the letter followed documented incidents of online foreign interference relating to the 2016 elections that took place in the United States of America.

Ms. Bruce explained that, due to Canada's paper-based voting system, the systems that CSE helps monitor are primarily administrative in nature, e.g., Elections Canada networks, voter registry, broadcasting of debates, and CSE also helps to safeguard the communications of elected officials. She also underscored the need to safeguard online infrastructure in order to ensure public trust in electoral systems, and recalled that CSE has also reached out to Canada Post regarding best cybersecurity practices for systems supporting mail-in ballots.

Security and Intelligence Threats to Elections Task Force (SITE TF)

All witnesses emphasized that SITE TF played a key role in the lead up to, and during, the elections. Ms. Bruce explained that SITE TF was composed of representatives of the RCMP, CSIS, GAC, and CSE. All witnesses noted that the cooperation that occurred between agencies in relation to SITE TF was representative of cooperation in the

Canadian intelligence community in other contexts. They emphasized that SITE TF was unique because the cooperation was public, formalized and specifically aimed at identifying threats to the elections.

Ms. Bruce and Ms. Tayyeb explained that all intelligence that CSE was aware of and that was relevant to the security of the elections was brought to SITE's attention by the CSE representative. This was consistent with one of the objectives of SITE, which was to ensure that intelligence pieces that, on their own would not be assessed as significant, could be combined with other pieces of intelligence to gain a broader understanding of potential threats and incidents. Ms. Bruce identified the protection of very sensitive collection techniques or sources as the only possible reasons that would justify reframing information that would be shared with SITE so that the gist of the intelligence could be delivered without disclosing the sensitive information.

Attribution

All witnesses noted the technical challenges of attributing a given activity to a foreign state. Ms. Bruce noted that CSE's activities tend to target actors and entities who want to remain covert. Mr. Rogers noted that this creates particular challenges when it comes to attributing the following activities:

1. **Cyber attacks** (*e.g.* hacks): These attacks usually require sophisticated forensic and technical analysis of SIGINT, as well as other cyber security forensics, to identify the entity or actor that is responsible for a given incident;

2. **Disinformation campaigns:** This type of cyber activity is challenging to attribute because the technical information required to do so is often in the hands of third parties, such as social media platforms.

Mr. Rogers added that, while CSE is the agency that is responsible for determining whether a given cyber attack can be attributed to a foreign actor from a technical standpoint, GAC has a lead role in determining whether this attribution should be made public. CSE may provide input to GAC in such circumstances to ensure that any collection techniques remain protected.

Specific Incidents

All witnesses discussed a specific SITE TF intelligence bulletin from the period leading up to the 2019 election related to potential social media interference in Canadian democratic processes by a foreign state. The bulletin contained information about a network of social media accounts potentially linked to the foreign state.

The witnesses had no specific memory of this incident. They did note, however, that it was likely an example of the relevant technical details being unavailable or that the information resides in the hands of a third party, such as a social media company. Mr. Rogers noted that CSE had good relationships with social media companies, but highlighted that government engagement with social media companies was specifically delineated across the various SITE agencies, and initiatives to address foreign disinformation was GAC's responsibility.

Ms. Tayyeb noted that this case was an example of the limits inherent in CSE's mandate. CSE's mandate is restricted to foreign intelligence. Where a social media activity does not, on its face, have a foreign element, CSE will not analyze it further, except under a request for assistance from another agency acting within the scope of its statutory mandate. She added that this creates challenges, especially in cases involving social media activity which can be designed to appear Canadian-based. Ms. Tayyeb mentioned that SITE's collaborative approach contributed to address this challenge by ensuring that each partner's mandate could be leveraged as appropriate.

Ms. Tayyeb also mentioned a CSE report that detailed potential FI by an official of a foreign state. This information was gathered and reported to SITE after the 2021 election. She identified this report as the most significant intelligence related to FI that CSE had collected during either the 2019 or 2021 election. Ms. Tayyeb explained that this report was shared with CSIS.

Mr. Rogers added that, while CSE did not detect much in the way of incidents in the 2019 and 2021 elections, they were monitoring relevant actors and in some cases were aware of what their specific priorities were. Ms. Bruce also noted that CSE had taken several

initiatives ahead of the elections to raise cyber awareness among Canadian citizens and institutions.