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: Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald

Commission Counsel examined senior officials from the Privy Council Office ("PCO") Security & Intelligence Secretariat ("**S&I**") 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 witnesses. 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] The witnesses confirmed the accuracy of the summary of their interview and adopted its content as part of their evidence before the Commission.

1.1 Witnesses

[2] Nabih Eldebs is Assistant Secretary to the Cabinet, S&I, and has held this role since December 2023. Within his purview, there are four different branches of S&I:

a) The Operations branch, headed by the Director of Operations Bridget Walshe, looks at all operational issues relating to security and intelligence in Canada, including elections security and cyber security, and liaises with the Prime Minister's Office ("**PMO**") on all such issues as they arise on a daily basis.

b) The Strategic Policy and Planning branch, headed by the Director of Strategic Policy and Planning Adelle Ferguson, looks at policy development within the federal government with respect to security and intelligence and the national security community. This includes things like bill C-70.

c) The Review Coordination Unit, [headed by a Director not on the panel] liaises with the National Security and Intelligence Review Agency ("**NSIRA**"), and the National Security and Intelligence Committee of Parliamentarians ("**NSICOP**").

d) The Security Operations Directorate ("**SECOPS**"), [headed by a Director not on the panel] is responsible for the physical security operations within PCO, as well as background checks and security clearances for all Governor-in-Council appointments.

[3] Michael MacDonald served as Assistant Secretary to the Cabinet, S&I, from May 2020 to June 2023. He now serves as Senior Assistant Deputy Minister at the Treasury Board of Canada Secretariat. There, he is overseeing an effort to modernize the security suite of Canada's public service (i.e. departmental security).

[4] Marie-Hélène Chayer was interviewed in her capacity as former Acting Assistant Secretary, S&I. She held this role from June to October 2023. Before this role, she led PCO's Task Force on Foreign Interference (from January to June 2023). She currently serves as Assistant Secretary to the Cabinet, for the National Security Council ("**NSC**") Secretariat, a role she has held since October 2023. As of July 8, 2023, the NSC Secretariat merged with the Intelligence Assessment Secretariat ("**IAS**"). Ms. Chayer now leads both.

1.2 Role and Functions of S&I

[5] The witnesses agreed that a portion of S&I's functions include:

a) Providing policy advice and support to the National Security and Intelligence Advisor to the Prime Minister ("**NSIA**") via the Deputy NSIA;

b) Performing a convening function across the security and intelligence community, which includes participating in and/or serving as secretariat for various national

security committees, such as the Deputy Minister Committee on Intelligence Response ("**DMCIR**"), the Assistant Deputy Minister National Security Operations Committee ("**ADM NS OPS**"), and the Assistant Deputy Minister National Security Operations Committee - Tactical ("**ADM NS Tactical**"); and

c) Helping to coordinate the process by which the Government of Canada's Intelligence Priorities are set.

[6] Mr. Eldebs noted that the intelligence priorities are but one of the files that are handled by the Strategic Policy and Planning branch and that there are a number of other issues on which S&I provides advice and policy development within the national security community.

1.3 National Security Council Secretariat

[7] Ms. Chayer testified that the NSC is a Cabinet committee chaired by the Prime Minister. The NSC sets strategic direction based on strategic advice regarding national security issues. The NSC is a forum through which the Prime Minister engages with Ministers on national security matters. The Deputy Ministers and agency heads supporting Council members also participate in the NSC.

[8] Ms. Chayer's secretariat supports the NSC's meetings. The Secretary of the NSC is the Deputy Clerk and NSIA, Nathalie Drouin. Ms. Chayer's work supports Ms. Drouin through development and the coordination of the policy advice and supporting intelligence documents to be presented to the committee, and the articulation of next steps following NSC meetings, including action items assigned to departments and agencies.

1.4 Policy Landscape

[9] Commission Counsel identified three items described by Counsel as the core of the Government of Canada's policy toolkit in responding to foreign interference:

a) Canada's Plan to Protect Democracy;

b) The Hostile Activities by State Actors ("**HASA**") strategy;

c) The Intelligence Priorities, and flowing from that, strategic guidance, Ministerial Directions and departmental requirements that tell agencies and departments how to implement the Priorities.

[10] The witnesses were asked if there was anything they wanted to add.

[11] Mr. Eldebs testified that there are a number of other Government of Canada policies and strategies that the government operates under in relation to FI. Mr. Eldebs clarified that the Intelligence Priorities are not a strategy, but rather, a process and a focus point for the national security community. He noted that certain departments must follow the Intelligence Priorities by law. He explained that the policies and strategies that govern the activities of government vary by department and can change over time. He gave several examples, including a cyber-security strategy, an Indo-Pacific strategy, and an advanced policy that guides the work of the Department of National Defence. He indicated that he could name others, but turned to his colleagues for their input.

[12] Ms. Walshe testified that the strategies and laws that govern Canada's response to FI have evolved over time. For example, there were legislative updates in 2015 and 2019 that updated the toolkit that was available both to obtain intelligence relating to foreign interference and to respond. For example, there have been updates to the statutes that govern the Communications Security Establishment ("**CSE**") and the Canadian Security and Intelligence Service ("**CSIS**") that evolved the toolkit.

1.5 A Common Understanding of FI

[13] Commission Counsel referred to the NSICOP Special Report on Foreign Interference in Canada's Democratic Processes and Institutions, which states its view that there is a lack of common understanding of FI threats across Canada's security and intelligence community, including a lack of understanding of what action should be taken.[1] Commission counsel noted that the witnesses did not agree with that characterization in their interviews. Commission Counsel asked the Panel what is being done to ensure the

[1] NSICOP, "Special Report on Foreign Interference in Canada's Democratic Processes and Institutions" (2024) at para. 146.

security and intelligence community can arrive at a common understanding of the threat, recognizing that there are different perspectives on the issue.

[14] Mr. Eldebs testified that the structures that have been set up within the Government of Canada to respond to FI, and to promote a common understanding of FI, are robust. He expressed that the process for handling FI activities are in a mature place.

[15] Mr. Eldebs explained that generally, any intelligence relating to FI will be discussed at an Assistant Deputy Minister ("**ADM**") level first. For example, ADM Tactical often reviews the intelligence, discusses the threat, and comes to a common understanding of the threat and what to do about it. The intelligence, along with the views and recommendations of ADM Tactical, then goes to DMCIR for consideration by Deputy Ministers ("**DMs**") who will have their own conversation.

[16] Mr. Eldebs cautioned that there will always be "gray space" in this area because the line between foreign interference and foreign influence and/or ordinary diplomatic activity is not a clear cut line. He explained that debate on this issue is healthy. Global Affairs Canada ("**GAC**") brings a very unique perspective to the table because they have Canadian diplomats abroad in foreign countries who are talking to people, lobbying on behalf of Canada, and trying to convince people of Canada's point of view, and it is important to understand how diplomats are supposed to work. In Mr. Eldeb's view, the line becomes fuzzy when there is a departure from normal diplomatic activity and when it either starts to stray into something different or something covert. Discussion helps to better understand the problem and better equip the Government to come up with operational and policy solutions that make sense for Canada.

[17] Mr. MacDonald expressed that guidance from the Commission on how governments and the public can deal with the "grey zone" between FI and legitimate diplomatic activity, and further policy development on this issue, would be helpful.

[18] Ms. Walshe testified that from an operational perspective, the committees are well-supported through coordinated, institutionalized decision-making processes. When a matter goes to ADM Tactical or DMCIR, there is a package assembled that puts both the intelligence and proposed response together to facilitate an informed discussion. These processes are meant to ensure consistency in decision-making, particularly

where there are questions about the intelligence or where the activities fall within the grey zone.

1.6 Intelligence Priorities

[19] Mr. Eldebs testified that the Government of Canada's Intelligence Priorities ("**Priorities**") are developed through consultation with departments across the Government of Canada, and set every two years. There is also a mid-year update to Cabinet to showcase how the community has been implementing the Priorities. The Priorities are not ranked in order of importance. This allows for flexibility in the work of departments and agencies. The Intelligence Requirements ("**Requirements**") that sit underneath the Priorities are much more detailed and set out the specific aspects of what each department can do or the intelligence sought in respect of the Priorities. The Requirements are ranked into tiers, and can shift over time. Authority over the Requirements resides with departments.

[20] Ms. Ferguson, whose branch is responsible for coordinating the process for setting the Priorities and Requirements, testified that it is helpful to think of the Priorities as a framework that guides the work of the security and intelligence community. They identify areas of strategic interest to the Government of Canada over a two-year horizon where intelligence support will be needed to advance Canada's interests. The Priorities are developed by drawing on the national security and intelligence community as well as other Government of Canada departments and agencies. Sources that inform the process are varied and include the federal budget, mandate letters, and departmental priorities. That information is then matched up with what the intelligence collection agencies are able to support in terms of both capabilities and resources in order to formulate the Priorities.

[21] Ms. Ferguson testified that once Cabinet approves the Priorities they are disseminated to the security and intelligence community. From there, S&I leads the process to develop the Requirements. The Requirements are more granular and focus on very specific questions that intelligence consumers need answered in order to support their work. The Requirements are tiered from Tier 1 (the highest) to Tier 4 (the lowest) and

are evergreen in that they can evolve to react to the threat environment, changes to government priorities, or outside events. S&I may convene the community to discuss the Requirements if they need to be adjusted for any reason, or this process can be initiated by another department. This can happen very quickly (i.e. in the space of a day). There is also a deliberate auditing process at specified intervals to make sure that the Requirements continue to serve the needs of consumers.

[22] Mr. MacDonald testified that the Five Eyes allies each likewise set intelligence priorities following similar processes. Through bodies like the Five Eyes Policy Forum, which S&I participates in, the alliance shares intelligence priorities with each other. This both gives Canada and its partners a broader look at the threats and risks they collectively face, and also presents an opportunity to close any gaps by helping each other fulfill their respective priorities.

[23] Commission Counsel referred to a document entitled Canadian Intelligence Priorities Strategic Guidance. Ms. Ferguson testified that S&I drafts the guidance document, which is ultimately approved by Cabinet. This document is the vehicle by which the Cabinet-approved Priorities are disseminated to the departments.

1.7 Types of Intelligence and Intelligence Dissemination

[24] Mr. Eldebs testified that the intelligence that S&I looks at on a daily basis is mainly discrete pieces of intelligence, i.e. reports produced by departments such as CSIS, CSE and our Five Eyes allies. These pieces of intelligence relay a specific intelligence development. In contrast, IAS (and certain other Government of Canada partners) produces assessed products that amalgamate intelligence reports and other sources of information provide an assessment of that intelligence. An assessment is generally a projection and expression of probabilities to try to provide guidance for the future of an issue. Assessments take more time to develop and produce.

[25] Mr. Eldebs stated that since he joined S&I, much of the reporting that S&I receives is circulated through electronic tools owned by the Government of Canada. These tools automatically record when a user has opened a document or report. Mr. Eldebs explained that not all government departments have access to the tools that track

readership automatically, for example, the PMO. For those clients, reports can be printed and readership marked manually.

[26] Ms. Walshe added that S&I is not the primary mechanism used by PMO to receive intelligence. However, S&I will share intelligence with PMO where there is an operational priority or reason to share information urgently.

[27] Ms. Chayer added that when she began acting as Assistant Secretary of S&I in June 2023, S&I had a tracking system in place. Over the course of her tenure, S&I worked with several other departments, including CSE, CSIS and GAC, to develop strategic guidance on how to better track intelligence going forward. Today, each of these organizations relies on electronic methods to distribute and track intelligence. Her team also sought to implement more systematic methods to track verbal briefings throughout the intelligence community. For each briefing, agencies would track the date, who was there, and what was discussed. She underscored that efforts to track the dissemination of intelligence are not new; new measures come in addition to those that already tracked the dissemination of intelligence.

1.8 Briefings to Parliamentarians and Political Party Leaders

[28] Mr. Eldebs explained that SECOPS provides general security briefings to Parliamentarians, new Ministers, and their staff. The briefings are meant to bring these individuals up to speed on the threat landscape, including FI. Recently, they have started to provide “refresher” briefings to Ministers’ offices. The CSE and CSIS also participate in these briefings.

[29] Commission Counsel referred to an email chain from April 2024 that stated that PCO was facilitating security clearances to opposition party leaders and had developed a protocol for providing them with briefings.[2]

[30] Mr. Eldebs testified that the process for obtaining clearances for opposition party leaders started before April 2024, though only two opposition party leaders took up this offer. SECOPs conducts the security clearance process, however the briefings

[2] CAN035671.

themselves are coordinated through the NSIA's and Deputy NSIA's office. This involves putting together a specific package of intelligence for opposition party leaders to read, based on both general issues about the security situation and what they specifically need to know. Opposition party leaders are then provided the opportunity to ask questions. Jagmeet Singh and Elizabeth May are the only two opposition party leaders that have received this briefing.

[31] Ms. Walshe stated that PCO first offered security clearances to opposition party leaders to allow them to read the classified annex to the report of the Independent Special Rapporteur of Foreign Interference when it was released.

[32] Mr. Eldebs testified that PCO has renewed its offer to remaining opposition party leaders to obtain security clearances. He is not certain why the offer has not been accepted by all leaders, as no reason was provided.

1.9 Briefings Concerning Threats to Parliamentarians

[33] Commission Counsel referred to a Governance Protocol for Threat Disclosures to Parliamentarians. Commission Counsel also referred to a 2023 email to Ms. Chayer from a CSIS employee related to a draft of the protocol, and a 2023 email chain that includes Ms. Chayer on emails relating to a pre-briefing process on the protocol. In the email chain, Ms. Chayer invites her colleague to "dig a bit deeper into the concept of 'threat' and what actually constitutes a credible threat."

[34] Commission counsel asked Ms. Chayer to explain her comment about what constitutes a credible threat.

[35] Ms. Chayer explained that the process through which CSIS shares intelligence has evolved significantly. The correspondence referred to by Commission Counsel reflects early conversations with CSIS about how to share intelligence, when to do so, and what kind of script would be used to protect sources and methods. Ms. Chayer wanted to put herself in the shoes of the politicians being briefed to ensure the briefings were tailored to achieve their purpose and to be as helpful to the recipient as possible. She noted that there was coordination amongst all relevant departments to develop the right content,

and that any proposed engagement goes through a robust committee process to refine the briefing.

[36] Mr. Eldebs agreed that there are now robust processes in place. He cautioned that intelligence is often a snapshot in time that tells only part of a story. He also noted that some intelligence comes from credible sources and some does not. It is important to look at intelligence from an objective perspective and understand its weight, noting that government action needs to be based on credible intelligence and a full picture. For these reasons, before any action is taken on a piece of intelligence, the intelligence is usually reviewed first at an ADM committee and then at a DM committee so that senior officials can discuss the intelligence and ask these and other questions.

[37] When asked who would have the final say in case of disagreement among senior officials, Mr. Eldebs stated that the ADMs generally come to a consensus and that he has not seen disagreement. He speculated that if there was ever a disagreement among ADMs as to the best course of action, both perspectives and ideas would be brought to the DM committee for their consideration. He added that bringing multiple viewpoints to a DM committee would be positive because it leads to the kind of healthy debate that must happen. He noted that Global Affairs can give a good indication of whether the activities of a diplomat have crossed the line, and CSIS can do the same with the activities of foreign intelligence officers.

[38] Ms. Walshe added that in the process of operationalizing intelligence, instead of disagreement amongst officials, S&I is rather seeing debate resulting in an adaptation of the response, e.g., a refining of the language to be used to brief someone in a Threat Reduction Measure ("**TRM**"). In her view, debate results in an improved briefing.

1.10 Parliamentarians

[39] Commission Counsel referred to a draft memorandum for the Prime Minister providing an update on Member of Parliament Han Dong. Ms. Chayer testified that the attachments to the draft memorandum had been shared with the NSIA. The other witnesses do not recall any other updates on Mr. Dong.

[40] Commission Counsel also referred to an email summarizing certain intelligence and government actions relating to the interactions between another MP and a foreign official. In the email, CSIS expressed the view that a TRM should not be pursued. Commission Counsel also referred to another email from Mr. Eldebs indicating further actions that were considered at the time. Ultimately, alternative actions were implemented.

[41] Ms. Walshe added that there are very specific governance mechanisms that control when CSIS can use a TRM within their mandate.

[42] Mr. MacDonald testified that CSIS TRMs are not the only way to address intelligence. CSIS TRMs carry a certain weight because of the seriousness that most people perceive when speaking with CSIS. However, PCO can also have conversations with Parliamentarians about foreign interference and these conversations may be received by the Parliamentarian differently. Mr. MacDonald emphasized that officials use the most appropriate strategy for any given situation, taking into consideration the impact that the strategy is likely to have.

[43] Ms. Walshe added that another important impact that officials consider in deciding the most appropriate and effective measure is the inherent risk in disclosing classified information (which is a typical use of a TRM).

[44] Mr. Eldebs was asked, how the intelligence community can tell if a person's actions are malign as opposed to well-intentioned if naïve or ill-advised. Mr. Eldebs expressed that it was hard to determine a person's intent from their reported activities. Intelligence provides a snapshot in time, but it does not get into intent unless a person states their intention. In this case, he also noted that there are gaps in the intelligence in relation to this individual. As a result, the intelligence community has to make assumptions, which is difficult.

[45] Mr. Eldebs confirmed that he has not seen or heard of any further activity of concern from this individual.

1.11 Sharing Intelligence with Provinces and Territories

[46] Commission Counsel referred to an undated document concerning a briefing for British Columbia Premier Eby.[3] The witnesses were referred to a bullet which indicated that provincial and territorial architecture is not well set up. Ms. Walshe recalled that this document was an early draft produced by an analyst informally looking at some of the issues associated with engaging the province of British Columbia on intelligence. She indicated that she would have asked an analyst for considerations for further engagement. Reading the document. Ms. Walshe surmised that at that point in time, PCO did not know much about the particular architecture the province had in place to receive intelligence or have classified discussions.

[47] The Commission asked why the document was not dated. Mr. Eldebs explained that draft documents and notes are not often dated. Drafts are usually kept in electronic form on PCO's system, which records the date electronically. A date is stamped onto the physical document itself whenever it is approved and transmitted in final form. Ms. Walshe added that the process Mr. Eldebs outlined relates to formal briefing notes. For documents recording informal thoughts that are not meant to go up to senior officials, they are not stamped.

[48] Commission Counsel referred to a memorandum for the Prime Minister recommending responses to a letter from the Premier of the Yukon regarding sharing intelligence with provinces and territories.[4] Commission counsel asked the panel provide an update on the work that has been done to liaise and share intelligence with provinces and territories.

[49] Mr. Eldebs testified that there is an ADM-level Federal-Provincial-Territorial national security table that S&I is working with Public Safety to reinvigorate, where officials from all provinces and territories can discuss national security issues. The most recent meeting (as of the date of this testimony) was held in the Spring of 2024, though not all provinces and territories attended that meeting. Mr. Eldebs has engaged with PCO Intergovernmental Affairs to have provinces identify appropriate national security points

[3] CAN037897.
[4] CAN033297.

of contact for every province and territory. He has engaged with these points of contact and set up bilateral meetings to introduce himself and to ensure that the federal government is engaging with provinces and territories on issues that they are interested in.

[50] Mr. Eldebs added that the Clerk of the Privy Council has met with the clerks of all the provinces and territories. Last week (July 2024), the Clerk met with provincial and territorial clerks to discuss Bill C-70 and FI in general. PCO is also working to help the provinces and territories set up the secure systems necessary to have more discussions at the classified level.

[51] Mr. Eldebs was asked about a prior comment he made to the effect that not all provinces and territories had the right infrastructure. Mr. Eldebs stated that he has seen a change, and all of the provinces and territories are involved and eager to engage with the federal government on national security issues. Mr. Eldebs acknowledged that provinces have different technological systems and infrastructure, but that is why PCO is working to set up a common secure communications method.

1.12 Governance Structure

[52] Commission Counsel referred to a presentation on proposals to streamline Canada's national security and intelligence governance structure and reduce the number of committees.[5] Noting her understanding that nothing has been finally agreed, Commission Counsel asked the panel to explain what the new format may look like and when they expected it to be implemented.

[53] Mr. Eldebs explained that the consultations to date have landed more or less on a structure comprised of 4 DM-level committees: (1) a policy committee for foreign and global affairs where topics related to foreign policy and military defense will be discussed; (2) a national security and intelligence operations committee, which he noted is already, in practice, a working committee in the form of DMCIR. He noted that DMCIR discusses intelligence and decision-making in response to intelligence and that it works extremely well; (3) a national security intelligence policy committee. Mr. Eldebs noted

[5] CAN037056.

that this committee, as its name suggests, will discuss policy issues, fulfilling the same function as the current DM National Security committee; and (4) an intelligence coordination committee that will handle operational issues, a role currently fulfilled by DMOC. Mr. Eldebs reaffirmed that, other than the foreign affairs committee, the structure discussed in the deck is more or less in place already and the committees were meeting on a regular basis. Through that process, the names of the current committees may or may not change. There is a meeting planned for the end of July at which the new structure would be discussed again.

[54] Ms. Chayer noted that the national security and intelligence governance structure is always evolving. She explained that just because the structure is being reviewed, it does not follow that it was broken. The committees currently in place function well. As the threat or context evolves, the governance structure must change to adapt to that context. This review is another normal evolution of the structure to optimize and adapt to current circumstances.

1.13 Process for Monitoring By-Elections

[55] Commission Counsel asked the witnesses to explain how decisions are made in respect of intelligence during by-elections and, in particular, what happens to the daily reporting, called SITREPs, prepared by the Security and Intelligence Threats to Elections Task Force ("**SITE TF**") when they are received by DMCIR.

[56] Mr. Eldebs testified that in addition to DMCIR, SITREPs regarding by-elections will go to an ADM-level committee that he co-chairs with Elections Canada, called ADM Elections Security, which meets on a weekly basis during by-elections. SITE TF gives status updates to both ADM Elections Security and DMCIR.

[57] The witnesses testified that there have been seven by-elections since June 2023 and no significant instances of FI have been reported in any of them.

[58] Generally speaking, if there is any issue, ADM Elections Security would discuss it and consider options to be presented to DMCIR. Mr. Eldebs added that the advantage of the SITE TF is not only that it brings together the expertise of the constituent member

departments, but also that SITE TF members can brief up relevant intelligence within their own departments and agencies, allowing things to move quickly.

[59] As with any piece of intelligence, every department and agency at DMCIR has their own authorities. They bring to DMCIR options based on what their department can do, and from there, decisions are made for the best course of action.

[60] Ms. Walshe added that ADM Tactical also plays a role in this process. Though ADM Tactical has a body of core members, it can invite other members to the table to enrich discussion and recommendations on specialized issues (e.g., if the issue is cyber-related, they can bring in individuals with cyber expertise). ADM Tactical tries to understand intelligence and can look at options so that when it reaches DMCIR, those options can be presented. She noted that agencies also have independent discussions on intelligence internally which they will brief to their DMs to bring to DMCIR.

[61] Commission counsel asked the panel if there would ever be a circumstance that would require a decision at the ministerial level, noting that the Panel of Five does not operate during by-elections. Mr. Eldebs and Ms. Walshe indicated that most cases would not require ministerial approval, though certain TRMs and cyber actions do. Mr. Eldebs and Ms. Walshe explained that as non-partisan public servants, their advice to Ministers in that hypothetical scenario would be non-partisan.

1.14 Counter Foreign Interference Coordinator (“CFIC”)

[62] The witnesses were asked how they saw the role of the CFIC working alongside the role of S&I. Mr. Eldebs testified that the CFIC looks at a number of things to help the government counter foreign interference. For example, at present, the CFIC is engaging with diaspora communities to understand the types of influence they encounter. That is a critical role as it brings important knowledge to the table and informs the toolkit. This will help ensure the Government of Canada’s approach to FI remains responsive to the needs of Canadians. Mr. Eldebs described the CFIC as a critical partner of S&I.

1.15 Open-Source Intelligence ("OSINT")

[63] [Open-source intelligence, or OSINT, generally refers to information and data that is unclassified.]

[64] Mr. Eldebs disagreed that Canada's OSINT strategy was a "gap". Mr. Eldebs explained that many departments and agencies in the Government of Canada currently use OSINT within their authorities and in furtherance of their mandates. He explained that it is very important to these departments and agencies to ensure that their use of OSINT complies both with privacy legislation and with evolving societal norms with respect to an individual's privacy online.

[65] In relation to work that is currently being done and the conversations that are underway, Mr. Eldebs spoke about the challenges in balancing the use of OSINT for national security reasons against a citizen's legitimate right and expectation that governments will not harvest their online data *en masse* or for no reason. Mr. Eldebs noted that the term OSINT is quite broad, and would include information posted to the dark web that may have been hacked or stolen by bad actors - the use of which carries further legal and ethical considerations. Other OSINT is information posted by Canadians online about their lives, which does not in and of itself mean that Canadians are comfortable with their government harvesting it for analysis. Separately, collecting Canadians' data necessitates the ability to protect that stored data from others.

[66] Mr. Eldebs expressed that this is an evolving space and one in which departments are rightfully proceeding with caution, given the privacy issues at stake. Mr. Eldebs suggested that guidance on this balancing exercise would be helpful.

1.16 Declassification

[67] [Some countries have protocols with respect to declassification, meaning that once a document is 20 or 25 years old, a process is triggered to determine whether the document still needs to have the same security classification. Canada does not have an official protocol in place to declassify historical documents.]

[68] Mr. Eldebs disagreed that the lack of a declassification protocol represented a "gap" in Canada's ability to combat FI. Mr. Eldebs explained that "declassification" refers to downgrading or removing security classification from *historical* documents whose disclosure no longer poses a national security risk because their content is outdated. The goal of a declassification policy is to increase transparency around historical records and reduce the workload associated with responding to ATIP requests. It does not relate to sharing or acting on *current* intelligence or responding to current threats [because the documents are historical and outdated].

[69] This may be contrasted with "sanitization", which is the process of redacting or summarizing classified documents to reduce the classification level so that information can be shared more broadly and used. Mr. Eldebs noted that Bill C-70 broadened CSIS's ability to share information, beyond their pre-existing TRM mandate, which filled a gap. He also noted that CSE has the ability to sanitize their information for public use. He does not perceive a current gap in terms of the government's ability to sanitize and use intelligence.

2. Examination by the Attorney General of Canada

2.1 Social Media, AI and Emerging Technology

[70] Counsel for the Attorney General of Canada took the witnesses to an intelligence memorandum prepared by IAS entitled "Mobilizing Disinformation in a Public Discourse War with the West" which stated that the CPC is targeting younger demographics as part of a long-term strategy to influence future leaders in western countries, including Canada. The memo stated that the CPC's future disinformation and propaganda efforts would have the greatest impact on teens and young adults, noting the reliance by youth on TikTok as their primary source of 'unbiased news'.

[71] Mr. Eldebs observed that the method by which FI occurs is evolving, and it is proliferating through social media. Mr. Eldebs noted that a hefty percentage of Canadians are on TikTok, and it is easier for China to reach Canadians through a series of 10 second videos than through articles in traditional media. Proliferation of social

media platforms has influenced how adversaries shape the information environment, and how they engage with youth. Tools like TikTok, for example, are ripe ground for targeting Canada's youth, especially because TikTok content is moderated and influenced by China. The security and intelligence community is aware of this threat.

[72] Mr. Eldebs opined that the answer to this threat is education. On that front, he described a multi-faceted approach from the federal government, highlighting that this is why the work of Heritage Canada as well as the Plan to Protect Democracy put out by the Democratic Institutions Secretariat at PCO are both extremely important. However, Mr. Eldebs underscored that the solution must be a whole-of-society approach, which is why engagement with diaspora communities, engagement with provinces and territories and the involvement of our education systems are also important.

[73] Ms. Chayer emphasized that the ability for threat actors to push messaging on social media is very broad. For that reason, there is a need to increase resilience of communities and societies to online threats, and to make Canadians aware of the threats that exist, including efforts to influence their views on specific issues.

[74] Counsel for the Attorney General of Canada referred the panel to a document on artificial intelligence ("**AI**")[6] and emerging technology and asked the panel to speak to government efforts at home and abroad to ensure that AI is not misused in FI. Mr. Eldebs noted that AI is a tool that can be used to power the economy, education and the national security community. He testified that Canada is a leader in AI research and it is important that Canada plays a leadership role in AI governance internationally.

[75] Mr. Eldebs described four buckets of work that Canada is pursuing on this front: (1) work to ensure that AI is ethical (e.g., non-discriminatory); (2) work to ensure AI safety through investment in research and local capabilities to build a secure technological framework; (3) work to develop a set of international norms governing AI use (similar to the international cyber security norms that have been developed); and (4) work to detect and defend against the malign use of AI.

[6] CAN032039.

[76] Mr. Eldebs explained that international norms are a critical first step to defending against the malign use of AI. International norms define what is normal and acceptable behaviour (and what is not), which enables a country like Canada to call out unacceptable behaviour. Canada and like-minded countries are currently working to define international norms for AI use. These are things that Canada is championing in the international community.