Unclassified

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

In Camera Examination Summary: Caroline Xavier, Alia Tayyeb, Sami Khoury

Commission Counsel examined senior officials from the Communications Security Establishment ("**CSE**") during *in camera* hearings held in July and August 2024. Counsel for the Attorney General of Canada appeared on behalf of the Government of Canada and had the opportunity to examine the witness. The hearing was held in the absence of the public and other Participants. This summary discloses the evidence that, in the opinion of the Commissioner, would not be injurious to 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. Examination by Commission Counsel

1.1 Witnesses and Evidence

[1] Caroline Xavier was appointed to the position of Chief of CSE, effective August 31, 2022.

[2] Sami Khoury is the Head of the Canadian Centre for Cyber Security ("**Cyber Centre**"), effective August 2021.

[3] Alia Tayyeb was appointed Deputy Chief of Signals Intelligence ("**SIGINT**") at CSE in 2022. She is also responsible for foreign cyber operations at CSE.

[4] The witnesses confirmed the accuracy of the summary of their panel interview and adopted its content as part of their evidence before the Commission. CSE's unclassified institutional report and classified annex were entered into evidence.

1.2 Threat Landscape: 2013 – Present

[5] Ms. Xavier testified that CSE has been putting out reports on national cyber threats, including FI, since at least 2017. CSE has been in the business of collecting foreign intelligence for almost 80 years. For that time frame, CSE has had a signals intelligence mandate to collect foreign intelligence. CSE's intelligence collection is guided by the Government of Canada's intelligence priorities, which are set through Cabinet decisions.

[6] CSE has long observed instances of foreign interference ("**FI**") in Canadian democratic institutions. FI has been an intelligence priority since at least 2016. Ms. Xavier testified that FI has increased over the last five to eight years. CSE has highlighted this fact in its public-facing reports, which include national cyber threat assessments from the Canadian Centre for Cyber Security ("Cyber Centre"), as well as four reports entitled Threats to Democratic processes.[1]

[7] The most significant development is that the People's Republic of China ("**PRC**") has become more audacious and sophisticated in the manner in which it conducts FI. CSE has reported this in its Threats to Democratic Processes reports. She added that the PRC has been, and continues to have, a significant strategic interest toward Canada. Russia, Iran, and North Korea also pose an FI threat to Canada, though CSE has primarily observed Russia and the PRC as the two main actors with an interest in Canada. These main actors are named in CSE's public-facing National Cyber Threat Assessments.

[8] Ms. Tayyeb testified that FI in democratic institutions is not a new phenomenon. From CSE's perspective, the focus for collection pre-2015 relating to foreign interference and influence threats was foreign espionage activities, as well as foreign monitoring of and influence on dissidents—rather than FI in democratic institutions. Following reports of Russian interference in the 2016 United States presidential election, FI in democratic institutions became a priority intelligence requirement.

[1] The most recent Threats to Democratic Processes was put out in December 2023, and can be found on CSE's website.

[9] Ms. Tayyeb noted that CSE has observed an increased amount of FI activity in cyber space. In earlier years, FI activity revolved around embassies and human proxies. Threat actors have remained relatively consistent since 2015, with the PRC and Russia being the most prolific actors, and with India and Iran also operating in this space. She added that another country was more active in conducting FI in Canada in previous years, and is less active today.

[10] Canada is a lower priority target for cyber threat activity from Russia than some of its allies, such as the United States. Ms. Xavier added that these facts were reiterated in CSE's most recent Threats to Democratic Processes report.

[11] Mr. Khoury testified that although the Cyber Centre was stood up in 2018, CSE has been involved in cyber monitoring as early as 2013. He described a 2013 cyber attack detected against Canada's National Research Council. This incident "opened eyes" to the fact that foreign nations could use cyber techniques to steal Canadian intellectual property from a Canadian organization. Before 2013, CSE was aware of cyber activity, but that activity was mostly directed from nation states to other nation states (instead of non-governmental organizations). Incidents like these led to the creation of the Cyber Centre. The Cyber Centre aims to share CSE technical knowledge and expertise with Canadian society outside of government.

[12] Mr. Khoury testified that over the years, the Cyber Centre has seen an evolution in cyber techniques and tactics. CSE has observed state tools being directed against non-state infrastructure, against provincial infrastructure, and municipal infrastructure. The Cyber Centre has also observed an increase in the sophistication of cyber techniques used. While the four main actors remain constant (i.e., Russia, China, Iran, and North Korea), the Cyber Centre has also named the Kingdom of Saudi Arabia ("KSA") in its most recent public-facing national cyber threat assessment. Techniques have evolved from simple espionage, to "hack and leak", to leveraging botnets to flood social media with disinformation, to using AI to amplify narratives and harvest big data.

[13] Ms. Xavier and Mr. Khoury agreed that, in terms of volume of activity, the PRC is the main actor when it comes to cyber threats. Mr. Khoury added that this activity has increased over the years.

[14] Mr. Khoury testified that the Cyber Centre tracks national elections around the world, including with respect to FI in those elections. The Cyber Centre has seen a constant rise in the level of FI threat activity in elections. Mr. Khoury explained the complexity in attributing those activities, including as a result of the use of proxies.

[15] Ms. Xavier testified that PRC-linked cyber threat actors targeting Canada have the ability to conduct malicious cyber activity, often with a goal of maintaining ongoing access to a target's network. PRC-linked threat actors have been observed attempting to compromise various cyber systems. The PRC is a difficult adversary because of its patience, and because it faces fewer constraints than a foreign state operating under a democratic government. Ms. Xavier opined that, nevertheless, Canada and its allies are well positioned to respond to PRC-related cyber threats.

1.3 Cyber Centre Support and Threats to Elections

[16] Mr. Khoury explained that the Cyber Centre is able to assist sub-national levels of government, such as provincial governments, and are aware of "nation state incidents" that have been directed at provinces or territories. The Cyber Centre has supported the provinces and territories in mitigating these incidents. For example, the Cyber Centre helped to mitigate a cyber attack against the Government of the Northwest Territories. The Cyber Centre mitigated the threat to the Government of the Northwest Territories' network. In response, the Cyber Centre worked with the Intelligence Commissioner and the Minister of National Defence to implement proactive deployment of cyber capabilities to prevent these types of incidents in the future.

[17] The Cyber Centre has also worked with other provincial governments to deploy Cyber Centre capabilities and proactively protect provincial government systems. Mr. Khoury testified that the Cyber Centre is currently working with a Canadian province to work through the mitigation of a serious cyber incident, and to help deploy these proactive and preventative cyber capabilities.

[18] Mr. Khoury testified when CSE released its fourth Threats to Democratic Processes report in December 2023, the Cyber Centre held a briefing to all Chief Electoral Officers ("**CEOs**") across Canada. The Cyber Centre is able to assist in provincial elections at

the request of the province's CEO. The first official ask came from a province to formalize a partnership between the Cyber Centre and the agency responsible for elections in that province to prepare for their upcoming provincial election and evaluate their security infrastructure. Discussions are also in progress with the CEO of another province. The Cyber Centre participates in an annual meeting of CEOs across Canada to update on cyber threats to elections, and to see whether they want help defending their electoral cyber infrastructure.

[19] Ms. Xavier stated there is nothing preventing CSE from assisting provinces and territories. In fact, s. 17 of the *CSE Act* allows CSE to give guidance and support to all of Canada. She underscored that good cyber hygiene was a group effort. It takes everyone—government and citizens—to ensure Canadians remain resilient to cyber incidents and attacks. She added that CSE has also been working with Elections Canada to reinforce Canadian electoral infrastructure since at least 2015.

[20] Commission Counsel referred to a document entitled "Countering Mis- and Disinformation: Developing an Emerging Protecting Democracy Agenda,"[2] which identifies that the threat surface is broader at sub-national government levels, because sub-national government electoral processes tend to rely more heavily on electronic means for voting. The document also indicates that the Cyber Centre does not have the capacity to support multiple parallel requests from elections administrators in multiple provinces.

[21] Ms. Xavier testified that this document is outdated. Over the past few years, CSE has received an influx of funding for the Cyber Centre. The document was drafted during a process meant to identify the needs of the Cyber Centre and does not reflect current resourcing. Since Budget 2022, there has been recognition of the fact that CSE is in a growth trajectory and performs an essential function in defending against cyber threats. As a result, CSE has received significant investment in its mandate.

[22] Ms. Xavier testified that digital solutions in elections are becoming more prevalent, and recommended that users build security measures into these systems from the

[2] CAN019525.

beginning. Risk will always exist, even if layers of security exist within a digital solution. Having layers of security, however, can help prevent worst case scenarios. A paper-based approach will limit digital risks, but carry its own risks.

[23] Commission Counsel referred back to "Countering Mis- and Disinformation: Developing an Emerging Protecting Democracy Agenda," which also speaks to the Cyber Centre's defensive planning in relation to GE43. The Cyber Centre leveraged a new defensive cyber-planning group to develop a strategic mitigation plan. However, the document indicates that process was not conducted in GE44 due to a lack of available resources.

[24] Ms. Xavier stated CSE had authority to conduct defensive cyber operations during GE43 and GE44, but did not trigger their cyber defence plan, because there were no incidents that required them to do so. She suggested that because of this defensive posture, the strategic mitigation plan became unnecessary in GE44.

[25] Mr. Khoury added that CSE's defensive capabilities were ready to be activated during GE43, but there was no need to do so. CSE worked with Elections Canada to make sure their infrastructure was secure.

[26] Ms. Xavier stated she would be surprised if the reason the strategic mitigation plan was not conducted in GE44 was a lack resources. Mr. Khoury echoed her view. He added that during an election period, CSE maximizes and reallocates its resources toward protecting elections. Ms. Xavier suggested that the strategic mitigation plan was likely not pursued, because other better defensive plans were available. Both Mr. Khoury and Ms. Xavier agreed that they did not anticipate that CSE would be unable to protect electoral infrastructure in 2025.

1.4 China's Cyber Capabilities and Threat Activity

[27] Commission Counsel referred to a Cyber Centre document from 2022 that provided a baseline threat assessment for the PRC. Mr. Khoury confirmed that the PRC's cyber capabilities have evolved significantly over the last two years, and have increased in terms of sophistication. The PRC has conducted activity against cloud infrastructure and is pre-positioning itself on critical infrastructure. In addition to international partners, CSE also works with multi-national bodies and governance bodies to address the PRC

threat. Ms. Xavier testified that the resolve of Canada and its allies to work together will enable the group to continue to be able to meet the threat posed by the PRC.

1.4.1 How Threat Actors Gain Access to Networks

[28] Mr. Khoury explained that there are two main ways a threat actor can gain access to a network: (i) they can find a vulnerability in the network perimeter and hack into it directly, or (ii) they can leverage emails, as a way of phishing someone or getting someone to click on a link. When the user opens the email or clicks on a link embedded in it, the threat actor gains access to the network, crossing over the boundary of the external defences. He likened these two ways to either coming through the front door, or climbing over a fence.

[29] Ms. Xavier explained that once an adversary enters a network, their aim is usually to steal intellectual property or other information. In other cases, the threat actor may not take any immediate action, but may be attempting to pre-position itself for a later goal.

1.4.2 Campaign Targeting Inter-Parliamentary Alliance on China

[30] [In January 2021, CSE became aware that there was an actor, determined to be APT31, conducting an email operation targeting Canadian Parliamentarians, including Parliamentarians who were members of the Inter-Parliamentary Alliance on China ("**IPAC**"), as well as House of Commons infrastructure.]

[31] Ms. Xavier testified that the Cyber Centre advised House of Commons IT security officials promptly of the operation and worked with them to further investigate and gather more information about what happened. This was normal procedure. Ms. Xavier underscored that CSE has a good relationship with House of Commons IT, and completed a Memorandum of Understanding with House of Commons IT in 2016. The witnesses undertook to provide a chronology of the incident and related communications. That chronology has been provided, and is publically available. It is entitled: "Chronology of Events | Email tracking link campaign targeting Canadian Parliamentarians."[3]

[3] CAN047441.

[32] Through multiple conversations and pooling of knowledge between the Cyber Centre and House of Commons IT staff, House of Commons IT staff were able to identify the names of the Parliamentarians who had been targeted. Ms. Xavier said that it is rare for the Cyber Centre to know the exact individuals targeted in a cyber attack. She could not say why the House of Commons IT staff did not advise the Parliamentarians that they had been targeted. However, the risk was mitigated.

[33] Mr. Khoury explained that the nature of this campaign was to email the Parliamentarians and send them a link that was meant to exploit some vulnerability. House of Commons IT staff were able to delete the tracking emails from the users' inboxes before they were accessed by most of the Parliamentarians. In other cases the tracking emails were caught by a firewall, mitigating the threat.

[34] Ms. Xavier was not able to speak to what, if anything, was done with respect to the tracking emails sent to the targeted Parliamentarians' personal (rather than House of Commons) email addresses. CSE is prohibited from directing operations toward Canadians and persons within Canada and is therefore unable to direct any of their capabilities toward a non-governmental email address. CSE can provide cyber advice and guidance to Canadians. It also has a Cyber Hotline for users to contact and report concerns and cyber incidents.

[35] Commission Counsel referred to a 2022 Cyber Centre update on PRC email operations against Canadians. The update assesses that APT 31 email operations almost certainly will continue to target Canadians, particularly those involved in Canada's foreign policy and political decision-making, at least over the coming year. Commission Counsel also referred to an email chain about APT 31 activity against IPAC. In the email chain, a CSE employee assesses that APT 31 was "almost certainly not attempting to *directly* interfere in democratic processes via cyber (unless 'interference' includes espionage)." The employee speculates that intelligence collected through this type of operation could be used to inform interference efforts.

[36] Ms. Xavier explained that politicians, voters, and electoral infrastructure are all targets of electoral interference by foreign state actors, which CSE has stated in its Threats to Democratic Processes reporting, even from the first published report. Information

operations could be one tactic used to advance these efforts. CSE views APT 31 as an actor that is more broadly pervasive and not focussed specifically on elections. APT 31's cyber threat activities are aimed more broadly at espionage and interference in general. It is difficult to say categorically whether this email operation was specifically intended to interfere in a democratic process.

[37] She added that Canada can be an unintended target because of its role in NATO or its proximity to the USA.

[38] Mr. Khoury testified that it is difficult to discern the intent of a threat actor at the cyber layer. A fraudulent email could be a means to secure a foothold on a network. Assessing intent requires an examination of technical information in tandem with context.

[39] Commission Counsel referred back to the email chain about APT 31 activity against IPAC. One of the emails describes reporting from a meeting between various national security bodies, the participants of which did not know if the relevant Parliamentarians had been briefed about APT 31 targeting of IPAC members.

[40] Ms. Xavier stated there have been conversations in general about the desire to brief Parliamentarians about information that concerns them. Briefings to Parliamentarians occur throughout the year. Ms. Xavier could not speak to whether the Parliamentarians targeted in the IPAC incident were briefed.

1.4.3 Ministerial Directive on Briefings to Parliamentarians

[41] Ms. Xavier testified that CSE views the APT 31 email operations against IPAC members as the type of activity intended to be captured by the Ministerial Direction to CSIS which directs that the Prime Minister, the Prime Minister's Office ("**PMO**"), and Ministers be proactively made aware of information related to national security threats to Parliamentarians and their families and that, wherever possible, the targeted Parliamentarians be informed of the threats.[4]

[4] See CAN027809. Note the referenced direction to CSIS was issued on May 16, 2023.

[42] Ms. Xavier noted that following the ministerial directive, she also issued a Chief Directive to CSE directing that all information concerning Parliamentarians should be flagged to get into the right hands at the right time to inform Government decision-making. If this kind of incident happened today, the ministerial direction to CSIS would likely apply and the Parliamentarians involved would likely have been briefed. CSE would not likely brief individuals directly, as CSE ordinarily provides classified information to cleared service providers or provides actions to take.. Briefings would likely come from the Canadian Security and Intelligence Service ("**CSIS**"), the Royal Canadian Mounted Police ("**RCMP**") or the Privy Council Office ("**PCO**").

1.4.4 Threats against Canadian Members of Parliament

[43] Commission Counsel referred to a 2023 document. Ms. Xavier confirmed that this information would be captured by the ministerial direction and the Chief's Directive. Ms. Tayyeb added that the Chief's Directive also requires CSE to immediately advise all responsible agencies of government, which was done in this case. The witnesses confirmed that the document went to hundreds of Canadian clients, including CSIS and the RCMP, and was flagged to PCO shortly after it was issued. Ms. Xavier clarified that CSE has no role in advising Parliamentarians directly of any threats. In general, CSE's role is to interact with systems and their service providers. If CSE collects information revealing a threat to Parliamentarians or has information about a cyber campaign targeting Parliamentarians, it ensures that this information is provided to the relevant officials, departments and/or agencies who can determine the appropriate response. For example, CSIS might want to conduct a threat reduction measure or seek a warrant, or the Royal Canadian Mounted Police ("**RCMP**") may want to investigate. Other agencies deal with domestic matters. CSE is prohibited from directing its actions toward Canada.

[44] Ms. Xavier stated that CSE would have advised CSIS, PCO, RCMP, and other partners of information, such as HoC Security Officials, related to threats against Parliamentarians, along with the reason why action is warranted. It would then be left to CSIS or the RCMP to determine next steps.

1.4.5 Progression in PRC's Cyber Capabilities

[45] The PRC's online foreign influence activity has become more sophisticated in recent years. At times, the PRC is successful in evading some social media platforms' mechanisms to spot fake content.

[46] Mr. Khoury stated that in his assessment, the PRC now exceeds Russia in terms of volume of cyber activity. Ms. Tayyeb noted that it is difficult to compare the two countries from a foreign interference perspective.

[47] Ms. Xavier testified that the PRC permeates multiple spaces, online and otherwise, where one might not necessarily expect, and described the PRC as having a "long game". Volume-wise, the PRC may exceed Russian's activities, but it is hard to quantify. The PRC is heavily involved in developing software, phone companies, and apps like TikTok.

[48] Ms. Tayyeb noted that the PRC responds to worldwide scrutiny because they value their reputation and seek to avoid embarrassment on the global stage. In recent years, there has been more publicity about the PRC's activity in Canada and other countries. As a result, the PRC has taken more steps to protect their activity from scrutiny.

1.5 Russia's Cyber Capabilities and Threat Activity

[49] Ms. Tayyeb explained that, in the past, Russia has not seemed to have the intent to directly interfere in Canadian elections. However, Russia does have a longstanding campaign to discredit the US and its allies, and western democracy in general. This impacts Canada and other allies. Ms. Tayyeb added that CSE has observed Russian cyber threat activity in Canada, but not directed against Canadian democratic institutions.

[50] Ms. Xavier added that CSE has learned about additional Russian tactics and techniques by observing the Russian invasion in Ukraine.

[51] Mr. Khoury added that the cyber landscape in Russia is broad and complex. Russia as a state is a threat actor, but there are also state affiliates, proxies, ransomware groups, and hacktivists that operate from Russia. Russia has very advanced cyber capabilities

of which Canada should be wary. For example, ten years ago, Russia took out the electricity grid in Ukraine.

1.6 India's Cyber Capabilities and Threat Activity

[52] Commission Counsel referred to a 2023 Cyber Centre report on spotting emerging state cyber threats. Commission Counsel also referred to a 2023 Cyber Centre threat brief on India. The threat brief assesses that India has a medium-sophistication national cyber program. Mr. Khoury agreed this assessment remains accurate.

[53] Ms. Xavier stated that CSE recognizes India as a state aspiring to build a modernized cyber program. For example, when the Prime Minister discussed the killing of Mr. Hardeep Singh Nijjar, or when the Prime Minister visited India, CSE noted mis- and disinformation ("**MIDI**"). CSE is aware that India is trying to counter narratives against India and the Indian government.

[54] Ms. Tayyeb clarified that CSE is aware of activities directed by India in Canada. Canada is one of India's targets due to Canada's large Indian diaspora community.

1.7 Sharing Foreign Intelligence

[55] Ms. Tayyeb stated that intelligence collected pursuant to the foreign intelligence aspect of CSE's mandate must be provided to the Government of Canada. The *CSE Act* does not provide a mechanism for CSE to advise Canadians directly about specific intelligence it collects, however CSE uses mechanisms such as the Annual Public Report and other public documents to provide assessments and advisories that are derived from intelligence reporting, cyber defence activities, and research.

[56] Only specific individuals with a mandate to take action would receive suppressed Canadian identities. Individuals can request the list through a specific process. Those requesting the list must justify why they are requesting it, and must demonstrate their legal authority to receive it. Ms. Xavier added that these requests are sometimes denied.

1.8 SIGINT Products

[57] Commission Counsel referred to a CSE document entitled "2021 – 2023 END Cycle Update Tasking Response that describes a new line of reporting called Tailored Intelligence Products ("**TIPs**").

[58] Ms. Tayyeb explained that CSE is always trying to render their intelligence products more accessible to clients, to tailor their products to intelligence requirements, and to incorporate feedback from clients.

1.9 Tools to Combat FI and Cyber Incidents

1.9.1 Combatting MIDI in Domestic Environments

[59] Commission Counsel referred to an email exchange about CSE's work with MIDI. One of the emails states that research into disinformation campaigns, and specifically the development of tools and techniques to detect them, has been limited due to real or perceived concerns with mandate alignment. Disinformation campaigns are generally not characterized as "cyber security" activities. As a result, malicious influence campaigns directed at Canadians and implemented on social networks used by Canadians has been considered "out-of-scope."

[60] Ms. Xavier reiterated that CSE cannot direct its apparatus toward Canadians or towards persons within Canada. CSE works hard to abide by this restriction and to avoid unintentionally capturing Canadian data. Because CSE cannot direct its apparatus toward Canadians, it is not best-placed to monitor for and dispel MIDI in domestic environments. Instead, CSE can advise on MIDI, educate Canadians on the MIDI threat, and lead educational efforts on encouraging critical thinking when digesting online information. This connects to s. 17 of the *CSE Act*, which sets out the cybersecurity and information assurance aspect of CSE's mandate. Ms. Xavier expressed that Canadian intelligence agencies should not direct their apparatus against Canadians lawfully expressing views or opinions. Canadians enjoy a *Charter*-protected right to freedom of expression. Ms. Xavier commented that there may be value in having a third party or non-governmental organization identify and correct MIDI.

[61] Ms. Xavier testified that CSE can play a role in the technical attribution of online MIDI, especially where technical identification is needed to find the originating elements of a malicious actor. However, it can only do so where there is some indication the source of the MIDI is foreign in nature.

[62] Ms. Tayyeb added that CSE could be called upon to clarify the source if it became aware that a foreign actor was engaging in MIDI. If the origin is domestic, however, CSE will not know about it unless there is foreign intelligence surrounding the MIDI. CSE cannot investigate a domestic lead because that would require CSE to direct its efforts against a Canadian. If there was a suspicion that a foreign state was involved, CSE could only look at foreign signals intelligence to see if it could confirm or disprove the suspicion, and could not take action against the Canadian.

[63] Ms. Xavier noted that CSE is also able to provide technical assistance through its assistance mandate. When CSE's assistance mandate is engaged, CSE can offer assistance under the mandate and authorities of the requesting agency. Following the examination, in response to an undertaking, CSE advised that it has not received any requests for assistance under their s.20 assistance mandate for technical attribution of a MIDI campaign in the context of General Election or democratic processes more broadly.

1.9.2 CSE's Cyber Operation Program

[64] Commission Counsel referred to an undated document summarizing CSE's cyber operation program. The document states that Canada has an advantage with world-class cyber operators, but that "our allies and adversaries are quickly outpacing us both in scope and in scale."

[65] Ms. Xavier explained that Budget 2024 allocated almost $1B to CSE over the next five years, part of which was to go to foreign intelligence, and another part to foreign cyber operations. In part, this allocation of funds was in recognition of the fact that CSE's new authorities required a commensurate increase in resources.

1.9.3 Email Operations

[66] Mr. Khoury clarified that in relation to email operations, clicking the link within an email will let an adversary into the email server. However, sometimes a system has vulnerabilities where simply loading the email allows an entry (this is called a zero-click vulnerability). Zero-click vulnerabilities can manifest through malicious emails or text messages. Receipt alone can create a vulnerability, depending on the platform and the nature of the attack. Speed is of the essence when fixing these issues.

[67] Ms. Xavier explained that CSE tries to find ways to protect against these malicious actors. CSE deploys sensors on government systems that prevent malicious messages from ever reaching the user. This is why multiple layers of cyber security are important.

1.10 Outreach to the Public

1.10.1 Outreach to Political Parties

[68] Commission Counsel referred to an email exchange about the Cyber Hotline. The email details that only one issue was reported to the Hotline during the GE43 election period. No issues were reported to the Hotline during the GE44 election period. The Cyber Centre did not solicit feedback from political parties on the Hotline service.

[69] In response to a Commission question on the subject, Ms. Xavier stated that she did not know why there wasn't more uptake of the Cyber Hotline. She explained that although CSE shared the Hotline with members of political parties and ministers, in 2019 the Hotline was novel. The Hotline was better known in 2021, but people were more cyber aware and practicing better cyber hygiene. She speculated that people running into cyber issues may have been mitigating issues themselves or may have reached out directly to software platforms or social media platforms.

[70] Ms. Xavier could not explain why CSE did not solicit feedback from political parties, and suggested this was something to pay more attention to in advance of the next election. She added that the Hotline is available outside of elections periods and has been used in between elections. CSE has received calls in between elections.

[71] Ms. Xavier testified that the Hotline has not been made available to candidates in provincials and territorial elections. CSE and the Cyber Centre have undertaken other initiatives to facilitate direct communication with provinces and territories. For example, the Cyber Centre has conducted numerous meetings with the provinces and territories on elections.

1.10.2 Outreach to the General Public

[72] Ms. Xavier explained that CSE publishes public reports aimed at all of civil society. CSE tries to make these reports as accessible as possible, but the primary objective is to help those who work in the information systems field to make sure they are practicing basic hygiene and building cyber resilience in the cyber domain. CSE's audience evolves as the threat landscape evolves.

[73] Mr. Khoury explained that CSE has also redesigned its website based on public feedback to make it more accessible to the public. In addition, CSE has undertaken a public awareness campaign called "Get Cyber Safe," meant to speak to Canadians in a way that is not technical. CSE runs other campaigns as well, and collects data on engagement and success for each campaign. Ms. Xavier explained that recent data on a MIDI-awareness campaign showed that the campaign was very successful.

[74] Commission Counsel referred to a document that details the various roles CSE could play in the Plan to Protect Democracy, and details a number of proposals on outreach to political parties and the public. For example, one proposal suggests CSE could translate its public outreach materials into the most spoken languages in Canada, including Mandarin, Punjabi, Cantonese, Spanish, and Arabic, among others.

[75] Ms. Xavier explained that this document was written by someone on a more operational level. It collects suggestions from employees on things that CSE could do to better protect Canada's democracy. Some of the ideas have already been actioned, or are things CSE hopes to improve on. For example, CSE conducted outreach to journalists and held a "cybersecurity 101" session. CSE has also translated advice into Indigenous languages to inform Indigenous communities about cyber threats. Ms. Xavier has opined that CSE could do more, and will continue to action improvements.

2. Examination by the Attorney General of Canada

[76] Ms. Tayyeb explained that under the foreign intelligence aspect of CSE's mandate, CSE provides information to government agencies. Mr. Khoury added that under the cybersecurity and information assurance aspect of CSE's mandate, CSE provides cybersecurity support to federal systems or other systems designated as being of importance to the Government of Canada. Provincial and territorial government systems are designated as being of importance, which enables CSE to support them when it comes to cyber security.

[77] Ms. Tayyeb compared and contrasted the ease of attribution of cyber incidents and MIDI campaigns. When it comes to attributing a cyber incident or activity, CSE is able to consult foreign intelligence and obtain technical details of the compromise. This foreign intelligence and technical information can be compared to CSE's knowledge of different foreign actors to assist in attribution. When it comes to MIDI, CSE is generally not able to get technical information to make the attribution because it doesn't exist, or has not been provided from a social media platform. If a foreign actor uses proxies in Canada to spread MIDI, that can further obfuscate CSE's ability to attribute the campaign.

[78] Ms. Xavier confirmed that CSE's primary role is in technical attribution. Even if CSE cannot identify an actor from a technical perspective, it can still put out an alert, or guidance or advice, to tell clients about the indicators of a compromise.