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

Interview Summary: Caroline Xavier, Rajiv Gupta, Alia Tayyeb

Senior officials from the Communications Security Establishment ("**CSE**") were interviewed in a panel format by Commission Counsel on June 14, 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 hearings held *in camera* in July and August 2024. It discloses the evidence 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.

Notes to Reader:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.

1. Witnesses

[1] Caroline Xavier was appointed to the position of Chief, CSE, effective August 31, 2022. As Chief, she is responsible for the management and operation of CSE.

[2] Rajiv Gupta was appointed Associate Head, Canadian Centre for Cyber Security ("**CCCS**") effective July 2021. In his role as Associate Head, Mr. Gupta is responsible for advancing the Cyber Centre's strategic vision to enable a secure digital Canada.

[3] 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.

2. Evolution of the Threat Landscape

2.1 Key Actors and CSE's Mandate

[4] Ms. Xavier explained that foreign interference ("**FI**") has been an intelligence priority for many years. Since 2017, the CCCS has released four public reports on cyber threats to democratic institutions.[1] These publications identify four main threat actors: the People's Republic of China ("**PRC**"), Russia, Iran, and North Korea. The PRC and Russia conduct most of the attributed cyber activities targeting foreign elections. However, in 2022, 85% of such cyber threat activity was unattributed.

[5] As highlighted in the last Threats to Democratic Processes report published in December 2023, Ms. Xavier stated that misinformation and disinformation are pervasive. Politicians, candidates and voters are key targets for disinformation and misinformation exacerbated by artificial intelligence ("**AI**"). Cybersecurity is of particular importance. CSE has identified in its various publications that critical infrastructure [including processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security, and economic well-being of Canadians and the effective functioning of government] are vulnerable to cyber-attacks and other cyber incidents. Protecting critical infrastructure is a part of CSE's cyber assurance mandate.

[6] Ms. Xavier explained that CSE gained further insight to the range of available foreign cyber tactics by observing Russian cyber tactics during the war in Ukraine, and from CSE actionable intelligence. By doing so, CSE added to its knowledge base of cyber tactics and techniques. She noted that some cyber threat actors of the PRC "pre-position" themselves by hacking into critical infrastructure systems and retaining access to those systems to later affect their functioning. This technique, sometimes called "living off the land", involves the use of native tools and processes to blend in with normal system activities and operate discreetly, reducing the likelihood of being

[1] The most recent is "Cyber Threats to Canada's Democratic Process: 2023 update", and can be found on the CSE website. This report is the fourth iteration of CSE's Cyber Threats to Canada's Democratic Process and provides an update to the 2017, 2019 and 2021 reports. CCCS also regularly releases a National Cyber Threat Assessment. It has done so in 2018, 2020, and most recently, 2023–2024.

detected or blocked. Ms. Tayyeb added that CSE observed threat actor, “Volt Typhoon”, use this tactic.

[7] Mr. Gupta added that to combat cyber threats in the context of democratic institutions, CSE provides advice and guidance on election infrastructure. He echoed that misinformation and disinformation, circulated through AI techniques like synthetic chat, deepfakes, and other types of “botnet activity”, have become prevalent.

[8] Mr. Gupta noted that federal systems are not the only targeted systems. Provinces, territories, municipalities, and Indigenous governments are also exposed. In some contexts, CSE helps protect important provincial, territorial and municipal systems, such as provincial and territorial electoral infrastructure, provided these systems fall within critical infrastructure, which are part of CSE’s cyber assurance mandate.

[9] Ms. Xavier added that the provinces, territories, and municipalities have fewer resources to deal with cyber threats. She noted that CSE works with the provinces and territories to provide advice and guidance. CSE has a Ministerial Authorization (“**MA**”) to provide technical support to the territories and has supported other non-federal entities that have been identified as systems of importance. While CSE recently acquired this MA, it had already been helping territories through its cyber assurance mandate. CSE’s efforts are aimed at responding where cyber incidents occur and working to prevent them. CSE has started to circulate guidance in Indigenous languages, in addition to English and French.

2.2 Specific Tactics and Techniques

[10] Ms. Tayyeb explained that CSE is currently focused on monitoring FI activities from the PRC, Russia, India, and Iran. In response to a question about new FI trends and techniques, she notes that aside from traditional cyber techniques, CSE has observed threat actors engaging in in big data collection for influence campaigns and leveraging resources from their own state apparatus and other communications organizations. Ms. Xavier explained that there is an increasing blending of state and non-state actors, as cyber criminals act on behalf of states as cyber proxies.

[11] In terms of other new trends, Ms. Tayyeb highlighted that Russia has increased its use of state-owned international media outlets to amplify influence campaigns. The PRC increasingly conducts its activities through non-traditional networks by subcontracting to non-state actors, including UFWD affiliates. Ms. Tayyeb also referenced the PRC's tactics like information manipulation, crafting false narratives, and propagating mis- and disinformation.

[12] Ms. Xavier stated that CSE's last National Cyber Threat Assessment published in 2022 highlights the targeting of diaspora groups, which is becoming more prevalent. This includes content monitoring on foreign-based applications and social media-enabled activity. She explained that the purpose of the published CSE cyber threat assessments is to identify trends and help Canadians understand the FI threat environment. Mr. Gupta noted that the Citizen Lab, an independent research group, has published some work on FI and diaspora groups within Canada.

3. Cyber Threats and Programs

3.1 PRC's Cyber Program

[13] The panel confirmed that the PRC's Cyber Program, a broad initiative that draws from the collective capacity of the PRC's intelligence services and across a wider ecosystem of state and non-state actors, has been assessed as demonstrating capabilities that pose a high-level threat to Canada and its allies. Mr. Gupta described the "sheer relentlessness" of the Cyber Program's threat activities. He observed the Cyber Program's efforts, given the involvement of state and non-state actors, was sizeable and ongoing. CSE has observed persistent PRC cyber activity against Canadian systems.

[14] In response, CSE is leveraging its authorities to conduct active cyber operations ("**ACOs**"), as well as defensive cyber operations ("**DCOs**"). The cyber techniques used by the PRC will inform the manner in which CSE defends Canada's infrastructure against anticipated future threats.

[15] Mr. Gupta identified a PRC-linked cyber threat actor as one of the biggest and most sophisticated cyber threat actors currently targeting Canada. This threat actor has the ability to conduct malicious cyber activity, often with a goal of maintaining ongoing access to a target's network. This threat actor has been observed attempting to compromise federal, provincial and territorial government systems, and to target government officials, researchers, politicians, and others. CSE has recently published an unclassified piece about this threat actor, though it does not name the threat actor.

[16] Ms. Xavier noted that CSE's cyber program is effective. Currently, for example, CSE stops nearly six billion malicious cyber actions against the federal government systems on a daily basis. Each action is an opportunity from which to discover information about the threat activity.

3.2 Defending Federal Government Systems

[17] Mr. Gupta explained that CSE uses a variety of sophisticated automated sensors to defend Canada's government systems. These sensors monitor the information pipelines leading in and out of government systems. The sensors help detect suspicious activity and cyber-attacks. The program has been rolled out over a number of years and now covers most federal government departments. CSE has recently begun installing these sensors on government-issued laptops, which has increased CSE's threat coverage.

[18] Mr. Gupta added that, since 2019, CSE also employs sensors on Elections Canada infrastructure, allowing CSE to support Elections Canada and ensure the integrity of their systems.

[19] Mr. Gupta emphasized that having more sensors does not eliminate all risk of malicious cyber activity. The best way to mitigate risk is through multiple layers of protection, including an informed public. Mr. Gupta noted that CSE has observed cyber-attacks in 26% of international elections observed globally in 2022, and has observed mis- or disinformation in 100% of those elections.

3.3 Defending Provincial and Territorial Government Systems

[20] Ms. Xavier explained that CSE also engages with provincial and territorial governments, including by placing sensors within their systems when they are deemed systems of importance and when appropriate. CSE does so further to a Ministerial Authorization (MA) that allows it to assist provinces and territories upon request.

[21] Mr. Gupta referenced a cyber incident that had affected the Northwest Territories' government systems. CSE exercised its authority under the MA to combat the cyber incident. Though CSE can advise of the best route forward, the territory retains ultimate authority to roll out CSE's proposed solutions. Mr. Gupta added that CSE is receiving more and more requests for CSE assistance from provinces and territories.

[22] Mr. Gupta also described a cyber-attack against critical IT systems supporting healthcare providers in Newfoundland and Labrador. CSE assisted the province to contain and address the attack.

4. Other Specific Intelligence Incidents

4.1 Overseas Police Stations

[23] Commission Counsel directed the witnesses to classified documents regarding Chinese overseas police stations located in Canada.

[24] Ms. Tayyeb explained that CSE is aware of the mandate of these police stations, which is officially to provide assistance with administrative matters for PRC citizens and ethnic Chinese living abroad, but are also used in transnational repression activities.

4.2 Access by Foreign Actors to Government of Canada Networks

[25] Commission Counsel directed the witnesses to an email in which a CSE employee disagrees with a Canadian Security Intelligence Service ("**CSIS**") statement regarding campaigns by foreign actors to access Government of Canada networks. Ms. Xavier explained that is not uncommon for individuals within CSE and CSIS to disagree or

have different interpretations or assessments of certain intelligence, given their different operational perspectives.

4.3 Follow-up on Reporting of Potential FI in 2021

[26] Ms. Tayyeb explained that CSE had no update on the intelligence that detailed potential FI by an official of a foreign state gathered and reported to SITE after the 2021 election.

4.4 Collection of Information by UFWD-affiliated Organizations

[27] CSE is aware that UFWD-affiliated organizations have interest in collecting information on Canadian Parliamentarians for the purpose of exerting influence on them.

5. CSE's Role in Attributing Cyber Incidents

[28] Ms. Xavier explained that attribution is an aspect of CSE's toolkit to deal with FI. CSE's first priority when a cyber-incident arises is to address and stop the incident. Generally, CSE will not take active steps to attribute an incident until it is under control. The attribution process requires a lot of technical work.

[29] Mr. Gupta added that the more information CSE has on the threat landscape, common techniques, and on the cyber incident itself, the better job it can do with attribution. If an incident involves novel behavior, it may take CSE take longer to attribute.

[30] Ms. Tayyeb distinguished between attributing cyber-events and attributing mis- and disinformation campaigns. Often, CSE does not have enough information about the open-source environment or the technical data to confidently attribute mis- and disinformation campaigns. Attributing cyber events is also challenging, however where CSE can obtain technical information from the affected party, this information can be used to patch against the tactics and techniques of known cyber actors. CSE may also have foreign intelligence about threat actor activities and intentions which can help with the attribution process.

[31] Ms. Xavier distinguished between technical attribution and public attribution. CSE is involved in technical attribution—that is, identifying who is behind the cyber event. Public attribution falls within the portfolio of Global Affairs Canada ("**GAC**") and Public

Safety (“**PS**”). These organizations have crafted a Cyber Attribution Framework to determine whether and how to publicly attribute a cyber-event.

[32] Ms. Xavier noted that she could express a view on whether public attribution was desirable, but explained that she was not the final decision-maker as to whether to publicly attribute a cyber-event. Public attribution may be desirable to educate the public or for security reasons. Public attribution may not be desirable in other circumstances because of diplomatic consequences, or because doing so would reveal CSE’s techniques, tactics, or other sensitive national security information.

[33] Ms. Xavier also noted that CSE’s public reporting—is also a form of attribution. Actors are identified in CSE reporting where possible. CSE also attributes actions to threat actors and names specific foreign states in its public reporting. This, too, is a form of attribution, termed “small ‘a’ attribution.”

6. Intelligence Collection, Dissemination, and Tracking

6.1 New Process for Senior Officials

[34] Commission Counsel directed the witnesses to an email from Mr. Dan Rogers, current Deputy National Security Advisor at the Privy Council Office (“**PCO**”), that states the work of the Independent Special Rapporteur (“**ISR**”) identified deficiencies in the way the national security community disseminates and tracks intelligence, and suggests putting together a working group to evaluate solutions.

[35] Following the ISR’s report, Ms. Xavier explained that CSE renewed its efforts to ensure that intelligence is received and understood. She noted that while CSE was already doing much of what was recommended in the report, CSE participated in a working group to examine how intelligence is conveyed and tracked to government clients. The aim of the working group was to identify best practices. Ms. Xavier said that the group actioned various recommendations, which allowed CSIS and CSE to better track who was reading what intelligence, and leverage the tools it had to ensure intelligence was reaching the appropriate audience(s). The group’s work resulted in the establishment of a new system to disseminate and track intelligence circulated to senior officials, set out

in a document called “Intelligence Dissemination and Tracking for Senior Leaders and Political Staff.”

[36] Ms. Tayyeb explained that the new process recognized that a core group of ministers charged with security and intelligence responsibilities needed dedicated support. The new process also enables CSIS to use CSE’s intelligence dissemination and tracking platform. Finally, the new process continues to leverage Client Relations Officers (“**CROs**”).[2] CSIS has also placed a dedicated information officer within Public Safety to help manage intelligence dissemination.

[37] The CRO network is still growing. Ms. Tayyeb explained that CSE continues to look for solutions to grow the capacity of CROs and meet the needs of government clients.

6.2 Criteria for Dissemination to Senior Officials

[38] Ms. Tayyeb explained that intelligence is disseminated to senior officials within government based on an analysis of intelligence priorities and feedback from departments and officials about their intelligence requirements and preferences. Usually, the applicable deputy minister will determine what intelligence goes to their minister. In CSE’s case, the Chief or her delegate decides what intelligence goes to the Minister of National Defence. In all cases, the decision as to what intelligence should be briefed is guided by Canada’s intelligence requirements.

[39] Ms. Tayyeb clarified that CSE does not unilaterally select what intelligence is provided to senior officials. Rather, senior officials and other clients identify areas of interests and ask CSE for specific intelligence. CSE fulfils these needs. CSE tracks requests and uses client feedback to adjust its collection and intelligence reporting, so as to better meet the needs of government clients. CSE prepares a list of intelligence it determines is interesting or relevant, based on what CSE knows, to circulate to security and intelligence Deputy Ministers, including the NSIA.

[2] CSE employees housed in other government departments, charged with the responsibility of communicating CSE intelligence to officials in those departments.

6.3 Briefings and Intelligence Regarding Members of Parliament

[40] Commission Counsel directed the witnesses to CAN027809, a memorandum from May of 2023 that states CSE and other Public Safety portfolio agencies are developing internal measures to ensure their respective Ministers are proactively made aware of any national security threats to Members of Parliament and their families, in response to a direction from the Prime Minister that he and Ministers are to be proactively made aware of such threats.

[41] Ms. Xavier explained that CSE already operated in a manner responsive to the Prime Minister's direction. Anything of broad importance is flagged to the Minister, including intelligence relating to or threats against Members of Parliament. Nevertheless, Ms. Xavier issued a "Chief Directive" specifically directing CSE to flag any intelligence collected that implicated Parliamentarians.

7. Cyber Operations

7.1 Active and Defensive Cyber Operations in General

[42] Ms. Xavier explained that 2019 legislative amendments permitted CSE to conduct ACOs and DCOs (together, termed foreign cyber operations ("**FCOs**")). FCOs are intended to protect the welfare of people living in Canada. She noted that ACOs are more relevant to combat FI.

[43] Ms. Tayyeb explained that CSE obtains MAs to conduct ACOs. Currently, CSE has a number of MAs including one to conduct DCOs against any activity directed at federal government systems or systems of importance (as defined by the federal government).

7.2 Specific FCOs

[44] Ms. Tayyeb noted that CSE has conducted a specific cyber operation against an adversary, and provided details about this operation.

7.3 Resourcing Limitations

[45] Ms. Xavier observed that cyber warfare has become a critical part of national defense. In 2022, CSE received an injection of funds from the government to counter hostile cyber activity.

[46] Commission Counsel directed Ms. Xavier to CAN041952, a document called “Canadian Cyber Operations,” from March 2024 which provides a summary of Canadian cyber space and CSE’s capacity to conduct cyber operations and identifies a lack of sufficient capacity. Ms. Xavier explained that CSE’s capacity to conduct cyber operations has increased since the preparation of the document. Ms. Xavier explained that because CSE has demonstrated what it can deliver, CSE was given increased resources in Budget 2024 that have increased its capacity to conduct more cyber operations at a time. The rate of growth was described as reasonable, particularly given the challenge CSE has in attracting and retaining employees with the specialized knowledge necessary.

7.4 Other Constraints

[47] The *CSE Act* provides that the Minister must be persuaded that the objective of the cyber operation could not be achieved by other reasonable means to obtain an ACO or DCO authorization from the Minister of National Defence. Commission Counsel asked whether this pre-condition poses an obstacle for CSE. Ms. Tayyeb opined that this is not an obstacle, as CSE does not interpret this provision as requiring that the cyber operation be a measure of “last resort” or the *only* means available to achieve an objective. The panel did not identify any other legislative issues or gap.

[48] Ms. Tayyeb noted that the legislative constraint that affects operational effectiveness the most is that it must not target Canadians or infrastructure in Canada. She did not suggest this constraint should be removed or amended. This requirement limits CSE’s capacity to collect intelligence and defend Canadian cyber space. However, Ms. Tayyeb explained that this kind of limitation on signals intelligence and cyber operations is common among other countries. She understands that other countries have different rules for cyber operations, as opposed to foreign intelligence collection. She

underscored that CSE must always consider the impact on Canadians, and that CSE takes care to ensure that its operations are constructed so that their effect is not directed at Canadians. Further, the Canadian identities are suppressed in CSE's intelligence reports, and can only be divulged through a formal procedure that is handled by a dedicated team at CSE.

[49] When asked about CSE's ability to leverage open source intelligence ("**OSINT**")[3], Mr. Gupta explained that under the cybersecurity aspect of CSE's mandate, its ability to acquire open source or commercial cybersecurity threat intelligence has been limited to some extent by the fact that CSE cannot directly acquire the information without a Ministerial Authorization, if doing so would interfere with the reasonable expectation of privacy of a Canadian or person in Canada.

[50] Ms. Xavier did not identify any issues regarding CSE reporting to the Minister of National Defence. Ms. Xavier emphasized that CSE's mandate is to protect Canadians. The panel explained that CSE lives in "three worlds" and that the mandate clearly outlines its involvement in International affairs, defence and security. Given the operational and historical connectivity between CSE and the Canadian Armed Forces, and the importance of SIGINT to Canada's national defence capabilities, it is logical to have CSE report to the Minster of National Defence.

8. Outreach

8.1 Public Outreach

[51] Ms. Xavier explained that CSE conducts public outreach on a regular basis, through publications like CSE's National Cyber Threat Assessments, by attending high schools and community centers to engage with youth, or hosting events such as Hackathons. She noted that CSE has begun to publish some of its public-facing materials in Indigenous languages, as well as in English and French.

[3] Information that is not classified and can be found online, for example.

[52] Mr. Gupta explained that CSE has engaged with marketing teams to ensure its publications reach Canadian audiences. CSE regularly tracks its readership. He would welcome recommendations on how to increase public awareness of the publications and guidance CSE produces.

8.2 Communications and Work With International Partners

[53] Ms. Tayyeb stated that CSE faces little to no obstacles to interacting with international partners. CSE needs a memorandum of understanding ("**MOUs**") to share intelligence and pursue relationships with international partners. CSE has a number of these MOUs already in place. New cyber centers are cropping up all around the world. It is in CSE's interest to connect with and learn from these centers to the extent possible.

[54] Mr. Gupta added that CSE also partners internationally with Computer Security Incident Response Teams (such as the International Watch and Warning Network) to share threat information.

9. Concluding Remarks

[55] Ms. Tayyeb noted that CSE has adequate resources and legislative authorities to fulfil its mandate, as well as the necessary Ministerial authorizations. There is no pressing need for many changes. One of the most important challenges in the broader community is in devising mechanisms to respond to foreign interference in a coordinated way across government. Ms. Xavier explained that it is important for Canadians to understand that cyber-threats will never be zero risk.