Public Inquiry Into
Foreign Interference in
Federal Electoral Processes
and Democratic Institutions

The Honourable Marie-Josée Hogue,
Commissioner

VOLUME 4 CHAPTERS 14-18

The Government's Capacity to Detect, Deter and Counter Foreign Interference (Facts and Analysis 2/2)

Public Inquiry Into Foreign Interference
in Federal Electoral Processes and
Democratic Institutions

Final Report
28 January 2025

Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions. Final Report.
Volume 4: The Government's Capacity to Detect, Deter and Counter Foreign Interference (Facts and Analysis 2/2).

Cette publication est également disponible en français :
Volume 4 : La capacité du gouvernement à détecter, prévenir et contrer l'ingérence étrangère (faits et analyse 2/2).

CP32-169/2-2025E-4-PDF
ISBN 978-0-660-75082-8

(Set) CP32-169/2-2025E-PDF

Note on the translation of hearing transcripts

Several footnotes in the report contain references to the transcripts of the Commission's hearings. These footnotes refer to the pagination of the bilingual version of the transcripts (the "floor" version, as spoken) and not to the pagination of the English-only version.

Table of Contents

CHAPTER 14

Intelligence Flow within Government

Information may be incomplete: *intelligence products are discussed in many areas of this public report. Please note that this report includes only relevant information that can be appropriately sanitized for public release in a manner that is not injurious to the critical interests of Canada or its allies, national defence or national security. Additional intelligence may exist.*

14.1 Introduction

Under Clause C of my Terms of Reference, I reviewed how intelligence about foreign interference is created, shared, assessed and distributed within the federal government. In this chapter, I summarize what I learned.

To be useful for government decision-making, intelligence must be shared appropriately. Intelligence agencies have different ways of doing this, but the purpose is the same: ensuring government has access to the intelligence it needs to inform its actions and decisions.

For several reasons, sharing intelligence requires an exercise of judgment.

First, intelligence producers must protect sources and methods. This protection is achieved by having processes that ensure intelligence is shared securely and in a measured way with individuals who have a need to know it.

Second, when sharing their products with senior levels of government, Canadian intelligence producers must use discretion because they distribute an immense volume of intelligence. Witnesses told me that the national security and intelligence community produces approximately 70,000 intelligence products per year. Other witnesses described the flow of information they received as a "river" in both volume and scope. Michael MacDonald, former Interim National Security and Intelligence Advisor to the Prime Minister ("**NSIA**") and Assistant Secretary to the Cabinet, Privy Council Office ("**PCO**") Security and Intelligence Secretariat, estimated that in his three years at PCO he received approximately 25,000 to 28,000 intelligence products. These were of varying degrees of importance, credibility and interest. There is a balance to be struck between ensuring that relevant intelligence is distributed, and over-saturating recipients. As I discuss further below, not all intelligence products need to go to the prime minister, ministers, deputy ministers or even other senior government officials. I will return to this in my recommendations.

The sheer volume of information, the pace at which it is collected and processed, the complications of classification and the sensitivity of intelligence operations mean that effective information sharing in the national security realm poses a significant challenge. But it is a challenge that must be met—responding to national security issues requires the right persons get the right information, in the right way, at the right time.

I heard evidence about several issues and problems in the way information flowed, or did not flow, to senior decision-makers in government. Some of these have also been considered by other review bodies, such as the National Security and Intelligence Review Agency ("**NSIRA**") and the National Security and Intelligence Committee of Parliamentarians ("**NSICOP**"). Some garnered a fair amount of public attention.

Since then, the government has taken several steps to improve its intelligence sharing processes.

In this chapter, I first describe the general processes by which various actors in the government's national security and intelligence apparatus receive and transmit information.

I then address the specific information flow issues that came to my attention over the course of the Commission's work.

14.2 A Centralized Intelligence Distribution System

Around late spring or summer 2023, the national security and intelligence community, led by PCO, undertook to modernize the way intelligence is disseminated and tracked. The goal was to address the problems government had experienced when trying to track certain pieces of intelligence so government would know whether, when and how a piece of intelligence was shared with a particular senior public servant or minister.

Prior to this, some agencies used SLINGSHOT, which was the Communication Security Establishment's ("**CSE's**")'s intelligence dissemination and tracking database system, but others did not. The Canadian Security Intelligence Service ("**CSIS**"), for example, shared its products by email over the Canadian Top Secret Network ("**CTSN**"). This resulted in difficulties in knowing who had seen what and when and how.

The modernization initiative resulted in a new system, which began operating in the fall of 2023, to disseminate and track intelligence sent to senior officials, including ministers.

The new process ensures all formal intelligence reports produced by CSIS, CSE, Global Affairs Canada ("**GAC**"), the Integrated Terrorism Assessment Centre and PCO's Intelligence Assessment Secretariat ("**PCO-IAS**") are disseminated and tracked through an updated CSE centralized database system.

This system has built-in mechanisms that allow the agency or department uploading an intelligence product to flag it for a recipient's attention. The database also tracks who accesses the documents and allows for input of feedback relevant to a product. Moreover, if anyone prints a document, the CSE database requires them to log who they are printing it for. Printing by individuals is logged and the system adds some security and tracking controls to the document.

Intelligence is often brought to the attention of very senior decision-makers, such as Cabinet ministers or the prime minister, by way of oral briefings rather than written intelligence products. Marie-Hélène Chayer, former Acting Assistant Secretary at the PCO Security and Intelligence Secretariat, explained that her team has tried to implement more systematic methods to track oral briefings throughout the intelligence community. For each briefing, agencies now track the date, who was there and what was discussed. In her view, this tracking system is working better, though there is always room for improvement.

14.3 The Communications Security Establishment (CSE)

CSE's foreign intelligence reporting, unlike that of other national security and law enforcement agencies, consists purely of factual representations of electronic communications data. The main audiences for CSE reports within the government are CSIS, GAC, PCO, and, to a lesser extent, the Royal Canadian Mounted Police ("**RCMP**"). Because CSE cannot target Canadians or persons in Canada, its foreign intelligence reporting is less relevant to the mandate of the RCMP. For that reason, CSE provides much less information to the RCMP than CSIS does.

The dissemination of CSE products is governed by the *Mission Policy Suite*,[1] which imposes strict requirements on how CSE products may be shared. CSE distributes intelligence to the national security and intelligence community through "End Product Reports" on its centralized database. With an account, government clients can directly access reports that their security clearance and indoctrinations allow them to view.

As will be explained further below, CSE also shares certain intelligence in hard copy by hand delivering it to named persons and usually taking it back after it has been read.

[1] The *Communications Security Establishment Act* determines what CSE can do under the law. The *Mission Policy Suite* is the written document that directs how CSE will use its authorities.

CSE's mandate relates to the collection of foreign intelligence. While its focus is on the communications of foreigners outside Canada, in collecting foreign intelligence, it may incidentally collect information concerning Canadians. When that occurs, CSE uses suppression to help protect the privacy interests of Canadians in its foreign intelligence reporting. Designated recipients of foreign intelligence reporting who have a need to know must request the identities through a specific process, justify why they are requesting them and show they have the legal authority to receive them. CSE then determines whether access should be given in accordance with the *Communications Security Establishment Act* and identifies in its central database who has received the names.

Distribution of intelligence products

CSE is responsible for two key components of the distribution of intelligence across government.

As explained earlier in this chapter, CSE manages the central database now used by the national security and intelligence community to share reports. CSE determines who among government personnel can access intelligence in the database based on sharing policies and an individual's need-to-know.

CSE is also responsible for the Client Relations Officers ("**CROs**") system. CROs are CSE employees stationed in other departments. They are generally responsible for sharing intelligence with their clients, namely senior government officials and ministerial offices.

CROs select reports relevant to their clients' intelligence requirements and flag them as "to be shown" in the database. Over time, they build knowledge about their clients' requirements. Clients can ask CROs for briefings on specific topics on an *ad hoc* basis. They typically deliver the intelligence to clients in paper format or other secure means and remain in their presence while the clients read it. CROs record the products their clients have read and obtain their feedback.

I heard evidence that there is a capacity issue with the CRO network. Demand for CRO services is high but supply is limited because there are only so many CROs to serve the national security and intelligence community. Alia Tayyeb, Deputy Chief of Signals Intelligence at CSE, said CSE is pursuing solutions to expand the capacity of CROs to meet the needs of government clients.

Intelligence flow to the ministerial level

CSE reports to the Minister of National Defence. The Chief of CSE or their delegate decides what intelligence is shared with the Minister of National Defence. In the normal course, CSE uses CROs to share its reports, and those

received from partners, with the Minister's office. The Chief of CSE also briefs the Minister of National Defence on relevant CSE reports orally during scheduled and *ad hoc* meetings. If a report requires urgent attention from the Minister, the Chief of CSE can take steps to alert the Minister's office by phone or email.

The current Minister of National Defence, Bill Blair, explained that he receives two to three briefings a week from CSE, in addition to *ad hoc* briefings when needed. He said that the record-keeping within CSE is robust: all intelligence products are dated, and he signs to indicate what intelligence reports he has received and read.

14.4 The Canadian Security Intelligence Service (CSIS)

CSIS produces a significant amount of intelligence. In 2022, it produced over 2,500 threat assessments and reports, including on foreign interference. CSIS intelligence is shared with other departments for information purposes, for use in their analysis, for briefings to their executive leadership and to inform their policymaking and decision-making.

CSIS shares a wide range of products across government. These may include raw intelligence[2] to add to a pool of background knowledge on a topic, or intelligence assessments, which analyze multiple pieces of intelligence at a more strategic level. CSIS also shares reports, briefing notes and ministerial memoranda. CSIS can create these products on its own initiative or in response to a request from a government department, or they can be created for a specific inter-departmental committee (see Volume 3, Chapter 11).

In addition to sharing written intelligence products, CSIS gives oral briefings to ministers, deputy ministers, PCO officials and the Prime Minister's Office ("**PMO**"). It will meet with these individuals and their offices at their request. CSIS also provides regular advice during preparatory work for Memoranda to Cabinet and ahead of Cabinet discussions.

When CSIS shares intelligence, the names of Canadian citizens are often "masked." This occurs when CSIS shares information collected as part of its foreign intelligence assistance mandate under section 16 of the *Canadian Security Intelligence Service Act*. CSIS may also mask identities for other reasons, including source sensitivity. CSIS said this practice is consistent with its focus on the threat actors themselves and not the subjects of the threat activity.

---

[2] Raw intelligence refers to information collected by an intelligence agency that has yet to be subject to evaluation or analysis.

Masked identities can sometimes make it challenging for a client to understand the relevance and impact of reporting. If a recipient believes names are required to understand the context of a report, they can ask CSIS not to suppress identities. In doing so, they must advise who is making the request and why the unmasking of that particular name would support their activities. CSIS then makes a decision.

Distribution of intelligence products

CSIS's Assistant Director Requirements decides whether intelligence should be shared, and which product is best suited to a given situation based on several factors.

One of the factors is source reliability. CSIS witnesses told me that CSIS communicates as much information as possible about its assessment of the source of the information. This assessment that may evolve over time. Source reliability is a very important consideration when sharing and interpreting intelligence.

From what I have seen, CSIS relies heavily on standard caveats and wording to convey source reliability. I do not view this as sufficient and will come back to this issue when I make my recommendations.

A dedicated unit under CSIS's Assistant Director Requirements is responsible for distributing CSIS intelligence products. The unit has a list of designated individuals at each government client who act as CSIS's primary points of contact. They are responsible for receiving CSIS intelligence products and then sharing them within their organization based on that organization's mandate, priorities and concerns.

Some intelligence products contain particularly sensitive information. If this is the case, CSIS uses a restricted distribution list of named identified recipients. It is, of course, necessary and appropriate to restrict distribution of highly sensitive intelligence.

However, limited distribution of intelligence due to its sensitivity can have the effect of preventing intelligence from reaching those who have a need to know it and who may be in a position to act on it. To take a concrete example, I heard evidence about an instance in which CSIS distributed an intelligence product to GAC in 2021 regarding the activities of Zhao Wei, a diplomat from the People's Republic of China ("**PRC**"). CSIS limited the distribution of the product to a junior analyst and a CRO, who were restricted in their ability to share it within GAC. As a result, GAC senior intelligence officers were unaware of this product and did not consider it before they produced a 2 May 2023 assessment of Mr. Zhao's activities. I discuss this further in Volume 3, Chapter 11.

CSIS can also flag reports that should be brought to the attention of senior officials within each department, either for action or strategic discussion, by naming them as a specific recipient. CSIS decides which pieces of intelligence to escalate based on its assessment of the importance and impact of a particular intelligence report.

Until the fall of 2023, CSIS sent all intelligence products to government clients by email on the Canadian Top Secret Network (CTSN), which left them unable to accurately track receipt of products. As mentioned above, CSIS now uses CSE's centralized database system to transmit information. This allows CSIS to securely control distribution of intelligence and track who accesses reports.

CSIS still uses CROs to personally give intelligence to ministers. It now also has a Liaison Officer posted at Public Safety Canada ("**Public Safety**"), which has improved its ability to share and track intelligence.

Intelligence flow to the ministerial level

CSIS reports directly to the Minister of Public Safety. CSIS meets regularly with the Minister and their office to inform them of national security developments and CSIS's operational activity, as well as to flag emerging issues. CSIS also sends important intelligence products, via Public Safety, to the Minister's attention.

One type of document produced by CSIS is called an Issues Management Note ("**IMU**"[3]). These are meant to alert the Minister of Public Safety and senior public servants when CSIS is going to take specific action. CSIS issues IMUs when the planned action is politically sensitive or if there is a chance it will become public. CSIS told me they send out approximately three IMUs per week. CSIS uses these products to inform the Minister of Public Safety of upcoming issues so that they would not be taken by surprise.

There appears to have been a lack of understanding between CSIS and its clients in relation to IMUs. The information in IMUs did not always reach the Minister and IMUs were not always considered by the senior Public Safety recipients as particularly significant, among the many intelligence products CSIS shared.

CSIS told me that communication gaps were particularly prevalent during the pandemic. Former Director David Vigneault explained to me that while CSIS generally had to work from the office (though sometimes with fewer people to respect public health guidelines), many of the recipients of its information were working remotely (without access to a secure communications system). As a result, on some occasions, information was not read by or passed to the appropriate people, because they were not there.

[3] For "Issues Management Unit Note."

Feedback on intelligence products

CSIS witnesses told me that it has at times been challenging for CSIS to receive feedback from government clients.

However, I also heard evidence of useful back-and-forth exchanges about intelligence between CSIS and its clients. For example, Katie Telford, the Prime Minister's Chief of Staff, explained that the PMO often provides feedback on intelligence or asks intelligence agencies for more information on particular pieces of intelligence, especially when the intelligence they are receiving could have an impact on someone's career.

I also heard that clients can and do give feedback on intelligence products through the new CSE centralized database. CSIS told me this feedback is important because it informs its future collection and reporting and gives it insight into the types of information recipients want.

I also understand that in setting Canada's intelligence priorities, PCO has a feedback process between the intelligence agencies and their regular clients.

Feedback is vital and should be encouraged at all levels regularly and frequently. Feedback that is received should be provided to those responsible for preparing reports so they can integrate the feedback into their work and ensure that future products better respond to the client's intelligence needs.

14.5 Global Affairs Canada (GAC)

GAC's Intelligence Bureau prepares weekly binders for the Minister of Foreign Affairs and her political staff, and for the Deputy Minister of Foreign Affairs. These include the most relevant raw and assessed intelligence. GAC keeps a record of the products circulated in its binders but is not able to confirm whether the contents have been read by their intended audience.

Distribution of intelligence products

Foreign intelligence assessments produced by GAC's Intelligence Bureau are distributed throughout government using CSE's secure database and shared with like-minded countries via Intelligence Liaison Officers.

The Intelligence Bureau distributes its assessments and other intelligence products to senior GAC officials via CROs.

If the Intelligence Bureau considers a product particularly important, it flags it to senior officials on an *ad hoc* basis or in the weekly binder and sends it to the relevant officials via a CRO to make sure it is read.

As priorities shifted between 2016 and 2020, and foreign interference grew in importance, the GAC binders began to include a section on foreign interference.

The Intelligence Bureau gives verbal briefings to senior officials at the assistant deputy minister level and above on its own initiative or by request. Philippe Lafortune, Director General of the Intelligence Bureau, explained that such briefings happen at least weekly.

Intelligence flow to the ministerial level

The Intelligence Bureau has a direct relationship with the Minister of Foreign Affairs' office.

The Prime Minister's December 2021 mandate letter to Minister of Foreign Affairs Mélanie Joly directed her to counter foreign interference through collective international responses.

The evidence before the Commission with respect to how much exposure Minister Joly had to information about foreign interference prior to 2023 was not clear.

Minister Joly testified that she first started to concretely consider foreign interference as relevant to policy development when she was working on the Indo-Pacific Strategy. She said that one of the several challenges it was developed to address is the significant impact of the People's Republic of China (PRC)'s foreign interference activities. The Indo-Pacific Strategy was publicly announced in November 2022.

In her interview with Commission counsel and her public testimony, Minister Joly said that she only started receiving intelligence about foreign interference in Canada, including briefings and CSIS products, in the spring of 2023. In her interview summary she said this began in March 2023. In her testimony at the hearings, she said it began in early May 2023, following the publication of media articles about the alleged targeting of Member of Parliament ("**MP**") Michael Chong.

At that time, she concluded that she had not previously received intelligence about foreign interference, and she considered this to be problematic. In response, she created the position of National Security Director within her office to ensure that she would get this intelligence. This has addressed the issue. Minister Joly now takes part in intelligence briefings every two weeks, covering a wide range of topics. She also gets *ad hoc* briefings for urgent or upcoming events. She received two or three threat landscape briefings in the summer of 2023.

The Commission's records contain no evidence indicating Minister Joly received specific intelligence briefings on foreign interference events before May 2023. However, some documentary evidence obtained during the Commission's investigation tends to show that Minister Joly was nevertheless exposed to information about foreign interference before May 2023 in the context of her ministerial work. This includes details in relation to section 16 *CSIS Act* foreign intelligence assistance requests, the Indo-Pacific Strategy mentioned above, and the Hostile Activities by State Actors Memorandum to Cabinet that went to Cabinet in May 2022. There are also preparatory notes related to Minister Joly's appearance before the House of Commons Standing Committee on Procedure and House Affairs in December 2022, during which she discussed foreign interference.

The picture of what exactly Minister Joly knew (or did not know) on foreign interference before May 2023 remains unclear to me. Two things, however, are clear.

First, it is clear that Minister Joly was exposed to the topic of foreign interference before the spring of 2023. This is entirely unsurprising given the close nexus between foreign interference and the work that falls to Canada's Foreign Affairs Minister. To the contrary, it would have been surprising if no information about foreign interference had come to her attention in the course of her work.

Second, whether the first intelligence briefings on foreign interference occurred in March 2023 or May 2023 does not change the fact that they should have begun much earlier in her tenure as Minister of Foreign Affairs. Being exposed to some information about foreign interference is one thing, but receiving specific intelligence briefings about it is quite another. When a state engages in foreign interference in Canada, this may be relevant to Canada's policy towards it. As the official responsible for Canada's relations with foreign states, the Minister of Foreign Affairs ought to have been in receipt of intelligence about these activities to inform her deliberations and actions.

It appears that since May 2023, significant steps have been taken by GAC and by the Minister to ensure that more foreign interference-related intelligence is conveyed to the Minister in a timely fashion. Efforts in this direction should continue in order to ensure this Minister and future Ministers of Foreign Affairs continue to properly protect Canadian interests on the international stage.

14.6 The Royal Canadian Mounted Police (RCMP)

Units within the RCMP's Federal Policing and National Security program consult and use all available reporting to prepare criminal intelligence assessments and products. These all-source intelligence products are meant to inform senior management both for awareness and for decision-making purposes. The primary clients for RCMP products that include information from intelligence agencies are senior officials within Federal Policing. However, where broader dissemination is appropriate, versions of these products can be prepared for other units within the RCMP or for government or Five Eyes partners (the United States, the United Kingdom, Australia and New Zealand).

Distribution of intelligence products

The RCMP provides reports, updates and briefings to government departments, agencies, senior government officials and ministers on a wide range of topics, including national security threats.

The RCMP uses distribution lists and chooses a distribution system based on the classification of the product. This applies to both internal sharing within the RCMP and external sharing with other government departments or agencies. Products classified Secret or Top Secret are shared internally through the RCMP Classified Environment or via the Canadian Top Secret Network (CTSN) and shared with recipients outside the RCMP over CTSN.

For internal information sharing, the RCMP has tried to strike the appropriate balance between granting investigators access to classified information and the "need- to-know" principle, though this is an inherently difficult thing to do. To restrict access to specific files that contain sensitive information, the RCMP has an "Access Control List." Very few RCMP units have unfettered access to all restricted files. If an investigator or analyst needs to see a restricted file that they do not have access to, they can make a request. RCMP witnesses recognized that these limits on information sharing within the RCMP could be viewed as hindering foreign interference investigations, which often rely on sensitive intelligence that may be relevant to multiple distinct investigations. But witnesses also said there are systems in place to mitigate this risk while ensuring protection of classified materials.

The RCMP also has integrated teams and relationships with local police to help ensure information sharing. The integrated teams are located in major centres and have representatives from local police. In more isolated communities, foreign interference may not be immediately recognized and information moves less quickly. Information sharing with local police forces

about foreign interference is important since they may often be the first to respond to the problem in its various forms.

The RCMP works closely with other government departments and agencies when coordinating a multi-agency response, including on foreign interference. This includes sitting on multiple committee meetings every week at the deputy minister, assistant deputy minister and director levels, which are both strategic and tactical in nature, to coordinate, deconflict and prioritize responses across the various government departments.

The One Vision Framework

The One Vision Framework governs intelligence sharing between the RCMP and CSIS. It was initially established in 2012 to ensure the two organizations were coordinated and de-conflicted in their responses to threats to public safety given their overlapping mandate to protect Canada. The One Vision Framework has been through several iterations. At the time of writing, the operative version is One Vision 3.0.

Under the One Vision Framework, intelligence is shared through meetings or "use letters." Use letters are how CSIS formally shares intelligence with the RCMP. The information may be caveated and may specify whether and how the information can be used. Sometimes the intelligence is provided to the RCMP for situational awareness only.

While formal meetings may not always result in a use letter, they often do. On average, the two agencies meet at least once a week at Strategic Case Management meetings.

Informally, the CSIS Director also shares information with the RCMP Commissioner at weekly deputy minister committee meetings. The goal of these committee meetings is to discuss the nature of threats and determine appropriate responses within the organizations' respective mandates.

Intelligence flow to the ministerial level

The RCMP reports to the Minister of Public Safety and may provide reports or briefings on classified or sensitive information to the Minister where appropriate. However, the relationship between the RCMP and the Minister is limited by the principle of police independence. This principle requires that police be free from the direction or influence of the executive in exercising their police powers or making decisions related to law enforcement and the investigation of individual cases.

14.7 Public Safety Canada

As I explained in Volume 3, Chapter 11, there are five Public Safety portfolio agencies: CSIS, the RCMP, the Canada Border Services Agency, the Correctional Service of Canada and the Parole Board of Canada. Each of these agencies has a deputy head (for example, the Director of CSIS or the Commissioner of the RCMP) who is equivalent in rank to the Deputy Minister of Public Safety. The agencies report to the Minister of Public Safety, not to the Deputy Minister.

Public Safety's primary function is to provide strategic and policy advice and guidance to its Minister that reflects the mandates and missions of the organizations in their portfolio. The department is separate from the portfolio agencies and is divided into a number of policy areas, including national security, emergency management and law enforcement.

Public Safety is a consumer of intelligence, not a producer. Given its broad mandate and that of the Minister of Public Safety, the amount of intelligence received by Public Safety is vast. Again, I note that it does not seem necessary or advisable to bring every piece of intelligence to the Minister. A selection should be made to ensure that they only receive the intelligence of which they must be aware and of which they are not already aware.

Distribution of intelligence products

The way intelligence is provided to Public Safety, distributed within it and sent to the Minister changed over the course of the Commission's work. Below, I describe these changes.

The National Security Operations Directorate

The National Security Operations Directorate ("**NSOD**") is the unit within Public Safety primarily responsible for receiving intelligence and distributing it to senior officials within the department.

NSOD does not analyze the intelligence it receives and distributes but instead performs a triage function. It elevates particularly sensitive or action-oriented intelligence to senior officials considering their requirements and shifting priorities in response to ongoing or domestic international events.

On a daily basis, NSOD reviews its holdings for exigent intelligence for timely dissemination to designated recipients. On a weekly basis, NSOD compiles routine, relevant intelligence it receives and provides packages to recipients. Additionally, on an *ad hoc* basis and upon request, NSOD provides specific intelligence reports to senior officials in support of classified briefings to the Minister of Public Safety.

The intelligence received by Public Safety pertains not only to foreign interference, but to many other topics including other hostile activities of state actors, threats to economic security, world events, assessments of geopolitical and economic situations, violent extremism and more.

Intelligence flow to senior Public Safety officials: 2019-2022

I heard evidence from Rob Stewart, the former Deputy Minister of Public Safety, and Dominic Rochon, the former Senior Assistant Deputy Minister of Public Safety's National and Cyber Security Branch (which houses NSOD), about intelligence flow during their tenures, namely the very end of 2019 to October 2022.[4]

Mr. Rochon said there were two main ways in which he and Mr. Stewart would receive intelligence products.

One way was through NSOD, which put together a binder every few days for senior officials. He estimated that the average binder held between 12 and 30 reports. NSOD did not have a formal tracking system that allowed it to identify which products were given to or read by senior officials.

The other way was through Client Relations Officers (CROs) every two weeks.

Intelligence flow to the ministerial level

The Minister of Public Safety receives intelligence directly from CSIS and their other portfolio organizations, as well as from Public Safety.

Pre-pandemic

I heard evidence on how Public Safety provided intelligence to the Minister before the pandemic.

Public Safety officials were responsible for transmitting intelligence marked for the Minister's attention. The Minister's office did not have a CTSN terminal, so NSOD would receive the intelligence and deliver a hard copy to his office in Ottawa. NSOD did not "filter" the products marked for the Minister, meaning it did not pick and choose which ones to send. Any intelligence addressed to the Minister was supposed to be provided to him. Mr. Stewart described NSOD's function in this circumstance as "the mail room."

[4] Rob Stewart was appointed as Deputy Minister of Public Safety Canada on 17 December 2019. He occupied this role until 21 October 2022, when he was appointed Deputy Minister of International Trade. Dominic Rochon held the position of Senior Assistant Deputy Minister, National and Cyber Security Branch from 19 October 2019 until October 31, 2022. At the time of writing, he is the Chief Information Officer for the Government of Canada.

Public Safety was also responsible for providing the Minister with a filtered subset of products, selected from the "river" of intelligence that the department received. This selection was generally done by staff within Mr. Rochon's office.

NSOD would also prepare a binder for the Minister's attention on a weekly basis. Public Safety staff did not flag specific intelligence of importance within the binder. The binder would be delivered to the Minister's office by a Departmental Liaison Officer, an employee of the department stationed in the Minister's office in charge of ensuring that the Minister's office was supported by the department, including ensuring that classified materials were delivered to the Minister's office.

Public Safety did not track what happened after information was provided to the Minister's office. Public Safety staff relied on CSIS to bring important matters directly to the Minister's attention, as the Minister had an independent relationship with CSIS.

During the pandemic

Witnesses had different recollections of how intelligence was shared with Minister Blair during the pandemic.

Mr. Stewart and Mr. Rochon said that Public Safety continued to produce binders of intelligence, which were delivered to the Minister at the CSIS Toronto Regional Office or brought to his home in Toronto. This practice was paused during the 2021 election, when the flow of information to the Minister was limited to urgent matters.

In Mr. Stewart's view, the pandemic did not have a very material impact on the flow of intelligence. CSIS staff worked in person throughout, and from Mr. Stewart's perspective, he had a continuous flow of intelligence.

However, he recalled that in the depths of the pandemic, including the spring of 2021, virtually all Public Safety staff were working remotely. NSOD would have two people in the office on any given day. Mr. Stewart did not recall how many people would normally have been there but estimated "a couple of hundred." Instead, it was sometimes just Mr. Rochon and his Chief of Staff. Still, Mr. Stewart told me that the resources were sufficient to decide what to print, print it and put it in a binder.

For her part, Zita Astravas, Minister Blair's Chief of Staff at this time, said the weekly binders stopped coming during the pandemic. She said she only received a smaller subset of intelligence, on a less than weekly basis, and not in a binder. She was told that the binders could no longer be produced, and that the staff who used to assemble the binders had been reassigned. Ms. Astravas recalled telling Marco Mendicino, when he assumed office as Public Safety Minister following the 2021 election, that the Minister's office used to receive an intelligence binder and that he should ask for that to resume.

Mr. Blair and Ms. Astravas said the flow of paper intelligence largely stopped during the pandemic, save for *ad hoc* readings, at CSIS's request. These readings occurred in a secure facility. When CSIS officials wanted them to read a particular product, they told Ms. Astravas and Mr. Blair to go to a secure facility and briefed them there. According to Mr. Blair, no intelligence was delivered at his home during the pandemic, as the CRO program was no longer bringing intelligence to him.

As mentioned above, Mr. Mendicino became Minister of Public Safety shortly after the 2021 election. Mr. Mendicino testified that he recalled Ms. Astravas encouraging him to reinstate the practice of having intelligence binders delivered regularly. Mr. Mendicino added that during his tenure as Public Safety Minister (October 2021 – July 2023), he and his staff worked closely with Deputy Ministers (Mr. Stewart until October 2022, followed by Shawn Tupper), and he had robust and frequent access to intelligence. He also received briefings, about every week and sometimes more frequently, directly from the agencies in his portfolio.

Clearly, there are different recollections as to whether or how routine intelligence was provided to the Minister's office during the pandemic. In my view, given that so few staff were working in person, and that the Minister himself was in Toronto, it is possible that while Public Safety continued to print and provide intelligence to the Minister's office, this was not done systematically, as it had been before the pandemic. This is effectively what Ms. Astravas said—she continued to receive intelligence, but less of it, and less often. Mr. Mendicino indirectly corroborated her testimony in that respect, as he recalled her suggesting that he should reinstate the practice of receiving intelligence binders regularly. However, it is also possible that Public Safety did continue to send binders of intelligence to the Minister's office, but for some reason they never reached Ms. Astravas. In any event, this difference in recollection across the witnesses shows a significant communication breakdown during this period.

Over the course of the Commission's proceedings, I learned that written intelligence products were not a particularly reliable way of conveying information to ministers. That said, the evidence before me shows that, often, when something urgent had to be brought to the Minister's attention, this was generally done by an oral briefing, not by sending a written intelligence product.

Therefore, the real issue was not so much whether an intelligence report had reached the Minister, but whether the information itself had been shared with him. The evidence in that respect is both convincing and concerning: some information was not provided to him in timely fashion. Understanding why there were delays is difficult because no one was able to provide clear explanations. I note, however, that no evidence before me indicates that the information was withheld intentionally, to illegitimate ends. I also did not see any evidence that would show that the information had reached the Minister and that he had decided not to act.

I will return to the topic of conveying intelligence to senior decision-makers in my recommendations.

Recent modifications to sharing intelligence with Public Safety

As described earlier in this chapter, in the spring or summer of 2023, the Privy Council Office (PCO) launched an initiative to standardize intelligence sharing within government. As a result of this change, which was in place by the fall of 2023, Public Safety modified its processes.

Senior Public Safety officials do not rely on weekly binders as much as they used to. Instead, there is a CSIS Liaison Officer posted at Public Safety who is responsible for curating intelligence for senior officials.

The creation of this Liaison Officer position coincided with the shift across the national security and intelligence community to the Communications Security Establishment (CSE)'s centralized intelligence database, which I discussed earlier, and which tracks who has read any given intelligence product. The CSIS Liaison Officer extracts reports from this database and delivers them to senior officials.

The presence of the CSIS Liaison Officer allows Public Safety to consistently track who has had access to intelligence.

Public Safety witnesses told me the CSIS Liaison Officer has good awareness of their interests and requirements and understands the broader context in which Public Safety operates. They see this system as more responsive than the previous one. I cannot say whether this is the case or not, but a close look should be kept on how the new system works to avoid replicating problems, such as those seen during the pandemic.

In August 2023, Dominic LeBlanc became Minister of Public Safety. From that time until December 2024 when he left the portfolio, Minister LeBlanc and his staff received intelligence from the department through the CSIS Liaison Officer. This means that the intelligence the Minister received and read was tracked, which strikes me as good practice.

The Minister also received intelligence directly from the Public Safety portfolio agencies. Mr. LeBlanc told me that he insisted that agency heads reach out to him directly, at any time, if there was anything urgent. He received frequent oral briefings from his agencies. He believes the topics discussed during these briefings were tracked, though he could not confirm this.

14.8 The Privy Council Office (PCO)

PCO's Intelligence Assessment Secretariat (PCO-IAS)

The Intelligence Assessment Secretariat (PCO-IAS) assembles all-source intelligence assessments. The Prime Minister and his Office are two of PCO-IAS's biggest clients, along with the Clerk of the Privy Council (the "**Clerk**"), the National Security and Intelligence Advisor to the Prime Minister (NSIA), ministers and deputy ministers.

PCO-IAS publishes a variety of intelligence assessment products, including the Daily Foreign Intelligence Brief ("**Daily Brief**"), which is widely distributed and reflects three to four important intelligence items based on raw intelligence. It also publishes the Prime Minister's Weekly Intelligence Brief ("**Weekly Brief**"), which contains highlights from the Daily Briefs or intelligence about upcoming events and national intelligence assessments. The Weekly Briefs can be quite lengthy and are peer reviewed.

Nathalie Drouin, current NSIA, said she is working with PCO-IAS to eventually move away from the Daily and Weekly Briefs. Because they are based on assessments, they too often repeat information that she has already sent to the Prime Minister. When those briefs contain information the Prime Minister has already seen, she may not share them with him. However, when PCO-IAS brings something novel, she includes it in the package. I discuss the role of the NSIA below.

PCO-IAS also provides oral briefings to the Prime Minister's Office (PMO).

All PCO-IAS products written for distribution are posted on its website, CTSN and on CSE's database. PCO-IAS now sends intelligence mostly via the CSE system because it automates the tracking of distribution, readership and feedback. PCO-IAS also uses a "push" system (sending email links) to specific points of contact, depending on the product. It also responds to requests for information from its clients.

PCO's Security and Intelligence Secretariat (PCO-S&I)

PCO's Security and Intelligence Secretariat ("**PCO-S&I**") receives reports produced by CSIS, CSE and Five Eyes partners that relay specific intelligence developments. Intelligence received and flagged for senior officials, including the Prime Minister's staff, is operational or tactical in nature. Bridget Walshe, former Director of Operations of PCO-S&I, told me she believes the process for sharing this intelligence is tracked and well recorded.

Much of the reporting PCO-S&I receives is circulated through electronic tools, which automatically record when a user has opened a document or report. However, the PMO has no access to CTSN so they require printed reports with readership marked manually.

PCO-S&I shares intelligence with the PMO if there is an operational priority or urgent reason to do so, but this is not the primary mechanism by which the PMO receives intelligence.

National Security and Intelligence Advisor to the Prime Minister (NSIA)

Former NSIA Jody Thomas explained how she received and distributed intelligence during her tenure (January 2022 to January 2024).

Intelligence flow to the NSIA

First, PCO-IAS gave her a daily intelligence package that could include up to 100 reports. The package had information that intelligence professionals thought she needed to see, as well as important world issues that she was interested in and had flagged. If Ms. Thomas was a named recipient of a report, her staff would bring this to her attention.

Second, for highly classified intelligence products with limited distribution, the materials would be brought to her directly by a Client Relations Officer (CRO). She received documents from CROs daily, sometimes several times a day. The CRO would have to stay and watch as she read the documents and take them away when she had finished. This intelligence was generally on subjects PCO-IAS was already covering. It was rare that there were topics of which Ms. Thomas was not already aware.

Ms. Thomas read her daily intelligence package every morning before her daily briefing with the Clerk at 9:00 a.m. If she did not have time to read through the entire package, she flagged where she had stopped reading, and her staff would read the remainder of the package and note anything that she should read.

Like other deputy ministers, another way in which the NSIA learned of intelligence was through inter-departmental committees (see Volume 3, Chapter 11).

Intelligence flow to the Prime Minister

The NSIA has primary responsibility for determining what the Prime Minister should see, though his staff or senior public servants can also flag matters for his attention.

Ms. Thomas said that what the Prime Minister needed to see changed day-to-day depending on the circumstances. In deciding what he should see, she considered the relevance and immediacy of the intelligence, upcoming events and the Prime Minister's existing knowledge. If she saw intelligence that was actionable and of which the Prime Minister needed to be aware to give direction or to understand actions that the government planned to take, Ms. Thomas flagged it for him.

A CRO hand-delivered the intelligence flagged for the Prime Minister, with arrangements typically made in advance with his office. Ms. Thomas would always ensure that the Clerk, the Prime Minister's Chief of Staff, and generally, the Deputy Chief of Staff, received the same products. On average, Ms. Thomas met with the Prime Minister at least weekly.

During Ms. Thomas's tenure as NSIA, PCO-IAS also gave the Prime Minister and his staff daily intelligence assessment packages. Ms. Thomas was not involved in identifying or approving the contents of the PCO-IAS package. The Prime Minister's staff would also have weekly briefings with PCO-IAS and regular briefings from the NSIA and the intelligence community on issues the community thought the Prime Minister should know about.

Both Nathalie Drouin, the current NSIA,[5] and Ms. Thomas believe the PCO-IAS package to the Prime Minister was over-inclusive. Ms. Thomas said when she came across an important item, she would highlight the most important aspects for senior PMO staff to read.

Ms. Drouin said she is trying to avoid having different channels of intelligence to the Prime Minister. She explained that the process for sharing intelligence with the PMO is becoming more systematic. To better track what goes to the Prime Minister and his office, all information now flows through the NSIA or the Deputy NSIA.

The NSIA determines what will go into the Prime Minister's weekly reading package. The NSIA and Deputy NISA identify intelligence products from their own daily intelligence packages that should be brought to the attention of the Prime Minister, his staff and the Clerk. They provide the identified products to a CRO.

The identified intelligence products are then bundled into a weekly intelligence package for the Prime Minister and his staff. He reads this package on a weekly basis, during a reserved time slot. When the CRO provides the Prime Minister with the intelligence, they note all his questions and bring these to the NSIA or Deputy NSIA's attention. The NSIA and/or Deputy NSIA will respond by briefing the Prime Minister verbally or, if the answer is simple, by a written response in the next reading package sent to him. The NSIA and Deputy NSIA also provide weekly briefings to the Prime Minister and his senior staff.

[5] Nathalie Drouin was appointed NSIA in January of 2024.

This streamlined process allows the NSIA to track what intelligence they receive, what they send to the PMO and who receives it there. It also ensures the Prime Minister receives what he needs without duplication.

Ms. Drouin explained that determining what intelligence should be briefed up is a difficult exercise requiring considerable judgment, given the vast amount received. This job is a fundamental part of PCO's role, since, as Ms. Drouin said, the most precious commodity of ministers and deputy ministers is their time. Ms. Drouin and her team consider a number of factors including what the Prime Minister is about to do, what needs to be done in response to the intelligence, if there is anything imminent he needs to know about, the reliability of the intelligence, whether it is corroborated and whether it is something he knows about already.

Agency heads of CSIS or CSE sometimes flag a document for the Prime Minister's attention. Ms. Drouin noted that sometimes the agency's recommendation to provide intelligence to the Prime Minister will have been overtaken by other events or may not add to his existing knowledge if he has already been briefed on the issue. If Ms. Drouin believes that reading a flagged product would not be a good use of the Prime Minister's time, she usually discusses this with the person who flagged the document and explains her reasoning. Sometimes she will also ask for information to be provided in a different format.

Hypothetically, if the agency head and the NSIA were unable to reach an agreement on whether to send intelligence to the Prime Minister, the agency heads could go to their respective ministers or to the Clerk and raise the issue. The ministers or the Clerk would decide whether to inform the Prime Minister.

The Prime Minister can receive classified information when he is travelling. Ms. Drouin often travels with him and may provide oral briefings to him while he is in transit.

PCO's Democratic Institutions Secretariat (PCO-DI)

PCO Democratic Institutions ("**PCO-DI**") sits outside the national security and intelligence community. Allen Sutherland, Assistant Secretary to the Cabinet responsible for PCO-DI, said he is not a regular consumer of national security intelligence. Much of the information PCO-DI receives is open source. However, PCO-DI requires an understanding of intelligence trends and the threat landscape for its policy work and most of its staff now have Top Secret security clearances. PCO-DI regularly receives intelligence assessments.

PCO-DI's conduit into the national security agencies is PCO-S&I because it deals directly with the national security agencies at an operational level. PCO-DI witnesses also receive intelligence through inter-departmental committees such as the Deputy Minister Committee on Intelligence Response, and they have monthly meetings with the Security and Intelligence Threats to Elections Task Force ("**SITE TF**") (see Volume 3, Chapters 11 and 12).

Mr. Sutherland said that he has access to the information he needs. He does not necessarily want policy analysts to receive raw intelligence, which could detract from their ability to see the bigger picture. He would prefer they work from the best assessments of intelligence. He believes there is no information gap as long as PCO-DI has relationships with the national security and intelligence agencies and can engage with its counterparts at the policy level. In his view, no additional formal machinery to facilitate intelligence sharing with PCO-DI is required.

The Clerk of the Privy Council (Clerk)

The Clerk receives a daily package of intelligence from national security and intelligence agencies and may receive further intelligence directly from agency heads. As a member of the Panel of Five (see Volume 3, Chapter 12), they also receive information on the threat environment from the SITE TF.

Janice Charette, who was Clerk from March 2021 to June 2023,[6] said she typically received a distilled version of the intelligence received by Ms. Thomas. CROs would give her information once per week, or more frequently, if needed. She also received the Daily Briefs and the Weekly Briefs produced by PCO-IAS and had a weekly oral briefing with PCO-IAS.

Ms. Charette said that sometimes Ms. Thomas would flag a piece of intelligence for her attention. They would then decide whether it should go to the Prime Minister. Ms. Charette might also have other information, about upcoming issues or the Prime Minister's concerns, which could indicate that a specific report needed to be shared with him. According to her, the Prime Minister would often ask questions about the intelligence he received. Ms. Thomas and Ms. Charette answered any questions with support from the agency that produced the intelligence.

Ms. Charette met with the Prime Minister on average several times a week.

[6] Janice Charette also served as Clerk between 2014 and 2016.

14.9 The Prime Minister's Office (PMO)

The Prime Minister's Office relies on PCO, chiefly the NSIA, to identify intelligence and brief them.

Katie Telford, the Prime Minister's Chief of Staff, explained that the flow of intelligence to the PMO during the time under investigation by the Commission could be divided into four key time periods: pre-pandemic, pandemic, after the 2021 election and after the reporting on foreign interference in 2023.

In the pre-pandemic period, the Prime Minister's senior staff received most intelligence products in paper form. The PMO was provided with both the Daily and Weekly Briefs. Very little raw intelligence was shared. In the rare event that raw intelligence was brought to staff, it was generally hand-delivered by a CRO.

During the pandemic, the PMO did not get the same amount of intelligence in paper form. The Daily and Weekly Briefs were no longer distributed. When PCO staff or security agencies determined the PMO needed to know about a piece of intelligence, they would make arrangements for this to happen. In some cases, they would go to Ms. Telford's home or ask her to go to the office. In other cases, intelligence would be repackaged to a lower classification level so that it could be shared electronically.

After the 2021 election, the system became more hybrid. During the pandemic, many senior staff were given access to Secret-level technology, which assisted in sharing information. They continued to use this after the pandemic. Sharing intelligence through paper products also resumed.

Ms. Telford said that the PMO began receiving more raw intelligence products during this period. She attributed this partly to the NSIA at the time, as each NSIA had their own style and focus, and partly to events going on in the world.

After the media leaks in 2023, intelligence-sharing protocols become much stricter. Now, intelligence is shared with the PMO through a CRO. The CRO brings Ms. Telford an organized and prioritized package of information and tracks each piece she reads. The CRO also flags intelligence that the Prime Minister has or is about to read, as well as any comments he had on the intelligence that he read. Even though the PMO has secure facilities to store materials, intelligence is not left with them. When Ms. Telford does not complete her reading package, she has to arrange another meeting with the CRO.

14.10 The Prime Minister

The Prime Minister generally receives the weekly reading package prepared by the NSIA on Monday mornings. He sets aside about 45 minutes to an hour to read it. It gives him a general baseline of knowledge, some of which comes from highly classified information. He will sometimes ask for follow-up on a specific issue, or for confirmation that the information has been shared with others who can act on it. When he has specific questions for the CRO, they will generally be answered in his next meeting with the NSIA or in a document in his next reading package.

Additionally, at least once per week, the Prime Minister meets with advisors and officials to discuss some of the more pressing intelligence issues.

The Prime Minister said he only needs to see information that is relevant to his role. He described this as any information that directly impacts or threatens Canadians, is linked to policy decisions the government needs to make or is relevant to upcoming or potential interactions.

In his view, the current system meets his needs well. He noted that his preference is to receive information orally so that he can ask questions and seek details right away from the NSIA or the people who have authority over the relevant collection and operations.

The Prime Minister said he trusts officials of the national security and intelligence community and the NSIA to decide what he should see. They discuss intelligence with him on a regular basis. While he agreed that the primary responsibility for determining what he should see lies with the NSIA, he added that others within his office or senior public servants may also flag matters for his attention.

14.11 Ministerial Accountability

As I said above, not every piece of intelligence needs to go to the prime minister. In Canada's Westminster system, ministers also have accountabilities. Moreover, if a deputy minister or agency head disagrees with the NSIA's decision to not send something to the prime minister, they can go directly to their minister, who has accountabilities to the Prime Minister and to their departments. They can raise the issue at a higher level.

My understanding of the evidence is that there are ongoing discussions about how ministers exercise their accountabilities with respect to foreign interference.

For example, minutes from a Deputy Ministers' Foreign Interference Committee meeting on 20 April 2023 indicate that the Independent Special Rapporteur on Foreign Interference had questions about ministerial accountability, which led to the NSIA tasking PCO officials with mapping the process of how intelligence on foreign interference is circulated to ministers. The minutes note that while the governance process around foreign interference appears to work well at the deputy minister level and between the Prime Minister and his office, the "gap at the ministerial level is a concern."

In the spring of 2023, following the media leaks in 2022 and 2023, the Prime Minister asked the intelligence services to brief four ministers (Minister Blair, Minister LeBlanc, Minister Joly and then-Minister Mendicino) on the relevant intelligence.

Witnesses told me there was a recognition at this time that, while the Prime Minister was being briefed on much of this information, other key ministers were either not getting the information in real time or were still, to a certain extent, in the dark about the allegations in the media. Thus, the Clerk started a series of meetings so that these ministers would be brought up to speed on things that had already been briefed to the Prime Minister and could discuss what to do about it.

While this is a small example, it may illustrate the larger issue regarding intelligence flow to ministers. I note, however, that Minister LeBlanc told me that as Democratic Institutions Minister at the time, he would not have needed that kind of granular information.

14.12 Specific Instances Where Concerns Were Raised

The Commission examined in depth four specific examples of alleged problems with the flow of intelligence within government. Below, I review the evidence and make findings about these incidents.

The PCO Special Report

In this section and the one that follows, I examine the distribution of two intelligence products within government. Both the National Security and Intelligence Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP) reviewed the events surrounding these products and drew certain conclusions about them in their 2024 reports about foreign interference.

Where my conclusions differ from theirs, this is not a criticism of NSIRA's or NSICOP's findings. Rather, it is likely the result of a more complete record available to the Commission and differing mandates between those bodies and the Commission. The Commission had more time, more resources and the ability to gather much more evidence than either review body. It also had the benefit of their very helpful reports.

The document that has become known as the "PCO Special Report" is a PCO Intelligence Assessment Secretariat (PCO-IAS) product about People's Republic of China (PRC) foreign interference prepared in late 2021 and early 2022. The document was never finalized. The PCO Special Report was referred to in the media leaks in early 2023.

Origin of the PCO Special Report

In the fall of 2021, then Acting National Security and Intelligence Advisor to the Prime Minister (NSIA) David Morrison[7] asked PCO-IAS to prepare a report after reading a CSIS Intelligence Assessment on PRC foreign interference. Mr. Morrison said that, in his view, the CSIS assessment raised more questions than it answered about the size and scope of the problem. He wanted a product that would give him a global perspective on PRC foreign interference and help him assess its severity.

Mr. Morrison told me that he was the intended audience for the PCO Special Report. He noted that while "much has been made subsequently [...] as to why this document didn't make it to X person in the political level," that was not his intention in requesting the PCO Special Report.[8]

PCO-IAS worked with CSIS to produce the PCO Special Report. PCO-IAS labelled the report "special" because such collaboration between PCO-IAS and CSIS was fairly novel, and because the report combined domestic and foreign intelligence. This has since become common practice for PCO-IAS products.

By sometime in December 2021, PCO-IAS had a draft ready. The evidence shows Mr. Morrison met with PCO-IAS on 16 December 2021 to discuss this draft. He provided feedback, including comments on the tone, which he found to be somewhat hyperbolic, and said he wanted a new draft provided to him. He also said he viewed some of the activities described as legitimate and common diplomatic activity.

Mr. Morrison had no more involvement with the PCO Special Report because he was appointed Deputy Minister for International Trade shortly after the December 2021 meeting.

---

7 David Morrison is currently the Deputy Minister of Foreign Affairs. He was Foreign and Defence Policy Advisor to the Prime Minister from 2019 to 2022. At the end of June 2021, he was also appointed Acting National Security and Intelligence Advisor to the Prime Minister and served in this capacity until January 2022.

8 Evidence of David Morrison, 4 October 2024, Transcript, vol. 28 at p. 101.

He has since read the second draft of the PCO Special Report because of the media reporting in 2023 and the subsequent review processes that have taken place. In his view, it still does not respond to his original questions about the size, scope and effectiveness of PRC foreign interference. He does not think it should have been shared with the Prime Minister.

The head of PCO-IAS at the time, Martin Green, had a different recollection about the origin of the PCO Special Report. According to him, he had suggested to Mr. Morrison that PCO-IAS produce a paper putting together what was happening internationally and domestically with PRC foreign interference. He understood the report would be used for a senior-level discussion about differing views of foreign interference versus legitimate foreign influence activities.

The NSIA asks for the PCO Special Report to go through governance review

Ms. Thomas succeeded Mr. Morrison as NSIA on 11 January 2022. Mr. Green told Ms. Thomas about the draft PCO Special Report at a meeting with her in late January 2022.[9] The cover letter from Mr. Green to Ms. Thomas attaching the PCO Special Report said that "[t]his report was requested by former a/NSIA David Morrison in order to better understand China's foreign interference in Canada."[10]

This cover letter recommended that Ms. Thomas share the report with certain deputy ministers, ministers, the SITE TF, the Clerk of the Privy Council and the Deputy Clerk. Mr. Green said he hoped the report would generate conversations at a senior level and lead to more direction on the issue.

When Ms. Thomas read the PCO Special Report, she thought it was useful but contained nothing particularly new. Rather, in her view, it was a collection of information from previous reports about PRC foreign interference. She told me that she was concerned generally that some of the language being used in intelligence products was too broad and inflammatory—prone to exaggeration and hyperbole rather than fact. Still, she thought the report was a useful primer for policy discussions and asked for it to go through the usual "governance" process for intelligence products at PCO.

Ms. Thomas explained that governance is an essential element of processing intelligence within PCO and the intelligence world. It ensures that intelligence products are peer-reviewed before they are broadly disseminated. There are committees at the director general and assistant deputy minister levels that review documents before they go to more senior officials like deputy ministers or the prime minister. Ms. Thomas said that this peer review process is critical for ensuring the national security community agrees with the assessment and the intelligence underlying it. Disseminating the PCO Special Report as suggested by Mr. Green would have circumvented the normal vetting process.

---

[9] Ms. Thomas told the Commission that the meeting was on 27 January 2022 while other evidence suggests that it was on 26 January 2022.

[10] CAN011049_0001: *Cover Letter to IAS Report on China's Foreign Interference Activities*.

Lisa Ducharme, current Director of Operations at PCO-IAS, confirmed that if a product is intended to go to deputy ministers or the prime minister, there has to be an assistant deputy minister level conversation about it first.

The PCO Special Report does not go through governance review

Ms. Thomas said that discussion about the PCO Special Report was put on hold at PCO-IAS because of major events that occurred immediately after her meeting with Mr. Green: the Freedom Convoy arrived in Ottawa on 27 January 2022, and Russia's invasion of Ukraine occurred in February 2022. The report only came back up for discussion in the spring of 2022, prior to the Hostile Activities by State Actors Memorandum to Cabinet that was sent to Cabinet in May 2022.

Ms. Ducharme testified it is not uncommon for draft reports to be delayed or remain unfinished. This happens for various reasons, including a shift of resources to focus on other events. She said that this does not mean the information they contain has not been helpful to those who reviewed the drafts.

Since the NSIA does not formally approve PCO-IAS products before distribution, Ms. Thomas did not think PCO-IAS was waiting for her approval to disseminate the PCO Special Report. The Assistant Secretary of PCO-IAS is responsible for ensuring products like this are properly peer reviewed. Ms. Thomas only learned the report had not continued through the governance process through the NSICOP and NSIRA reviews.

PCO-IAS's authority to distribute the PCO Special Report

Ms. Thomas said PCO-IAS had the authority to distribute the PCO Special Report if it had wanted to. PCO-IAS is independent from the NSIA and has the authority to share its assessments as it likes, which ensures there is no interference or perception of interference, whether that be political, bureaucratic or policy-driven.

Mr. Green said he did not feel comfortable sharing the PCO Special Report any further because of the sensitivity of the issue. However, according to Ms. Thomas, the sensitivity of the intelligence does not change the governance process. The purpose of that process is for the national security and intelligence community, including the owners of the relevant intelligence, to agree on how a product has been produced and how it should be released.

The Prime Minister's view of the PCO Special Report

The Prime Minister has now read the PCO Special Report. He said that while some details were new to him, its general contents were not. It did not add anything that he did not already understand and know about PRC foreign interference across Canada. He described the report as useful and a good compilation of information that would have been important for someone new to the job of prime minister.

The Prime Minister does not believe that his reviewing the PCO Special Report sooner would have changed the government's response to foreign interference. The issues and information about PRC foreign interference compiled in the report were not new. In his view, they were known to the government and informed its policy responses, such as the Countering Hostile Activities by State Actors Strategy and later Bill C-70, which was enacted as the *Countering Foreign Interference Act*. Both initiatives are discussed in Volume 3, Chapter 12.

The Targeting Paper

The document known as the "Targeting Paper" is a CSIS analytical product that describes the PRC's strategy to "target" Canadian political actors for influence operations. CSIS witnesses explained that "targeting" in this context simply means the PRC is looking to influence someone. The "target" is not necessarily aware, complicit or threatened in any way. The Targeting Paper discusses how the PRC classifies parliamentarians into three groups:

- Those who are positive towards the PRC.
- Those who are neutral and might be convinced to be more positive towards the PRC.
- Those who are antagonistic to the PRC.

The Commission had access to the Targeting Paper and was able to review it in its entirety during its investigation.

Origin of the Targeting Paper

The Targeting Paper was prepared by a CSIS analyst in 2021, but CSIS did not publish it until 13 February 2023. According to a written response provided to NSIRA during its review, the report's classification level made its distribution challenging. The author continued to raise the Targeting Paper within CSIS when opportunities arose, but it never made it onto the Director's agenda. However, in the fall of 2022, in light of the public conversation on foreign interference, the author got the support they needed to move the Targeting Paper outside of CSIS, and it was made available to certain public servants.

The NSIA reviews the Targeting Paper

Ms. Thomas, the NSIA at the time, received the Targeting Paper as part of her daily intelligence package. She had some concerns with it.

First, the distribution list was both relatively extensive and inaccurate. For instance, people who no longer held certain positions were still listed. At a time when the government was experiencing significant leaks of classified information, Ms. Thomas was particularly concerned about the size, inaccuracy and currency of the distribution list.

Second, the Targeting Paper included the names of individual members of Parliament ("**MPs**") who were "targeted." Ms. Thomas was concerned because this was contrary to the usual CSIS practice of masking names, and it was occurring at a time when there were significant leaks of information. The names could look explosive or salacious if leaked. Janice Charette, Clerk of the Privy Council at the time, explained that sanitization of the names was important because the point of the Targeting Paper was the behaviour of the hostile state actor, not the "targets." In the context of the media leaks, it was particularly important to make sure names were not released and taken out of context.

Third, Ms. Thomas had some questions about whether the Targeting Paper was describing foreign interference or legitimate foreign influence attempts and wanted to discuss that issue with other deputy ministers.

Ms. Thomas therefore asked that distribution of the Targeting Paper be temporarily stopped.

Deputy ministers review the Targeting Paper

The Targeting Paper was subsequently discussed at a deputy ministers' meeting on 24 February 2023 that included the CSIS Director, the Chief of the Communications Security Establishment (CSE), the Deputy Ministers of Foreign Affairs and Public Safety, the NSIA and the Clerk. According to both PCO and CSIS witnesses, the deputy ministers had the same concerns as Ms. Thomas about the highly sensitive nature of the product. They agreed that the distribution list should be reduced and that CSIS should create a less sensitive version, without certain information such as the names of the MPs.

Distribution of the sanitized Targeting Paper

It seems that there were differing understandings about the intended distribution of the revised Targeting Paper following the deputy ministers' meeting, as some participants were under the impression that it would be provided to the Prime Minister.

CSIS is one of the attendees that appears to have been under the impression that the sanitized version of the Targeting Paper was destined to go to the Prime Minister. It conveyed this to NSIRA and NSICOP in the context of their reviews. These review bodies concluded that the Targeting Paper was supposed to go to the Prime Minister but did not. NSIRA suggested it was the NSIA who decided not to share the Targeting Paper with the Prime Minister.

Neither NSIRA nor NSICOP spoke with Ms. Thomas, who was NSIA at the time but had since retired. The Commission was able to hear from her.

Ms. Thomas and Ms. Charrette, both of whom were present at the 24 February 2023 meeting, testified that they never understood the Targeting Paper as destined for the Prime Minister. Moreover, Ms. Thomas said she never even received the revised version of the Targeting Paper from CSIS.

The evidence indicates that the CSIS analyst prepared a sanitized version, but it was never distributed because the distribution list was never updated. It appears that the matter of revising the distribution list fell through the cracks.

CSIS was responsible for giving CSE a list of recipients for the Targeting Paper so that it could be distributed over the CSE database system. In a response to questions from NSICOP and NSIRA, CSIS advised that "conflicting priorities during the spring and summer meant that the Director's office did not raise the issue with [the] Director."[11] Mr. Vigneault, Director of CSIS at that time, only learned through the NSIRA and NSICOP review processes that the revised paper had not been distributed as intended.

Mr. Vigneault told the Commission that he understood from the NSIRA and NSICOP reports that Ms. Thomas had made a specific decision not to share the paper with the Prime Minister because she determined the conduct described was more legitimate diplomatic activity than foreign interference. However, he said he had no personal knowledge of this—his source of information was the NSIRA and NSICOP reports.

CSIS's evidence suggested that the revised distribution list was supposed to be provided by the CSIS Director's office *and* the NSIA. When asked about this, Ms. Thomas testified that the responsibility for creating a new distribution list would fall to CSIS, since they owned the intelligence.

My understanding of the evidence is that the NSIA did not make a decision that the material should not be provided to the Prime Minister. She never received the revised version, and no one followed up.

In my view, the responsibility for updating the distribution list for a CSIS product would fall to CSIS. While the NSIA's input might be sought, the onus was on CSIS to raise the issue. Instead, the Director's office appears to have lost track of the need to revise the distribution list.

This shows that better communication and follow-up regarding draft intelligence products are needed, both within CSIS and between departments.

Differing perspectives on foreign influence vs foreign interference

I also find there were different perspectives about the Targeting Paper's significance, and, in particular, whether some or all the activities described in it were foreign interference or legitimate diplomatic activity. Multiple witnesses testified that the practice of creating different lists of legislators based on their positions on certain issues is commonplace diplomacy. The fact of creating or keeping a list of legislators is not in itself foreign interference; what matters are the reasons for making such a list and the use to which it will be put, which are very difficult to determine.

---

[11] COM0000364: NSIRA, *Review of the dissemination of intelligence on People's Republic of China political foreign interference, 2018-2023* at para. 129.

Ms. Thomas recalled reading the Targeting Paper and finding that the behaviour it described—convincing parliamentarians from a country to vote in favour of another country's interest or change their vote or opinion on an issue—was not necessarily foreign interference. She noted that Canada's diplomats regularly engage in similar behaviour, and that Canada needs to proceed with caution before accusing states of foreign interference when Canada is doing similar things in other countries. Failure to do so could put Canada's diplomats at risk.

Ms. Charette and John Hannaford, the current Clerk, both former ambassadors, agreed. Ms. Charette remembered having lists of legislators who were for and against Canada's positions when she was High Commissioner to the United Kingdom. Mr. Morrison, Deputy Minister of Foreign Affairs, also did not find the Targeting Paper alarming because the concept of "target" lists is normal in the world of diplomacy. The issue was not the existence of such a list, but rather how such lists were used. The Targeting Paper, he noted, did not involve information about threats to individuals.

Ms. Thomas noted in her public testimony that the national security and intelligence community frequently meets to discuss issues and products. If a deputy minister or agency head does not agree with the collective view, they have both the ability and the accountability to raise this with their minister, who in turn has accountability to the Prime Minister and responsibility for directing their department's work. Thus, if there had been a serious disagreement here, the Minister of Public Safety should have been informed (he was not).

Importantly, I note that despite these differing views, the decision at the end of the deputy ministers' meeting was not that the Targeting Paper should be abandoned. On the contrary, it was that a new version should be produced for distribution.

What would have happened if the Targeting Paper had been given to the Prime Minister?

I also find that, even if the Targeting Paper had been given to the Prime Minister in March 2023, it would not have changed the government's response to foreign interference.

CSIS witnesses, including Mr. Vigneault, said that if given to the Prime Minister, the Targeting Paper would have been for information only and not for any particular action. In addition to sharing the Targeting Paper with senior officials, CSIS intended to use an unclassified version to educate MPs.

Nevertheless, Mr. Vigneault thought the Prime Minister should have received the Targeting Paper because it was an important piece of analysis describing PRC activities targeting elected officials in Canada. In his view, if the Prime Minister had read the report, it could have informed him how the national security and intelligence community and the government should continue to assess the PRC's actions. The goal was to generate a discussion between CSIS, the Prime Minister, the Prime Minister's Office and the NSIA.

Ms. Charette noted that by the time it was published in 2023, the information in the Targeting Paper was two years out of date. Ms. Thomas agreed, saying that it might have been different if the Targeting Paper had been brought to the attention of the NSIA in 2021, when it was originally prepared.

The Prime Minister was provided with the Targeting Paper in the context of the Commission's proceedings. He said it shows that PRC diplomats research and categorize MPs, which is not particularly revelatory and is part of what diplomats do in every country around the world. While the Targeting Paper contained some interesting elements, none of them altered his perception of the PRC's behaviour, focus or engagement in foreign influence and interference. The document did not significantly add to his understanding of the situation.

Targeting terminology

Finally, quite apart from the question of distribution, I find that the Targeting Paper provides a good illustration of a problem I noticed in much of the intelligence reporting I saw: a lack of clear and precise terminology. Here, the word "target" is used to mean someone a foreign state is looking to influence (whether legitimately or illegitimately). The same word, "target" is used elsewhere to mean someone who is the object of harassment by a foreign state. And still elsewhere, "target" is used to mean someone whom CSIS is investigating.

To any but the most experienced readers of intelligence—and perhaps even to them—this will result in confusion and misunderstandings. The intelligence community should make efforts to clarify terms like these and ensure this is communicated to the reader.

The Uyghur Motion

On 22 February 2021, MP Michael Chong introduced a motion in the House of Commons declaring the PRC's actions towards the Uyghurs and other Turkic Muslims in Xinjiang a genocide ("**Uyghur Motion**"). The House of Commons passed the Uyghur Motion.

In the aftermath, Canada and the PRC engaged in "tit for tat" targeted sanctioning. As explained in Volume 3, Chapter 11, targeted sanctions prohibit persons in a country and nationals of that country abroad from engaging in commercial and financial relations with the sanctioned individual or entity. They may also restrict the sanctioned individual's ability to travel to the country. Sanctions may be directed at entities, individuals and members of their family.

On 22 March 2021, Canada, along with the United States, United Kingdom and European Union, imposed sanctions on four PRC officials suspected of involvement in the persecution of Uyghurs in Xinjiang.

On 27 March 2021, the PRC responded by placing sanctions on Mr. Chong and all the members of the House of Commons Subcommittee on International Human Rights of the House Standing Committee on Foreign Affairs and International Development.

Two years later, on 1 May 2023, the *Globe and Mail* published an article based on allegedly leaked CSIS intelligence stating that Mr. Chong had been the target of PRC foreign interference efforts in 2021. The article suggested a PRC Ministry of State Security Officer had tried to obtain information on a Canadian MP's relatives who may have been living in the PRC in relation to potential further sanctions.

Mr. Chong was aware of the PRC's sanctions against him in response to his leadership on the Uyghur Motion in 2021. However, until the *Globe and Mail* article, he had not heard that a diplomat working at the PRC Consulate in Toronto had been asked to research him and his relatives in Hong Kong. He said he was disturbed that the intelligence had, in his view, not been acted on for two years and that he was not informed.

The Commission reviewed the flow of information within government from the time CSIS first reported the intelligence relating to Mr. Chong in 2021 until CSIS briefed him in May 2023.

Flow of information within government

Prior to May 2021, CSIS distributed intelligence products about the PRC's interest in MPs, including Mr. Chong and Kenny Chiu, to then-Minister of Public Safety Blair and other named recipients. The distribution list for these intelligence products included: PCO, including the Clerk (Ian Shugart) and NSIA (Vincent Rigby), GAC (including Deputy Minister Marta Morgan), Department of National Defence (including Deputy Minister Jody Thomas), CSE (including its Chief Shelly Bruce) and Public Safety (including Deputy Minister Stewart and Minister Blair). CSIS used Canada's Top Secret Network (CTSN) to email the products to the named recipients, or to the departmental contacts for distribution to the named recipients.

Three of these products reference Mr. Chong. The Commission requested the government produce redacted versions of the three documents for public disclosure. The government refused to do so for reasons of national security confidentiality. In the absence of public versions of the three intelligence products, there was understandably some confusion at the public hearings about these documents.

For clarity, I can confirm that neither the Targeting Paper nor the PCO Special Report, discussed earlier in this chapter, are among these three products. Rather, each product is a CSIS intelligence report.

Intelligence holdings collected at various times indicate that:

- There was interest in certain MPs, including Mr. Chong and Mr. Chiu, from multiple PRC threat actors, including the Ministry of State Security.
- A PRC diplomat was conducting research on a parliamentarian believed to be Mr. Chong.
- PRC officials sought to conduct research on certain MPs, including Mr. Chong, who voted to support the Uyghur Motion, with the intent of imposing sanctions.
- The PRC reportedly sought information about and wanted to invoke sanctions against Mr. Chong's relatives in the PRC.

Mr. Blair testified that he never received the three intelligence products disseminated prior to May 2021 referencing Mr. Chong, nor any other intelligence products disseminated via CTSN. This took place during the pandemic, and he was no longer receiving classified information sent over CTSN. Others could not remember whether they received or read these reports at the time.

Deputy Minister Marta Morgan did not recall reading the reports specifically, but said GAC was closely monitoring the PRC's response to the Uyghur Motion.

Deputy Minister Stewart did not remember whether he received the intelligence products but was almost certain he would have, given the large volume of such material he received as Deputy Minister.

Neither Mr. Morrison, Foreign and Defence Policy Advisor to the Prime Minister at the time, nor Vincent Rigby, the then NSIA, remembered whether they saw these intelligence products.

In response to the intelligence, CSIS decided to provide unclassified defensive briefings (also called "protective security briefings": see Chapter 15) to MPs Chong and Chiu to sensitize them to foreign interference threats posed by the PRC.

CSIS determined that the threshold for a threat reduction measure ("**TRM**"), which would enable it to share classified information with the MPs, was not met. To conduct a TRM, CSIS must have reasonable grounds to believe that the activity the measure addresses constitutes a threat and believe that the TRM will reduce the threat. In these cases, as the threats were non-physical in nature and the sharing of information with the MPs would not have altered the behaviour of the threat actor, the threshold was not met.

On 31 May 2021, CSIS sent—again via CTSN—an Issues Management Note (IMU), to the NSIA, the Minister of Public Safety, the Minister's Chief of Staff Zita Astravas and the Deputy Minister of Public Safety. The IMU explained CSIS's plan for the defensive briefings. It said that the two MPs were targets of

PRC foreign interference threat actors and that the PRC's interest in Mr. Chong included interest in his relatives who may be in the PRC.

Mr. Rigby remembered seeing the IMU when it was first distributed.

Mr. Stewart could not recall receiving it but suspects it would have been included in his binder of intelligence.

Minister Blair and his Chief of Staff, Ms. Astravas, said they did not receive the IMU.

On 20 July 2021, CSIS issued a lengthy intelligence assessment on PRC foreign interference in Canada. This product was distributed more broadly throughout the national security and intelligence community. It briefly mentioned the above intelligence about the PRC's interest in Mr. Chong but did not mention him by name. The relevant portion states that a PRC official sought information on a Canadian MP's relatives who may be located in the PRC for further potential sanctions and that this effort was almost certainly meant to make an example of this MP and deter others from taking anti-PRC positions.

Minister Blair said he saw this intelligence assessment, including the paragraph about PRC officials being interested in relatives of Canadian MPs who may live in the PRC for the purpose of further potential sanctions. He did not know that the paragraph was about Mr. Chong until the media reporting in 2023. Minister Blair did not follow up with CSIS or others on this reporting.

Ms. Astravas did not remember receiving the assessment but indicated that she must have seen it since she received all material provided to Minister Blair.

Mr. Morrison remembered reading the assessment in September 2021, when he was Acting NSIA. He did not know the MP referred to was Mr. Chong. He found the assessment as a whole somewhat lacking in that it raised more questions than it answered, which prompted him to ask his team for more information about PRC foreign interference efforts in Canada. PCO's Intelligence Assessment Secretariat (PCO-IAS) later produced the PCO Special Report in response, which I discussed earlier in this chapter.

Like Minister Blair, various other government witnesses, including senior staff in the Prime Minister's Office (PMO) and the Prime Minister, also first learned of the PRC's interest in Mr. Chong in 2021 from the 1 May 2023 news article. The article prompted a series of meetings between senior public servants, ministers and ministerial staff.

Government response to the intelligence

Prior to the enactment of the *Countering Foreign Interference Act*,[12] which provided CSIS with additional authority to share classified information in certain circumstances, CSIS was limited in its ability to share classified information outside of the federal government. The only mechanism for CSIS to provide an individual who did not hold the requisite security clearance, such as Mr. Chong, with classified information, was a TRM (see Volume 3, Chapter 11). As explained above, CSIS concluded that the threshold to conduct a TRM was not met here as it did not have reasonable grounds to believe that the PRC's activity amounted to a threat.

As mentioned above, in response to the intelligence reporting in 2021, CSIS provided Mr. Chong with an unclassified defensive briefing in June 2021. CSIS also had subsequent discussions with him following that briefing.[13] In these encounters, CSIS did not reveal the intelligence about the PRC's interest in him. However, then-CSIS Director Vigneault told me that, although they were unclassified, CSIS's interactions with Mr. Chong were informed by the CSIS representatives' knowledge of the full, classified picture. In his view, this allowed them to properly contextualize the information provided to Mr. Chong.

A representative from the CSIS Regional Offices who was present at the defensive briefing said their perception was that Mr. Chong was well informed about possible PRC actions associated with his position. Although Mr. Vigneault was not present at the briefing or subsequent meetings, he similarly understood from the documentation of these meetings that the interactions were positive, and that Mr. Chong was aware of the risks of foreign interference.

Mr. Chong told me the defensive briefing provided general advice on how to protect against foreign interference, but he was not told that a PRC diplomat was conducting research on him or his family for the purpose of imposing sanctions. He also told me that following the briefing, he met with CSIS on multiple additional occasions during which he provided information to CSIS officials.

As mentioned above, on 1 May 2023, the *Globe and Mail* published an article based on allegedly leaked CSIS intelligence stating that Mr. Chong had been the target of PRC foreign interference efforts in 2021.

On 2 May 2023, the Prime Minister, Ms. Thomas, the NSIA at the time, and then-CSIS Director Vigneault met with Mr. Chong to discuss the news article. The Prime Minister told Mr. Chong that part of the story was true and other parts were exaggerated. He also told Mr. Chong that he wanted him to have as much information as possible from senior officials.

---

[12] Introduced to Parliament as Bill C-70: see Volume 3, Chapter 12.

[13] A CSIS document indicates that the briefing occurred on 25 June 2021, while Mr. Chong testified that it occurred on 24 June 2021. In my view, nothing turns on this.

Immediately after Mr. Chong met with the Prime Minister, Mr. Vigneault and Ms. Thomas briefed him under CSIS's TRM authority. This allowed them to refer to classified material.

Mr. Vigneault told Mr. Chong that the media reports did not accurately reflect CSIS's 2021 assessment. There was no information suggesting a risk of physical harm to Mr. Chong or his family. In this way, some of the narratives in the media were incomplete or incorrect. Importantly, he told Mr. Chong that the media's understanding of the word "target" in the intelligence reports did not align with CSIS's use of the term. For example, in the intelligence realm, "target" can mean "of interest"; it does not necessarily mean target "for harm." I discussed this problematic terminology in the previous section of this chapter.

Before CSIS conducts a TRM, it completes a four-pillar risk assessment that examines the operational, reputational, foreign policy and legal risks of the proposed action. CSIS assessed that the TRM briefing to Mr. Chong had elevated risk.

Marco Mendicino, who was the Minister of Public Safety at the time of the 2023 TRM, told me that although the intelligence did not indicate any physical threat to Mr. Chong and his family, the TRM was necessary because of the allegations that were circulating in the media of such a threat.

Between 2021, when CSIS provided Mr. Chong with an unclassified protective security briefing, and 2023, when Mr. Vigneault and Ms. Thomas briefed him on classified information under CSIS's TRM authority, the nature of the information about the PRC's interest in Mr. Chong did not change. I query how the threshold for a TRM could have been met in 2023 when it was not in 2021, but my mandate is not to review the exercise of CSIS's powers.

CSIS does not have a specific policy on sharing threat to life information with police, I heard evidence from CSIS witnesses that, when it has information about a threat of physical harm or to the life of an individual, CSIS immediately engages police authorities through established channels. Law enforcement can then advise the individual of the potential threat, under their "duty to warn."

Brian Clow, the Prime Minister's Deputy Chief of Staff, attended a meeting with senior public servants and ministers on 18 May 2023 during which this incident was discussed. Mr. Clow's notes from this meeting confirmed CSIS did not think there was a threat of physical harm to any MP or their family. Dominic LeBlanc, who was Minister of Public Safety at this time, recalled that during this meeting, he sought to understand what type of "research" was allegedly being done—whether this was a euphemism for clandestine activity or merely open source research. He recalled hearing about open source research, which in his view was different from the public discourse of a "threat." His understanding from the meeting was that there was some distance between CSIS's explanation about the research and what Mr. Chong and others saw as threats.

In 2023, CSIS also gave TRM briefings that allowed them to divulge classified information about PRC foreign interference efforts to MP Jenny Kwan, MP Erin O'Toole and former MP Kenny Chiu. I describe this in more detail in **Chapter 15**.

Would anything have been different if CSIS intelligence had been more widely distributed in 2021?

Various witnesses told me that if they had received or read CSIS's intelligence reporting about the PRC's interest in Mr. Chong in 2021, it would not have prompted a different government response.

CSIS reporting about the PRC researching Mr. Chong and his family described economic sanctions as a possibility. Deputy Minister of Foreign Affairs Morrison said the PRC wanted to know more about certain Chinese Canadian MPs and sought to conduct research on them. According to him, merely researching politicians is not foreign interference. It is something all diplomats do. He also said sanctions are common diplomatic practice.

Mr. Morrison explained that after the Uyghur Motion, Canada and the PRC engaged in some reciprocal sanctioning. GAC discussed with CSIS that the PRC's economic sanctions against Canada were a legitimate tool of state craft and diplomacy. Such sanctions can legitimately target a principal's family.

Vincent Rigby, NSIA in 2021, said that throughout his career in the security and intelligence field, he learned "not to push the panic button" but rather to wait and see how a situation might develop. In his view, the intelligence reporting was still in the world of "let's see how this develops" because it was not clear what was happening.

Michael MacDonald, Assistant Secretary to PCO's Security and Intelligence Secretariat (PCO-S&I) said that the behaviour described in the intelligence was not necessarily nefarious.

Martin Benjamin, GAC Director General, Intelligence and Chief of Intelligence (now retired), would have forwarded the intelligence to the relevant GAC geographic desks. But given the absence of actionable intelligence, he did not expect that GAC would take any measures against PRC diplomats.

Mr. Stewart, former Deputy Minister of Public Safety, explained that the IMU in May of 2021 (regarding the defensive briefings to Mr. Chong and Mr. Chiu) would have been included in the broader conversation between Public Safety and CSIS about CSIS's response. This information, however, would not have been taken as news. This type of IMU was not unusual. Mr. Stewart viewed IMUs as a way to pass on information. They did not require action. He would have taken it as an indication that the foreign interference threat was increasing, which could inform policy decisions.

Mr. Vigneault told me that the media reporting sensationalized the intelligence about Mr. Chong and presented information without context. CSIS's assessment was that there was never any physical threat to Mr. Chong or anyone else. While the intelligence was important and resulted in the unclassified defensive briefing, it was not the "biggest red flag ever," which the media made it seem.

Minister Blair said that upon seeing the July 2021 assessment, he had no concerns about anyone's safety. He noted that the document reflected a collective concern regarding foreign interference and that the activities reported were consistent with what he had already said publicly, including in his December 2020 letter to parliamentarians about foreign interference. For Minister Blair, research into an MP for the purpose of sanctions did not raise concerns. Canada also imposes sanctions on foreign nationals.

For his part, Mr. Chong testified that if he had known about the nature of the PRC's interest in him, he would have informed his relatives that they were potentially being targeted. He said that he would have been more situationally aware when taking meetings near the PRC Consulate in Toronto. He also noted that he would have recorded a Zoom call on an all-candidates' debate.

Conclusions

In my view, when there is specific information indicating that a state is planning to undertake punitive measures against an individual or those connected to them it is important to ensure that the individual is informed.

I accept that, in this instance, there may never have been any threat of physical harm to Mr. Chong or any member of his family. However, I also accept that it is very difficult, if not impossible, to know for sure what a hostile state intends to do with information it collects. We may know this, or come to understand it in hindsight, but this does not help determine if someone should be advised at the time the intelligence is collected.

Thus, I believe that CSIS was correct to offer a defensive briefing to Mr. Chong in 2021, even if the intelligence described legitimate diplomatic activity. He was not specifically told, however, about the PRC's interest in him and his family, as this was classified information. In my view, in such a situation, efforts must be made to provide as much information as possible to the person who is targeted.

To be clear, I am not suggesting that the safety and security of human or technical sources or intelligence methods should be compromised to brief targeted individuals. Rather, every effort must be made to find ways of communicating as much information as possible to the person being briefed.

The evidence shows that the information about the PRC's interest in several MPs after the Uyghur Motion did not flow as it should have in the spring of 2021.

I accept that, in the larger picture of intelligence reporting, the pre-May 2021 CSIS intelligence reports may have been viewed as not particularly significant. However, the May 2021 IMU was sent specifically to make the Minister of Public Safety aware of CSIS's intelligence and its action plan, and the information never reached the Minister.

There appears to have been a discrepancy between CSIS's view of IMUs, and the view of the recipients of those IMUs. This demonstrates a problem in the way intelligence products were being distributed at the time. It also indicates the problem with relying on a written intelligence product, without any follow-up, as a way to inform a minister or senior decision-maker. In my view, sending a written product is not enough—if the issue is important enough for the minister to be made aware of it, follow-up should occur, and the minister should be briefed on it.

The CSIS warrant

I received evidence about an application by CSIS to the Federal Court for a warrant. There was an extraordinary delay between the moment the department approved the application and the moment the Minister approved it.

The government made a claim of national security confidentiality in respect of the subject and details of the warrant. I determined that I could make the necessary findings without having to disclose the subject of the warrant in the public report. It was therefore unnecessary to have the government's national security claim resolved by the Federal Court.

The warrant approval process

The *Canadian Security Intelligence Service Act* requires approval of all warrant applications by the Minister of Public Safety. CSIS warrants are one of the state's most powerful and intrusive investigative tools, as they allow a wide range of highly invasive activities that, by their very nature, are destined never to come to light. In part because of this, the process of obtaining a warrant is both complex and labour intensive, involving many internal steps and levels of approval.

This process is as follows:

When an application is ready, CSIS sends it to Public Safety. Public Safety officials then review it and draft a summary with advice to the Minister as to whether or not to approve it. Once everything is in order, the Deputy Minister signs this consultation document and sends it to the Minister's office for consideration by the Minister. The Minister's office may ask questions or request further information from CSIS or Public Safety staff. If the Minister approves the application, the Department of Justice files it with the Federal Court, and a judge holds a hearing to decide whether to grant the warrant.

How the warrant approval process unfolded in this instance

In this instance, CSIS's internal process of preparing the warrant application took several months. I received evidence that there were particular considerations around this warrant application that CSIS had to take into account when preparing it.

The day the application was submitted to Public Safety is referred to in the Commission's public proceedings as "Day 0." The affidavit supporting the application for the warrant was drafted several months prior to Day 0 and was refreshed a month before Day 0. The application was sent to Public Safety with a letter signed by CSIS Director Vigneault, recommending the Minister approve the application within six days.

Mr. Stewart, the Deputy Minister of Public Safety at the time, said CSIS normally gave fairly tight timelines for ministerial decisions about warrant applications, reflecting the fact that significant work is done before the application arrives at Public Safety. However, he said these were meant to be instructive, not hard deadlines. He also noted that, this warrant application happened during the pandemic. When getting an application before the Minister was not an easy thing to do, deadlines such as this were more aspirational than real.

All warrants came with a fairly short time frame, partly because of the prior review and partly because of CSIS's desire to "get on with it." Mr. Stewart testified that putting a deadline of longer than two weeks would pretty much guarantee the application would disappear to the "bottom of the pile."

Mr. Stewart, in his capacity as Deputy Minister, signed the warrant consultation document on Day 4. He then arranged for the warrant package to be sent to the Minister's office in Ottawa through the Departmental Liaison Officer, with a cover note requesting that the Minister approve it that same day. The Minister was in Toronto at the time.

Mr. Vigneault testified that he did not understand why approval was requested for the same day, as it was not a time-sensitive issue. CSIS generally builds in 10 days for the Minister to review and approve a warrant application. Mr. Stewart said he would not have paid particular attention to the due date. Instead, he would simply have waved the due date through. He felt the due date should not be taken to mean the warrant had to be dealt with urgently.

Mr. Rochon, the former Senior Assistant Deputy Minister, National and Cyber Security Branch, said typically the expectation is that it would take one to two weeks to have a warrant application approved by the Minister. Mr. Stewart noted that if the warrant was urgent, a different process would have been followed: the CSIS Director would have told him that it was of high urgency.

According to Mr. Stewart, once the warrant application package was sent to the Minister's office, it was essentially the responsibility of that office and CSIS to coordinate putting it before the Minister. The Departmental Liaison Officer was responsible for tracking the application and reminding the

Minister's office of the need for his signature. However, Mr. Stewart had no recollection or specific knowledge of whether the Officer flagged the warrant when it was sitting in the Minister's office.

Zita Astravas, Minister Blair's Chief of Staff at the time, did not remember exactly when she first received the warrant application; she said that it may not have been on Day 4. Ms. Astravas did not recall seeing the Day 4 requested return date but did not dispute that it was on the materials she received. I note that at the time of the Commission's proceedings, Ms. Astravas had left Minister Blair's office and was working in the private sector. As a result, there were no records before the Commission of her emails or calendar entries from the relevant time.

As per the usual process, CSIS briefed Ms. Astravas on the application before it went to the Minister. This briefing took place on Day 13 and is referred to in the Commission's proceedings as the "Initial Briefing."

Ms. Astravas asked questions about the warrant at the Initial Briefing. She said that, as Chief of Staff, it was part of her function to ask questions about documents that the Minister would have to approve such as this one, to ensure they were ready to present to him. Ms. Astravas's questions were about whether the activities described in the application met the threshold to obtain a warrant, and about other specific information underlying the warrant application that was conveyed to her at the Initial Briefing. Ms. Astravas said that, on a separate occasion, she also received a briefing on the Vanweenan List[14] and how the individuals on that list could be impacted when executing the warrant. There is no record of a specific briefing on this in the materials before the Commission.

Ms. Astravas said these questions were for her information only, not on behalf of the Minister. She did not intend to convey that the warrant was at risk of not being approved until her questions were answered. A senior CSIS official agreed with Ms. Astravas. Michelle Tessier, who attended the Initial Briefing, said her impression was that Ms. Astravas was asking these questions for "follow-up and understanding." She noted that at that point, Ms. Astravas had not yet read the affidavit; she was just being briefed and was asking questions for information. According to Ms. Tessier, Ms. Astravas was "challenging" to ensure there was enough information to bring the activities described in the application over the threshold for a tool as intrusive as a warrant.

In an internal CSIS email, the affiant, who was also present at the Initial Briefing, but who did not testify before me, seemed to have had a different impression. They expressed their view that the application was in danger of not getting signed by the Minister and it would be necessary to make additional arguments as to why CSIS needed warrant powers.

---

[14] The *CSIS Act* requires CSIS to identify "known" persons who are directly affected by the measures in a warrant (for example, if their communications are proposed to be intercepted). The term "Vanweenan List" comes from a 1988 Supreme Court of Canada case, where the Court found that one of the appellants, Ms. Vanweenan, was a "known" person as per an similar provision of the *Criminal Code* about electronic wiretaps, because she was known to the police and there were reasonable and probable grounds to believe that her communications may assist the investigation: *R v Chesson*, [1988] 2 SCR 148.

Ms. Tessier did not agree with the affiant's comments. She did not perceive Ms. Astravas's questions as a condition of moving the warrant ahead. There was never any indication in her mind that Ms. Astravas would not put the warrant to the Minister until her questions were answered.

Ms. Tessier explained that from CSIS's perspective, Ms. Astravas's questions needed to be answered because they could very well be questions the judge hearing the warrant application would ask.

CSIS eventually followed up on Ms. Astravas's questions from the Initial briefing. The classified record includes several internal CSIS email exchanges dating from Day 14 to Day 21 that document this. During this follow-up, CSIS sought information about a matter that, if true, would have been "absolutely crucial" for CSIS, as it would need to be mentioned in the affidavit for CSIS to fulfill its duty of candour to the Federal Court.[15] The duty of candour was top of mind for CSIS at the time, because the Federal Court had released an *en banc* decision in which it found that CSIS had breached its duty of candour in relation to several CSIS warrant applications.

CSIS's concern about the matter referred to above turned out to be a misunderstanding; the event that CSIS was concerned about had not occurred, and the issue was resolved by Day 21. There is no indication in the evidence before me of whether Ms. Astravas was made aware of this, and no indication of whether or when Ms. Astravas received answers to the questions she had posed in the Initial Briefing.

Indeed, there is little useful information in the record about what occurred in the weeks following Day 21 until Day 48, when the CSIS Director discussed the warrant application with Ms. Astravas. CSIS did not recall a back-and-forth on this warrant. Mr. Vigneault testified that the discussion on Day 48 was not about whether the application would go forward, but rather how to manage the complexity of the file in terms of logistics like distribution lists. Ms. Astravas said this could have been the briefing on the Vanweenan list.

The Minister's briefing was scheduled for approximately one week later, on Day 54. Minister Blair reviewed the warrant application in the secure facility immediately prior to his briefing and approved it that same day. Mr. Vigneault's recollection was that Minister Blair did not show or express any hesitation in approving the warrant when presented to him.

When did Minister Blair learn about the warrant?

Minister Blair testified that he did not learn that there was a warrant requiring his review in a secure facility until two or three days before his ministerial briefing occurred.

---

[15] This duty requires that parties that are before a court in *ex parte* proceedings (i.e. without the other side being present) be of utmost good faith in the representations that they make, including a full and frank disclosure of all relevant material facts.

Several months before this briefing, Minister Blair had been briefed about the subject matter of the warrant, but he was not told at that time that CSIS would be seeking a warrant. He anticipated that CSIS would continue to investigate, but no mention was made at that briefing of its intention to seek a warrant.

Shortly before his briefing, Minister Blair learned he would have to attend a secure facility in Toronto to review a warrant application, but he did not know what the warrant was about, as that information could not be communicated outside a secure setting. Nonetheless, he was not surprised when he saw the warrant application and its subject, given the earlier briefing.

Ms. Astravas said Minister Blair was not aware the warrant application was waiting for his approval until he saw the application for the first time on Day 54. However, she believed that he was aware, from his previous discussions with CSIS, that CSIS was moving towards a warrant application.

Delay in the warrant approval process

CSIS officials testified that the delay in getting the Minister's signature was highly unusual, especially given there had been so much discussion before the warrant was submitted. CSIS operational officers found it very frustrating. Ms. Tessier said that CSIS officials always want operations to move quickly, but she was not troubled.

Neither CSIS nor Public Safety staff raised any concerns about the delay with Minister Blair or Ms. Astravas during the 35-day period between Day 13 (the Initial Briefing) and Day 48 (the discussion between the CSIS Director and Ms. Astravas) or otherwise suggested that it was urgent. There is no documentation indicating that CSIS or Public Safety raised the warrant application with the Minister's office during this period at all, which is surprising.

The normal process when there was an issue with the contents, or timeliness, of the approval of a warrant application package, would have been for CSIS operational staff responsible for the application to communicate with their counterparts at Public Safety. There is no evidence that they did so here. The only emails raising concerns about the delay were internal to CSIS.

Mr. Vigneault said he was letting the process follow its course. His staff did not communicate any urgency to him, he understood that this was a "more complicated" warrant and was not surprised the Minister was giving the matter "a sober second thought." It was not something about which Mr. Vigneault "was hounding the minister, or the chief of staff or the deputy." He only learned later, after the Minister testified before the Standing Committee on Procedure and House Affairs in June 2023, that Minister Blair only became aware of the warrant application on the day he signed it.

Public Safety officials also never raised the warrant with the Minister after they sent the application to his office. They considered the matter within the remit of the Minister's office, to be addressed by him and CSIS. For them, CSIS had a direct relationship with the Minister and could raise the issue if needed.

Although Ms. Astravas attended a number of briefings with the Minister and the CSIS Director in classified spaces between days 13 and 54, she did not recall raising this warrant application on any of those occasions. The agenda for these meetings was set by the CSIS Director, and she was not sure whether everyone present had the required indoctrinations to discuss the warrant application.

In the Commission's public hearings, Minister Blair agreed that he had approved two other warrant applications around this time and had attended a Secure Compartmented Information Facility ("**SCIF**") to do so. To be clear, although the warrant applications in question were approved during the pandemic, neither of them was approved between Day 13 and Day 54. Rather, they were approved a few weeks earlier, which was nevertheless during the height of the pandemic. There is no evidence that Minister Blair attended a SCIF for the purpose of reviewing or approving warrant applications other than for this warrant between Days 13 and 54. Had he done so, it would have been surprising if no one from CSIS, Public Safety or his own office had informed him that there was another warrant application outstanding. There is evidence that he attended a SCIF in this period, but for other purposes.

The two warrant applications referred to were applications for a renewal of existing warrants, not brand-new applications. Ms. Astravas said that renewing warrants is a quicker process than new warrants as the Minister is already familiar with the materials, which have previously been approved by a court. Minister Blair agreed that the renewal process was usually "a little bit more straightforward." He also noted that applications to renew a warrant can be fairly urgent, since CSIS requires Federal Court approval before expiry of the existing authorizations.

In any event, I understand the evidence as suggesting that a warrant application is usually received and approved by the Minister within two weeks. And in this case, Minister Blair testified he was able to review and approve the application in a few hours.

Ms. Astravas explained the length of time for the warrant to be approved by the fact it had not been identified as a briefing agenda priority item by the CSIS Director. She also noted that Public Safety was managing several other issues during this time frame: the pandemic, which meant they were in COVID-19-related Cabinet committee meetings every day for multiple hours at the time, as well as Canada's withdrawal from Afghanistan, border security, gun control, the mass shooting in Nova Scotia, economic security, updating terrorist organization listing and security risks resulting from 5G technology. Public Safety officials made a similar point.

Ms. Astravas expressed the view that the length of time between approval of the warrant application by the Minister and the court hearing for authorization indicated that this was not an urgent matter. Urgent matters could go to the court within hours or days. I note, however, this was an observation made in retrospect, not something she would have known at the time.

Minister Blair could not comment on whether the delay was abnormal here. He expected that all officials involved—Ms. Astravas, Mr. Vigneault and Mr. Stewart—ensured that he saw what he needed to see. He noted that the urgency of warrant applications depends on various factors, including whether they are renewals or new applications.

Allegations of interference

Ms. Astravas said that she was forthcoming with CSIS staff throughout the review of the application. She said that she always disclosed any personal knowledge she might have of anything related to a matter to the CSIS Director and had done so here.

In internal CSIS email exchanges that occurred between Days 13 and 48, the affiant expressed frustration with the time it was taking to hear back from the Minister's office and expressed concern about the possibility of interference in the warrant process. Similar concerns were voiced by various Participants in the Commission's public hearings. Those concerns are legitimate and understandable given the unusual delay between Day 0 and Day 54. Furthermore, interference in a warrant application would be very serious.

Ms. Astravas categorically denied having any intent to stall the warrant. She reiterated that she disclosed her relevant personal knowledge to CSIS before the warrant application and when it came to the Minister's office and had also disclosed this to Minister Blair. Mr. Vigneault confirmed that Ms. Astravas had disclosed this to him and said that he took it as a sign of her transparency.

Minister Blair said the warrant was never in danger of not being approved, and that he only considered his statutory responsibilities in assessing the application, without giving any consideration to other factors. Whether he knew someone on the Vanweenan List was not relevant for his review.

Both Minister Blair and Ms. Astravas categorically said they did not tell anyone, including at PCO or the Prime Minister's Office, about the warrant application.

CSIS officials were not under the impression that Minister Blair or Ms. Astravas had any reservations regarding the warrant. When asked to comment on the affiant's concerns, Ms. Tessier said she never had the impression that there was any interference by Ms. Astravas, or any attempt to prevent the warrant application from going forward:

> [the affiant is] perfectly entitled to have that opinion, but all I can say in that regard is, in any dealing I had with Zita on this file or in this file in general, I did not feel there was any (…) interference. I'm very clear on that. I was never told this shouldn't go forward. As I said (…), it was never even alluded to in any discussions I had in terms of we can't go forward with this file. If anything, it would be contrary. I don't think they would want to be seen as interfering in a file.[16]

Mr. Vigneault was equally categorical in dismissing allegations of interference. He noted that unless things change drastically in the coming years, if the Minister of Public Safety were to refuse to approve a warrant application for illegitimate reasons, the CSIS Director would know, and it would be extremely problematic. This is consistent with the evidence that I heard regarding intelligence involving opposition MPs. Mr. Vigneault told me that it would be more complicated to share intelligence about opposition parties with the government of the day. I discuss this further in **Chapter 15**.

Approval of the warrant

The warrant was approved by the Federal Court approximately three weeks after Day 54.

Conclusions

I am in an odd position vis-à-vis this issue. Nothing in the evidence really explains the highly unusual delay that lapsed between the moment the warrant application was given to the Minister's Chief of Staff, Ms. Astravas, and the moment it was brought to the Minister's attention. I do not understand why no one, be it from CSIS or from Public Safety, raised a red flag and asked if anything was missing from, or otherwise problematic about, the warrant application. It seems to me that everyone involved dropped the ball. When a Minister of Public Safety does not know he has to review a warrant application, he cannot exercise his statutory duty.

However, although the delay itself was unacceptable, the evidence does not show any wrongdoing beyond lack of diligence. Nor is there any indication in the evidence before me that the execution of the warrant was compromised.

What this event shows, however, is that there was an urgent need to put in place a more systematic and stringent process for tracking and keeping a record of warrant applications from the moment they leave CSIS to their submission to the Federal Court. I understand from the evidence offered by current Public Safety officials and former Public Safety Minister LeBlanc that such a process is now in place at Public Safety and warrant applications are monitored and tracked. In my view, such a process is essential.

[16] Evidence of Michelle Tessier, Summer 2024, Transcript of *in camera* hearing.

Warrants, as mentioned, are a powerful and important investigative tool and very often are time sensitive. Delay in approving a warrant application can risk compromising a CSIS investigation by materially delaying the start of surveillance. This could give rise to questions about the integrity of the process, which, if substantiated, would be a serious concern.

14.13 Conclusion

As the preceding chapters explained, there are many entities within the federal government that play a role in responding to foreign interference. A great deal of information is generated by these bodies, and the ways in which that information is shared internally are complex.

This chapter has focused on intelligence flow within the public service and the ministry. As this report's previous chapters have also explained, entities outside the government also play key roles in countering foreign interference, and they too require access to information to fulfill their responsibilities. In the next chapter, I examine how information related to foreign interference is shared with parliamentarians and with political parties.

CHAPTER 15

Information Sharing with Parliamentarians and Political Parties

Information may be incomplete: *intelligence products are discussed in many areas of this public report. Please note that this report includes only relevant information that can be appropriately sanitized for public release in a manner that is not injurious to the critical interests of Canada or its allies, national defence or national security. Additional intelligence may exist.*

15.1 Introduction

In **Chapter 14**, I discussed how agencies and departments of the federal government share information and coordinate responses to foreign interference. In this chapter, I begin my examination of how they share information outside of the government.

This chapter focuses on a set of actors who may both be targeted by foreign interference and play a role in countering it: parliamentarians and political parties.

15.2 Unclassified Briefings to Parliamentarians

In a November 2021 Analytic Brief, the Canadian Security Intelligence Service ("**CSIS**") wrote:

> [o]ne of the greatest challenges for [members if Parliament] appears to lie in correctly identifying FI [foreign interference] and recognizing what to do when they believe they are being targeted. Many of the interactions between MPs and foreign officials appear to fall into the FI "grey zone," where the nature and motivations of the contact are ambiguous. This increases the challenge of distinguishing interactions that could be legitimate diplomatic advocacy from clandestine and deceptive attempts to cultivate, co-opt and influence MPs.[17]

I heard that both public servants and political leadership accept that informing parliamentarians, their political staff and party representatives about foreign interference is an important part of Canada's efforts to protect our democratic institutions. In practice, however, disclosing information to these groups is not straightforward.

[17] CAN003712_R01: Canadian Security Intelligence Service, *CSIS Engagement with Elected Officials on Foreign Interference: An Initiative of National Significance*, CAB 2021-22/89 (3 November 2021) at p. 5.

One source of complexity is the issue of classification and the need to protect sources and methods used to collect intelligence. Some parliamentarians may hold security clearances, but most do not. This limits the information that the government can give them. When parliamentarians are given sensitive information, there are unique risks respecting disclosure. Unlike most individuals, who can be prosecuted for disclosing classified information, parliamentarians may be protected by parliamentary privilege when they speak on the floor of the House of Commons or the Senate. Without commenting on the strength or extent of this privilege, I can say that this necessarily changes the risk calculation for the government when deciding when and what to disclose.

One way the government addresses these considerations is by providing parliamentarians unclassified briefings about foreign interference. Sharing unclassified information presents fewer risks and allows the government to reach a broader audience, albeit at the cost of being limited in the amount and detail of information it can provide.

Defensive Briefings (Protective Security Briefings)

Defensive briefings, also referred to as protective security briefings ("**PSBs**"), are one of the tools that CSIS uses to engage with individuals and share information. They are unclassified briefings that can be given to elected officials, and in some cases their staff. Their purpose is to inform recipients about foreign interference in Canada, how to detect it and how to defend against it.

PSBs do not disclose classified information. However, because PSBs are informed by classified information, CSIS's general practice is to advise the recipient that they should not disclose the information. That said, there is no rule that prohibits the recipient from doing so.

There is no standard script for PSBs, though briefers have used an unclassified placemat[18] outlining CSIS's mandate on foreign interference and information about what is and is not foreign interference. The briefings cover topics such as how states try to engage in foreign interference, its covert nature and how elected officials can protect themselves and their staff. The briefings are often tailored to a particular individual, and may change as the conversation develops.

Examples of targeted PSBs are the briefings given to Members of Parliament ("**MPs**") Michael Chong and Kenny Chiu in the spring of 2021, which I mentioned in **Chapter 14**. The purpose of these briefings was to sensitize the MPs to the foreign interference threat, give them advice on best practices and give them a chance to express concerns. Mr. Chong described this as a briefing of general application about foreign interference.

[18] A "placemat" in this context is a diagram with significant information about a concept.

The 2021 PSB campaign

In the summer of 2021, CSIS embarked on a national campaign to provide PSBs to a diverse group of MPs from the Liberal Party of Canada (“**Liberal Party**”), Conservative Party of Canada (“**Conservative Party”)** and New Democratic Party of Canada (“**NDP**”). CSIS prioritized briefing MPs in high-priority ridings and those who could potentially be impacted directly by foreign interference activities.

CSIS received positive feedback from MPs who attended. Some MPs reported being surprised by the information, while others said that they recognized the activities that were described. Many said that all MPs would benefit from such briefings. Following their briefings, several MPs sought to re-engage with CSIS.

CSIS would ideally have been able to brief every MP in 2021. That did not occur, in part because of limited availabilities and timing. There were also discussions within the government about establishing an appropriate approach. In the end, CSIS prioritized the MPs who would most benefit from receiving the briefing. When it saw someone specifically targeted by a foreign state, CSIS said it either provided a PSB to the individual or conducted a threat reduction measure (“**TRM**”). I discuss CSIS’s use of TRMs to brief parliamentarians in more detail below.

A briefing note dated 22 September 2022, indicates that CSIS had decided to continue providing these briefings to individuals at all levels of the government. CSIS continues to provide PSBs both proactively and when asked.

Unclassified briefings to all parliamentarians

2019-2020: The Privy Council Office seeks approval to provide unclassified briefings to all parliamentarians

In December 2018, the National Security and Intelligence Committee of Parliamentarians (“**NSICOP**”) recommended that parliamentarians get briefed on the risks of foreign interference and extremism in Canada upon being sworn in, and regularly thereafter. This recommendation was reiterated in NSICOP’s 2019 annual report. The Sergeant-at-Arms of the House of Commons has also advocated for these types of briefings since 2019.[19]

In response to NSICOP’s recommendation, CSIS and its government partners began working on a plan to brief parliamentarians. According to CSIS witnesses, the general consensus among those working on this issue was that the briefings needed to be developed by a multidisciplinary team of people

[19] The Sergeant-at-Arms is responsible for the security of the House of Commons and members of Parliament when they are in the Chamber and when they are outside the Parliamentary Precinct.

from different agencies and departments. Officials prepared several iterations of the presentation.

In a memorandum dated 16 December 2019, the Clerk of the Privy Council ("**Clerk**") sought the Prime Minister's approval for the delivery of unclassified briefings on foreign interference to MPs and senators. The memorandum stated that such briefings could both raise awareness and provide strategies to mitigate the foreign interference risk. It noted that CSIS had prepared an unclassified introductory briefing and attached briefing materials.

The memorandum was marked "for decision," meaning that policy staff within the Prime Minister's Office ("**PMO**") would typically consider the note, provide their own advice, and then send it to the Prime Minister to make a decision. The PMO receives approximately 1,000 similar notes every year. Some are for information only, but most are for decision. PMO witnesses said that it is not atypical for it to take months to consider and consult on a note.

The PMO received the memorandum in December 2019. PMO witnesses told me the general sentiment within PMO was that the briefings should be implemented. However, the note did not proceed to the Prime Minister. I was told this was because the COVID-19 pandemic arrived shortly thereafter, and the government's focus shifted to responding to the pandemic. Moreover, parliamentarians were no longer in Ottawa as the House of Commons ceased to sit.

The National Security and Intelligence Advisor to the Prime Minister ("**NSIA**") renewed this proposal in a memorandum to the Prime Minister dated 22 December 2020. As I discuss in more detail later in this chapter, the NSIA's memorandum also proposed a series of classified briefings for the leaders of the recognized parties in the House of Commons and attached draft letters to opposition party leaders offering such briefings.

The December 2020 memorandum was again discussed among PMO staff, who remained supportive of the initiative. Some discussions and exchanges occurred in 2021 within the PMO regarding how the briefings should proceed and how they should be introduced to opposition leaders in letters sent to them about the briefings. However, the memorandum did not proceed to the Prime Minister for decision before the 2021 election was called on 15 August 2021.

Therefore, the Prime Minister never received either the December 2019 or December 2020 memoranda. He testified that neither the Privy Council Office ("**PCO**") nor CSIS took steps to bring this matter to his attention or sought to prioritize the two memoranda. The Prime Minister's Chief of Staff, Katie Telford, testified that for urgent matters the Clerk or the NSIA will raise issues directly with the Prime Minister. In her view, the lack of such follow-up meant that the public service did not see this initiative as urgent at the time compared to other issues.

In my view, the briefings should have happened. I find the PMO's explanation for failure to ensure the notes were put before the Prime Minister to be unsatisfactory. The mere fact that the Clerk and the NSIA were able to raise issues directly with the Prime Minister cannot, and should not, excuse the PMO's lack of follow-up.

2022-2024: Renewed efforts to brief all parliamentarians

In January 2022, the idea of providing unclassified briefings to all parliamentarians was apparently raised again within PCO. A draft third memorandum to the Prime Minister was prepared under the NSIA's name. However, it was never finalized or sent. The NSIA at the time, Jody Thomas, testified that she had no recollection of it.

In the summer of 2023, the Sergeant-at-Arms asked CSIS to provide briefings to all caucuses. David Vigneault, then the CSIS Director, said CSIS could not provide such briefings unilaterally. CSIS told me that while it could have provided unclassified briefings on its own, it wanted the broader intelligence community to brief parliamentarians because of the heightened attention that was being paid to foreign interference.

CSIS worked with Public Safety Canada ("**Public Safety**") to develop the content for these briefings. Public Safety then engaged with the Canadian Centre for Cyber Security ("**CCCS**") and the Royal Canadian Mounted Police ("**RCMP**") to create the new briefing materials.

CSIS told me the briefings to all caucuses could not be scheduled before the House of Commons' recess for the summer. Efforts therefore started again in the fall of 2023.

On 7 November 2023, Public Safety staff sent then Minister Dominic LeBlanc[20] a memorandum seeking his approval of the briefing materials. He asked staff to seek further input from the House of Commons administration and approved the material.

Brian Clow, the Deputy Chief of Staff in the PMO, testified that when the PMO received the NSICOP *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* ("**NSICOP Report**") in the spring of 2024,[21] the PMO, the Prime Minister and the NSIA all had conversations about the briefings and agreed that they should happen, which subsequently occurred.

---

[20] Mr. LeBlanc was Minister of Public Safety from July 2023 to December 2024, which covered the period of the Commission's investigation and hearings. MP David McGuinty, former chair of the National Security and Intelligence Committee of Parliamentarians, replaced Mr. LeBlanc as Public Safety Minister in December 2024.

[21] The classified version of the NSICOP Report was delivered to the Prime Minister on 22 March 2024. Brian Clow testified that the PMO received the report in April: Evidence of Brian Clow, 15 October 2024, Transcript, vol. 34 at p. 27.

I pause here to say that I wonder whether these briefings would have ever taken place without the NSICOP Report.

The briefings were delivered caucus-by-caucus in June 2024, and were attended by a representative from CSIS, Public Safety, the RCMP and CCCS. They were comprised of a 20-25-minute presentation followed by a question-and-answer session. The caucus-by-caucus approach was intended to allow parliamentarians to ask questions without another political party present. The briefings were high-level and discussed what constitutes foreign interference, why states do it and examples of foreign interference activities. MPs were told to reach out through the Sergeant-at-Arms if they had subsequent questions. One caucus did so.

Government officials who participated in the presentations said the briefings seemed well received. MPs were engaged and seemed to have a lot of questions. About 50% to 60% of each caucus attended.

Then-Minister of Public Safety LeBlanc testified that he planned to ask Public Safety to re-engage with the Sergeant-at-Arms to determine whether parties wanted an updated briefing. He stated that colleagues told him that the briefings were interesting, and they were able to ask questions to non-partisan experts.

Who had the authority to approve the unclassified briefings?

From the evidence that I heard, there was some uncertainty about who had authority to decide to provide unclassified briefings to all parliamentarians, and whose approval was required. While CSIS provided PSBs to individual parliamentarians on its own, when it or PCO wanted to brief all parliamentarians, officials sought approval initially from the Prime Minister, then from the Minister of Public Safety.

Former CSIS Director Vigneault testified that while CSIS had the authority to brief individual MPs, it would be highly unusual to brief an entire caucus, and that doing so would require working with parliamentary officials like the Sergeant-at-Arms. Caucus briefings would not be something that CSIS would undertake on its own initiative. PCO and Public Safety would also have to be comfortable with the engagement, and because of the direct engagement with Parliament, PCO ought to be involved.

Mr. Clow told the Commission that CSIS has the authority to brief MPs as it sees fit and did not require approval from the Prime Minister. In his view, there was never a need for the Prime Minister to respond to the 2019 or 2020 notes for this to happen, though he acknowledged that the PMO did not communicate this to PCO and that, with the benefit of hindsight, it should have. I agree with him that this should have happened, and I do not understand why it did not. Not answering such a request for years is hard to explain.

That being said, I also wonder why this request was routed to the Prime Minister rather than the Minister of Public Safety. Even if PCO would need to be involved, it strikes me that if CSIS wanted to initiate a briefing campaign, the logical port of call would be with its minister, the Minister of Public Safety, rather than the Prime Minister directly. This may speak to a certain confusion about accountability and reporting chains in matters relevant to countering foreign interference, and the confusion of roles between Public Safety and PCO that I mentioned in **Chapter 14**.

Minister LeBlanc acknowledged in his testimony that public servants do not normally go around and meet with opposition caucuses, and this may be an uncomfortable or unusual space for them. In his view, when officials sought his approval in November 2023 to conduct briefings, it was not a technical or legal requirement, but because the briefings would be outside of the officials' routine business.

The Prime Minister's evidence was that the authority to brief parliamentarians falls to Parliament and the national security and intelligence agencies, not the government. In his view, his approval was not required for briefings to occur. It is the NSIA's responsibility to assess the need and consult with security agencies on how briefings will be conducted and what information can be shared.

Nathalie Drouin, the current NSIA testified that, while the briefings are not necessarily conducted by her, she has the authority to trigger them in cooperation with the Sergeant-at-Arms. The National Counter Foreign Interference Coordinator at Public Safety is now responsible for coordinating these unclassified briefings to caucuses in the House of Commons and groups in the Senate.

The impact of the delay in providing caucus-wide briefings

I heard evidence about whether the failure to start caucus-wide briefings in 2019 made a difference.

While acknowledging that it would have been better had caucus-wide unclassified briefings started earlier than they did, several witnesses provided reasons why this delay may ultimately have had a limited impact. In particular, they emphasized that the information contained in such briefings was at a relatively high level, and that most of the information was available to parliamentarians from a range of other sources. These include a letter on foreign interference sent to all parliamentarians by then Public Safety Minister Bill Blair in December 2020.

However, it is clear that many government actors believed from as early as 2018 that parliamentarians should be briefed more consistently about foreign interference. I also heard testimony from MPs that even basic information can be valuable to them, enabling them to take some measures to protect themselves or prompting them to seek out additional advice and support. I understand this position very well and, as I have already mentioned, I fail to see why these briefings were delayed for so long when they had been requested.

Need for greater transparency by the government

Several MPs who testified said there is a need for greater information sharing by the government. They spoke of a "sunlight policy" that would move away from a regrettable "culture of secrecy." The idea being that more transparency could advance national security. One MP suggested, for example, that strategic disclosure of information could counter foreign interference threats.

15.3 Briefing Parliamentarians under CSIS's Threat Reduction Measure Authority

Since 2015, CSIS has had the authority to take measures to reduce threats to the security of Canada in certain circumstances. These activities, referred to as threat reduction measures ("**TRMs**"), may include providing individuals with information. CSIS has used TRMs to brief individuals about foreign interference. I discuss TRMs in more detail in Volume 3, Chapter 11.

TRM briefings can be similar to protective security briefings (PSBs). However, during a TRM briefing, CSIS may provide more specific information, including classified information, even if the recipient does not have a security clearance.

If the measure is assessed to have an elevated risk, the Minister of Public Safety must approve the briefing before it can occur. There are also legal requirements that must be met, including reasonable grounds to believe that the activity the TRM addresses constitutes a threat to the security of Canada, and that the measure is reasonable and proportionate to the threat. Approving a TRM to disclose classified information to a parliamentarian is time-consuming and laborious.

If this process is followed and these requirements are met, CSIS could use its TRM authority to brief a party leader about foreign interference activities targeting members of their caucus.

In other chapters of this report, I discuss several examples of TRMs wherein CSIS provided classified information to parliamentarians to reduce the threat of foreign interference.

For instance, in Volume 3, Chapter 11, I discuss a 2021 TRM that CSIS implemented in response to foreign interference activities by India, which involved informing current and former MPs about India's foreign interference activities in Canada.

In **Chapter 14**, I discuss a TRM in May 2023 that consisted of briefing Mr. Chong about the intelligence that CSIS had vis-à-vis the People's Republic of China's ("**PRC's**") interest in him, which occurred following media leaks about this topic.

In Volume 2, Chapter 7, I refer to a TRM that CSIS undertook to reduce the foreign interference threat by Pakistan in advance of the 2019 election. This TRM included meeting with candidates or elected officials to discuss the activity of concern.

I also heard evidence about TRMs that are currently being implemented or that CSIS has recently considered implementing. One TRM being planned is to share classified information with an MP about potential foreign interference directed at them.

The Ministerial Directive

Following the 2023 media reporting, which I discuss in Volume 2, Chapter 1, the Prime Minister announced that he would ask the Minister of Public Safety to issue a directive to CSIS to ensure that all information about threats to parliamentarians or their families would be elevated, regardless of its credibility or reliability.

Former CSIS Director Vigneault explained that discussions on a draft directive then began within Public Safety. CSIS was concerned about the content of the draft directive, as it required CSIS to disclose *all* information that it had collected with respect to threats to parliamentarians, regardless of whether the information was corroborated, verified or credible. Although Mr. Vigneault was told that he would have the opportunity to speak with the Minister about his concerns, the *Ministerial Directive on Threats to the Security of Canada Directed at Parliament and Parliamentarians* ("**Ministerial Directive**") was issued the next day, with the content that CSIS found concerning. It goes without saying that the speed of this reaction shows that the Minister clearly understood the need to act quickly following the media reporting and did so.

The Ministerial Directive instructed CSIS to, wherever possible, "ensure that Parliamentarians are informed of threats to the security of Canada directed at them."[22] According to CSIS, this reflected the government's prioritization of activities that CSIS was already doing through its tools like PSBs and TRMs. The Ministerial Directive came at a time when the activities of hostile threat actors were intensifying and gave precision in terms of how the government expected CSIS to engage with parliamentarians.

[22] CAN021931: *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians*, at para. 3.

The Prime Minister told me that the Ministerial Directive was a direct response to what Mr. Chong raised during his May 2023 briefing. In hindsight, Prime Minister Trudeau questioned whether the Ministerial Directive was the right policy, noting that it was implemented in response to media stories and political events rather than a more considered and deliberate policy process. In particular, he felt that it forced officials to elevate what may be fairly unreliable or low-level information to a higher level than would otherwise be merited. The Ministerial Directive was important, however, to demonstrate that the government was taking the issue seriously and that threats to parliamentarians would not be tolerated.

In light of the Ministerial Directive, CSIS identified current and former MPs who were of heightened interest to the PRC, including Jenny Kwan, Erin O'Toole and Kenny Chiu. CSIS decided that it would deliver briefings to these MPs, with content specific to each, in response to the Ministerial Directive.

Threat reduction measures briefing to Erin O'Toole and the House of Commons speech

On 26 May 2023, CSIS conducted separate TRMs pursuant to the Ministerial Directive to MPs Jenny Kwan and Erin O'Toole.

CSIS interpreted the Ministerial Directive as requiring it to inform parliamentarians of all threats directed at them even if not necessarily credible, corroborated or verified. While CSIS would not share information it knew to be not credible, it did share unverified or uncorroborated information.

CSIS officials testified that the briefing script for Mr. O'Toole was "painstakingly crafted" so as to contextualize the classified information that would be provided. This included clearly distinguishing between when CSIS had a strong basis for an assessment versus when information was unverified or uncorroborated.

However, CSIS also acknowledged that the briefing was long, given orally, contained a lot of information and that Mr. O'Toole could not take notes. Dr. Nicole Giles, Senior Assistant Deputy Minister and Deputy Director for Policy and Strategic Partnership at CSIS, explained that, when Mr. O'Toole recalled the briefing after the fact, it may not have always been clear to him which particular information was verified or corroborated and which was not.

Mr. O'Toole testified that the briefing did not leave him feeling better prepared to face the foreign interference threat. It provided him with better insights into the type of intelligence being gathered but did not provide him with safeguards or best practices.

On 30 May 2023, Mr. O'Toole spoke in the House of Commons and discussed what he had been told during the TRM briefing. He said that he did this to put on record what he viewed as violations of his ability to carry out his duties as a parliamentarian, the wider gaps in the system and the risks parliamentarians

face from foreign interference. Mr. O'Toole believes that because he spoke in the House of Commons, his speech was protected by parliamentary privilege.

Mr. O'Toole told me he was very careful to be very general in what he said. He said that it was important to him to not reveal intelligence source information, and that he sought legal advice from counsel experienced in national security matters before making his speech. He viewed this as a responsible way of putting his concerns on the record and being open while protecting classified information.

Despite this, CSIS concluded that Mr. O'Toole's speech did in fact disclose some classified information, including unverified information without proper qualifications. This was communicated to the Prime Minister in a memorandum from the National Security and Intelligence Advisor to the Prime Minister (NSIA) following the speech. The memorandum said that parts of the speech misconstrued or overstated the information given by CSIS and included a chart comparing Mr. O'Toole's statements with the information he received from CSIS. The chart was based on a national security review conducted by CSIS following the speech to assess the potential national security injury that might have resulted from the disclosure of classified information.

I note that the government ultimately provided the Commission with a publicly disclosable version of this memorandum, but it was not available when Mr. O'Toole testified before me. He was therefore not able to see the chart or respond to it. However, he said in his testimony that he did not misconstrue or overstate anything.

Mr. Vigneault considered parts of Mr. O'Toole's public comments inaccurate, although he gave him the benefit of the doubt, recognizing that Mr. O'Toole could not take notes during the briefing. CSIS witnesses felt that Mr. O'Toole understood intelligence and the information presented, but perhaps did not understand all the contextual information provided. Prime Minister Trudeau found Mr. O'Toole's speech frustrating because he thought Mr. O'Toole had mischaracterized what he had been told and made the intelligence sound more certain than it was.

When asked if it was possible that Mr. O'Toole was referring to some of the media reporting as opposed to the information provided by CSIS, Jody Thomas, who was NSIA at the time, said she believed that at least some of the language was taken from what CSIS told him.

The Governance Protocol

As a result of Mr. O'Toole's speech, Public Safety and CSIS paused further briefings under the Ministerial Directive in May 2023 to develop a Governance Protocol ("**Protocol**") that would provide the national security and intelligence community an opportunity to review the briefing messages and underlying intelligence before briefings were done. While the Ministerial Directive was directed at CSIS, it said it needed the entire intelligence community to think strategically about the information being provided in the briefs. The Protocol was meant to correct the requirement to disclose *all* information collected with respect to threats to parliamentarians, whether or not corroborated, verified or credible.

Marie-Hélène Chayer, PCO Assistant Secretary to the Cabinet for the National Security Council, said that the national security community needed to find the right way to explain the information to parliamentarians. For example, the meaning of certain words was not always clear. The Protocol now has a governance process involving several committees and various rounds of consultation intended to come up with a product that is as useful as possible.

Under the Protocol, CSIS prepares a threat briefing package of information on the specific threat directed at the parliamentarian, including classified intelligence, as well as key messages that CSIS officials will use to brief them. Members of the Assistant Deputy Minister National Security Operations Tactical Committee review the intelligence and work on the briefing package. It is then referred to the Deputy Minister Committee on Intelligence Response ("**DMCIR**") for consultation. The Protocol does not specify time limits for all these steps. In my view, it should, since time can be of the essence in the circumstances contemplated by the Protocol.

Within this process, the national security and intelligence community can give the CSIS Director advice, address concerns with the key messages and coordinate an approach to briefing ministers. Witnesses from PCO and CSIS said the Protocol has ensured that the briefings reflect the broader set of information available to the government and allowed coordination among relevant departments to develop the right content.

I heard testimony that the debates at the committees involved in this process have been quite robust so far, have shed light on the perspectives of different departments and have helped to ensure that information is shared effectively with individuals outside of the intelligence community. In some cases, these debates have led to refinements in language in the briefs.

The Protocol also recognizes the possibility for conflicts of interest to arise during the consultation process, and that at times participants may have an interest in the outcome. The Protocol states:

> Modification for conflicts of interest: Public servants, exempt staff, and Ministers operate in and around Parliament. There is a risk that individuals involved in this process have an interest in the outcome. From time to time, adjustments to the protocol may be needed to limit distribution of a document or otherwise modify a step to avoid real or perceived conflicts of interest. If CSIS identifies such a concern, they will raise it with Public Safety Canada for agreement on the revised process for that specific instance. [23]

CSIS said this speaks to one of the challenges it faces in investigations of, and engagements with, the political sphere. This is a unique group, whose members know each other well. This part of the Protocol could potentially allow DMCIR members to not advise their relevant ministers, as is provided for under the Protocol, where doing so could create a potential conflict of interest for the minister.

Although his approval was not required, Minister LeBlanc was sent the Protocol for approval. He approved it on 19 September 2023.

Once the Protocol was complete, CSIS resumed disclosures to parliamentarians, beginning with Mr. Chiu in September of 2023.

Particular considerations in providing classified information to parliamentarians

Providing classified information to parliamentarians is a very sensitive issue for CSIS because parliamentarians may rely on parliamentary privilege to disclose it. CSIS said that the government is currently trying to identify the best ways to address the issue of what to do when the risk of disclosing classified information is too significant.

The Ministerial Directive requires CSIS to take action, including, but not limited to a threat reduction measure (TRM) when it becomes aware of a threat. In deciding what to do, CSIS considers the nature of the information, its source and the risks of exposing the source. CSIS also considers whether alternatives to a TRM, like a PSB, may achieve the desired result without disclosing classified information. Other national security and intelligence community partners can help to identify other options when the risks of using classified information are too significant.

Michelle Tessier, former CSIS Deputy Director of Operations, noted that this issue showed the need to increase general awareness of the intelligence collection process. She expressed the hope that, if people had a better understanding of the impacts of revealing classified information, they might

[23] CAN028170_0001: Update – Upcoming Threat Reduction Briefings to Parliamentarians (13 September 2023) at p. 15.

be less likely to expose a source. Ms. Tessier said that it is also important to increase understanding of the limits inherent in intelligence. However, Mr. Vigneault noted that information sharing with parliamentarians is a very sensitive area for CSIS, as it always has to be mindful of their parliamentary privilege.

15.4 A Concern about Sharing Information with Parliamentarians: Advanced Persistent Threat 31 Cyber Campaign Targeting Members of the Inter-Parliamentary Alliance on China

Emails to Inter-Parliamentary Alliance on China members in 2021

The evidence before me indicates that Advanced Persistent Threat 31 ("**APT 31**") is a group of malicious cyber actors who work at the direction of the Ministry of State Security of the People's Republic of China (PRC). The group is focused on espionage and foreign interference in general. It is a pervasive cyber espionage threat that targets the governments of many Western countries, including Canada. It has a long-standing and ongoing interest in Canadian government officials and parliamentarians.

In January 2021, APT 31 conducted an email campaign targeting members of the Inter-Parliamentary Alliance on China ("**IPAC**"), an organization of parliamentarians from around the world who share a common view that the PRC represents a threat that should be dealt with in a stronger and more risk-conscious way. APT 31 sent spear phishing emails to IPAC members in a number of countries, including Canada, embedded with tracking links. The idea was to get the recipient to open the email, at which point the tracking link would allow APT 31 to confirm the validity of the email address and gather certain basic information, such as the IP address of the device. This kind of email can be a precursor to follow-up activity by a threat actor. It cannot, however, compromise an account or device by itself.

Several Canadian parliamentarians are members of IPAC and received emails from APT 31. Messages were directed to both parliamentary and personal email addresses.

As I will discuss further below, the parliamentarians targeted by this email campaign first learned about it in the spring of 2024. This incident, and the absence of notice to parliamentarians, raises questions about whether the parliamentarians who were targeted ought to have been informed about the email campaign and, if so, who was responsible for telling them.

Detecting and responding to the APT 31 email campaign

Before I consider how parliamentarians learned about the APT 31 campaign and whether the government ought to have informed them sooner, it is important to explain how the government responded to the threat.

On 22 January 2021, the Communication Security Establishment ("**CSE**")'s Canadian Centre for Cyber Security (CCCS) received a tip from a trusted partner about an email campaign targeting parliamentarians. CCCS did not know which parliamentarians were being targeted; the information it had consisted of technical details associated with network traffic.

That same day, CCCS emailed an unclassified Cyber Event Report to House of Commons IT officials ("**House IT**"). The report stated that emails with tracking links had been sent to parliamentary email accounts, provided technical information and recommended that House IT take certain steps in response. The instructions with the report said House IT had to get CCCS's permission to share this information with others.

Although CCCS was aware of APT 31's involvement, the report did not attribute the activities to APT 31, as this was classified information. CCCS's priority was to get information to House IT that it needed in order to mitigate the incident from its end. For CCCS to provide the initial technical information to House IT quickly, the report was sent at an unclassified level.

House IT investigated and identified eight members of Parliament (MPs) who had been targeted. It reached out to all of them to ask whether they had received the emails. None reported receiving them. House IT then learned that the emails had been quarantined by the system and had not reached their targets.

House IT also notified the Senate's Information Services Directorate ("**Senate IT**"). Unlike the House of Commons, the Senate's system did not quarantine all the emails, and a few reached senators' mailboxes. Senate IT ensured these emails were destroyed. Ultimately, Senate IT assessed that the attack had been unsuccessful since the emails were either quarantined or deleted before they were opened.

While the initial priority was to mitigate the risk, it was important to CCCS to educate House IT about the identity of the threat actor behind the campaign. As such, on 17 February 2021, CCCS sent a second report to House IT, saying that sophisticated actors were doing network reconnaissance of devices known to connect to the House of Commons' virtual private network. Representatives from CCCS and CSIS met with House IT to deliver a Secret

level classified briefing that same day. Agency officials told House IT that they suspected APT 31 was responsible for the email campaign and briefed House IT on APT 31's suspected links to the PRC, its tactics and its historical targets. This meeting took time to organize because of the impact of the pandemic on organizing and holding classified meetings.

Neither House IT nor CCCS informed Senate IT of APT 31's involvement at this time. The Senate did not have a Memorandum of Understanding with CCCS at the time, as the House of Commons did. Senate IT only learned of APT 31's involvement in April 2024 from the media, and subsequently, in May or June 2024 from House of Commons officials. Senate officials testified that knowing that the campaign was linked to a foreign state would not have changed how they responded.

Immediately following the 17 February 2021 meeting, CCCS officials internally raised concerns to CCCS executives that House IT had not been given sufficient information to appreciate the significance of the threat. Additional meetings were held between CSIS, CCCS and House IT on 19 and 22 February 2021 to discuss the scope of the incident, and at which House IT gave forensic data to CSIS and CCCS.

Further communications between House IT, CCCS and CSIS took place in the days that followed. In one instance, CCCS asked House IT for copies of the actual emails. House IT did not provide them because it did not have consent from the MPs to do so. House IT said it did not seek consent because the emails had never reached the MPs.

In the following days, House IT identified a total of 14 MPs whose email accounts had been targeted. House IT assessed that some MPs' personal email addresses may have received emails. Two Senate email accounts were also identified. Senate officials told me that the senators who received the emails deleted them. On 1 March 2021, House IT informed CCCS that at least one IP address identified in the CCCS report was associated with the home network of a user of the House of Commons' network.

A few weeks later, CCCS detected that a device located at the House of Commons was connected to suspected malicious infrastructure and sent House IT a report requesting more information so they could assess the situation. However, House IT determined that this was about a personal device, on a portion of the House's network intended for personal devices, and that the device had not been detected inside the office network. Because of this, it did not, from their perspective, amount to a threat to the parliamentary infrastructure.

On 3 June 2021, CSIS told House IT that all targeted parliamentarians were members of IPAC and provided a full list of Canadian IPAC members. A year later in June 2022, the United States ("**US**") Federal Bureau of Investigation ("**FBI**") learned that APT 31 had been targeting members of IPAC and notified governments with impacted legislators, including Canada. House of Commons officials were not aware that the FBI had given this information to the government.

How parliamentarians came to learn of the APT 31 campaign

Parliamentarians first became aware of the APT 31 campaign in April 2024, though at least one targeted former MP did not learn of the events until May 2024.

On 25 March 2024, a US indictment charging several members of APT 31, which referenced the campaign targeting IPAC, was unsealed. The London-based IPAC Secretariat learned of the indictment and met with the FBI in mid-April. The FBI reviewed IPAC's member email distribution list and identified 122 addresses that the FBI believed had been targeted by APT 31.

In each country where it operates, IPAC has national co-chairs. In Canada, they are Conservative Party MP Garnett Genuis and Liberal Party MP John McKay. Sometime on the weekend of 19 April 2024, the Executive Director of IPAC phoned Mr. Genuis and briefed him on the information the FBI had shared. During this call, Mr. Genuis learned that it was his personal email account that had been targeted. The Executive Director of IPAC and Mr. Genuis had a second call, this time with Mr. McKay, on 24 April 2024. Later that day, the IPAC Executive Director and Canadian Co-Chairs held a telephone briefing for Canadian IPAC members. The Executive Director also sent an email to all impacted parliamentarians, providing them with information about the attack.

On 29 April 2024, Mr. Genuis raised a question of privilege in the House of Commons about the APT 31 campaign and the fact that officials did not notify parliamentarians. The Speaker ruled that there was a *prima facie* breach of privilege and referred the matter to the Standing Committee on Procedure and House Affairs (see Volume 2, Chapter 2).

The nature of the threat

To the extent CCCS has detected PRC threat actors, such as APT 31, on Canadian networks, their activities have been consistent with espionage and intelligence collection. Cyber espionage is used to collect information that will provide an economic and diplomatic advantage. As such, unless there is a specific reason to believe cyber actors like APT 31 are accessing a network for an attack, CSE has previously assessed this type of activity through the lens of espionage.

Global Affairs Canada ("**GAC**") similarly views APT 31's cyber activities as espionage. The legality of espionage is a complex question, and beyond the scope of this Commission's mandate. For present purposes, it is sufficient to note that in the view of some, espionage is not necessarily contrary to international norms.

Although, while espionage is not itself foreign interference, a cyber actor could use information obtained through espionage to later carry out foreign interference activities.

In November 2021, CSIS assessed that the APT 31 email campaign had been unsuccessful.

Determining the intent behind this type of online activity can be difficult. Commenting on a 2023 email from a CCCS analyst, Alia Tayyeb, Deputy Chief of SIGINT, expressed the view that there may be a legitimate intelligence advantage for a foreign adversary to collect MPs' emails. In this case, there was no indication that the cyber activity was undertaken to directly interfere in democratic processes. However, a malicious email can be a means of securing a foothold on a network.

Likewise, CSIS assessed that the intention could have been to gain insight into IPAC's work, which could potentially allow the PRC to better position itself to respond to any forthcoming IPAC announcements that may be critical of the PRC. The intention may also have been to gather information about IPAC members to embarrass or discredit them.

Should parliamentarians have been notified?

I heard a range of views about whether MPs should have been notified of the APT 31 campaign.

As targets of the email campaign, Mr. McKay and Mr. Genuis felt that they should have been notified when it occurred, but disagreed on who was responsible for telling them. Mr. McKay said it should have been the House of Commons. Mr. Genuis said it was the government's responsibility.

Caroline Xavier, the Chief of CSE, testified that if the APT 31 campaign had occurred today, steps would absolutely have been taken to brief the targeted parliamentarians, because of the Ministerial Directive now in force. Briefings would be provided either by CSIS or by the House of Commons. Both she and Nathalie Drouin, the NSIA, viewed the APT 31 campaign as the type of activity intended to be captured by the Ministerial Directive. This perspective suggests that the APT 31 campaign was the type of threat that parliamentarians ought to have been briefed about.

I heard from Bo Basler of CSIS that if a similar campaign occurred today, a discussion would likely have to take place between CSIS, CCCS and House of Commons' officials about whether to tell parliamentarians.

However, House IT shared a slightly different perspective. House IT witnesses said that there are hundreds of millions of attack attempts in a year, so briefing about all of them would be operationally impracticable. House IT did not inform MPs about APT 31 because the campaign had been unsuccessful:

APT 31 never reached its targets. A briefing would generally occur if a cyber attack resulted in an impact on an MP's devices or their information.

All targeted senators were informed in January or February 2021, although Senate IT did not learn the campaign was attributed to APT 31 until April or May 2024. As mentioned above, Senate IT acknowledged that knowing APT 31 was responsible would not have changed its response.

Who is responsible for notifying parliamentarians of a cyber threat?

The APT 31 incident speaks to the broader issue of who was, and who currently is, responsible for informing parliamentarians of this type of cyber threat. The evidence suggests that, at the time of the email campaign, it was unclear who was responsible for briefing the targeted parliamentarians, if indeed they should have been briefed.

Mr. Vigneault, the CSIS Director during this time, said that while CSIS was involved in many of the meetings with House IT, CCCS was the lead agency on the government side.

However, Ms. Xavier testified that her expectation during the events was that House IT would continue to engage with CCCS in responding to the campaign. Ms. Xavier said CCCS only had information about the targeted IP addresses. Only House IT could determine which individual parliamentarians were targeted. House IT noted that CCCS had not advised it to inform MPs.

I heard from several witnesses that this issue would not arise today since, if CSE identified intelligence about a threat to parliamentarians, it would go through the Ministerial Directive and Governance Protocol. In early September 2023, Ms. Xavier issued a directive outlining her expectation that CSE would support CSIS in carrying out its duties under the Ministerial Directive.

CSE told me that it would not likely brief individuals directly under the Ministerial Directive. I heard that it remains within the authority of CSE's clients to determine what measures, including briefing a parliamentarian, they can take within their own authorities. CSE ordinarily provides classified information to security-cleared IT service providers or provides advice on steps to take.

Providing CSE or other agencies and departments with additional authorities to engage parliamentarians may still be worth considering. I was told there is an active discussion at the Deputy Minister Committee on Intelligence Response (see Volume 3, Chapter 11) about whether the Ministerial Directive should be extended to the entire national security and intelligence community rather than just CSIS. While it is clear that CSIS has the authority to engage with parliamentarians about threats, it is less clear if other departments can

engage directly. Nevertheless, CSIS told me if it learns of a threat from CSE, CSIS will ensure there is a discussion to determine if parliamentarians should be informed and by whom.

15.5 Information Sharing by the Privy Council Office

Aside from protective security briefings (PSBs) or briefings pursuant to CSIS's threat reduction measure (TRM) authority, I also heard evidence that, at times, officials from the Privy Council Office (PCO) have met with MPs to share information on the threat of foreign interference. Michael MacDonald, former PCO Assistant Secretary to Cabinet for Security and Intelligence, testified that while CSIS TRMs carry a certain weight because of the seriousness that most people feel when interacting with CSIS, PCO can also speak to parliamentarians about foreign interference. Officials tailor the strategy to the situation.

For example, I heard evidence where the Prime Minister's Office (PMO) asked the NSIA to meet with an MP to discuss various topics, including how foreign states may try to manipulate parliamentarians. While the NSIA does not have the authority to deliver a defensive briefing or implement a TRM, the PMO saw value in this approach. The NSIA explained that they were very limited in terms of the information they could share. My understanding is that they could not include any classified information or specifics.

15.6 Information Sharing by Global Affairs Canada

I heard evidence indicating that GAC can also share information about potential foreign interference with MPs in specific circumstances. The evidence before me outlines two examples from 2023 in which information obtained by GAC's Rapid Response Mechanism ("**RRM**") Canada was shared with parliamentarians.

Misinformation targeting Mr. Chong

As I explained in Volume 3, Chapter 10, in the summer of 2023, RRM Canada detected a campaign that spread false narratives about the identity, background, political stances and family heritage of Mr. Chong. RRM Canada had a high level of confidence that the campaign was linked to the People's Republic of China (PRC) and assessed that between 2 and 5 million WeChat users had viewed the false or misleading content. After this matter was discussed at the Deputy Minister Committee on Intelligence Response (DMCIR), PCO and CSIS briefed the Prime Minister about this campaign.

On 9 August 2023, GAC senior officials briefed Mr. Chong about disinformation targeting him. Information about the campaign was also released publicly.

Mr. Chong told me he felt the government's decision to release information provided him some protection and reassurance. He believed this was a good example of how things should be made public. However, he would have liked the government to have acted more quickly.

Spamouflage campaign

In September 2023, RRM Canada was advised by one of its counterparts that a bot network affiliated to the PRC had left thousands of comments on the Facebook and Twitter accounts of more than 40 MPs.[24] The comments claimed that Xin Liu, a well-known critic of the Chinese Communist Party ("**CCP**"),[25] had accused the MPs of criminal and ethical violations, including "political corruption," "sexual scandals" involving minors and bribing voters during an election.[26] RRM Canada agreed with its counterpart's assessment that this unusual network activity was "spamouflage"[27] produced by a bot network likely controlled by the Ministry of Public Security, a PRC law enforcement entity.

RRM Canada assessed that an exceedingly low number of Canadians had seen the posts, and that, therefore, the impact on MPs was likely low. However, RRM Canada assessed the impact on Mr. Liu was likely very high. It issued a report about the spamouflage on 15 September 2023. I also referred to this spamouflage campaign in Volume 3, Chapter 10, as an example of how disinformation can be a powerful foreign interference tactic.

---

[24] Targets included the Prime Minister, the Leader of the Opposition, several members of Cabinet, and backbencher MPs across the political spectrum and spanning multiple geographic regions of Canada.

[25] Xin Liu is a Vancouver-based video commentator who participated in China's 1989 democracy movement. He maintains a popular video blog on YouTube and a large following on Twitter/X. He frequently criticizes the governance practices of CCP General Secretary Xi Jinping.

[26] CAN025903_0001: RM Canada, *Probable PRC "Spamouflage" Campaign Targets Dozens of Canadian MPs in Disinformation Campaign, as well as Chinese-language Commentator in Vancouver* (15 September 2023), at p. 1.

[27] The word "spamouflage" is a combination of the words "spam" and "camouflage" and describes covert and hidden attempts to spread spam-like content and propaganda among more benign, human interest-style content.

The matter was discussed at DMCIR on 6 October 2023, and DMCIR approved a briefing package to the MPs. On 23 October 2023, GAC sent a notice to all MPs and emailed the MPs who had been targeted by the spamouflage.

15.7 Briefing Political Party Representatives During Elections

The government has used various means to provide information about foreign interference to political parties around elections.

Classified briefings to cleared party representatives

As I discussed in Volume 2, Chapter 8, the Security and Intelligence Threats to Elections Task Force ("**SITE TF**") offered Secret level briefings to security cleared representatives of the Conservative Party, Liberal Party and NDP in both 2019 and 2021. The briefings included open source information, as well as some classified information about the kinds of foreign interference tactics in use. They did not refer to specific intelligence or threat actors. The information was not specific, which allowed it to be shared at the Secret level, rather than at a higher level of classification.

SITE TF members explained that the briefings had two purposes. The first was to provide a bit more information than could be found in publicly available sources about foreign interference tactics and techniques to raise political parties' awareness and allow them to identify potential foreign interference in their processes. The second purpose was to open a two-way path of communication so that, if political parties had concerns, they could tell the SITE TF.

Security-cleared representatives from the Conservative Party, Liberal Party and NDP told me the information they received was general, background information about threats. There was no specific or actionable intelligence. SITE TF members agreed that the type of information provided in these briefings was not immediately actionable.

Unclassified briefings to parties

The government has also offered unclassified briefings to political parties. As I discussed in Volume 3, Chapter 12, PCO and the SITE TF offered to brief political party representatives at the unclassified level for nearly all by-elections since June 2023. As I note in that chapter, attendance at these

briefings has been poor. The SITE TF has made efforts to give more concrete examples of what foreign interference could look like in the Canadian electoral context going forward. It is not yet clear whether parties will attend these briefings and if they will find the information to be more useful.

I would strongly encourage party representatives to attend such briefings when they are offered, and I would urge PCO and the SITE TF to ensure that the briefings are as meaningful, specific and useful as possible.

15.8 Classified Briefings to Political Party Leaders

The special role of party leaders

The leaders of political parties have unique powers and responsibilities within Canada's democratic system, and thus may have a significant role to play in responding to foreign interference.

Under the *Canada Elections Act*, political party leaders have absolute discretion to decide who is allowed to run for the party in an election. Leaders must sign off on candidates and may appoint a candidate with or without a nomination contest.

After MPs are elected, party leaders are responsible for assigning people to positions and functions within the caucus. The leader of the governing party decides who sits in Cabinet or becomes a parliamentary secretary. Opposition leaders assign critic portfolios and decide who occupies positions such as whip or house leader. While party leaders cannot expel MPs from Parliament, they can remove them from caucus. At a more informal level, party leaders can speak with MPs to discuss concerns, articulate expectations and convey warnings.

A number of witnesses pointed to these powers as being potential tools to address foreign interference targeting parliamentarians. For example, a party leader can remove an MP from positions of power, other than their status as an MP, or avoid putting them in such positions in the first place if there are questions about their integrity. Leaders can discuss concerns with parliamentarians about relationships they may have, such as with foreign officials.

I also heard, however, that for leaders to be able to do this, they may need access to intelligence to know that an issue exists. Providing leaders with timely access to intelligence can be particularly important during election periods, when leaders may have more options, such as not allowing a candidate to run under the party's name.

For the party that forms the Government, giving this type of intelligence to the party leader is fairly straightforward, since the Prime Minister can be briefed as necessary. However, it is more complicated when the intelligence concerns an opposition MP or candidate. The Prime Minister testified that, while he can be briefed, it would be awkward for him as leader of one political party to be engaged with the issue of whether members of a different political party should be allowed to run or hold a certain role. He suggested that party leaders should instead be accountable for ensuring their own systems are resilient against threat actors.

Challenges with briefing party leaders

Giving opposition parties access to intelligence is not as simple as it sounds. Indeed, opposition leaders have traditionally not had regular access to classified intelligence about members of their caucus or candidates.

One challenge is that providing classified information to party leaders, who are often sitting MPs, comes with all the risks that I discussed earlier in this chapter about sharing classified material generally with parliamentarians. Like other parliamentarians, party leaders enjoy parliamentary privilege, which may (I make no finding on the point) shield them from liability for disclosing sensitive information without authorization if this is done in Parliament.

There are also challenges for party leaders who receive intelligence, particularly if they are told that there are limits to how they can use it due to national security concerns. When this happens, a party leader may feel as if there is little they can do.

Even when there is an action that can be taken, sharing sensitive intelligence about an MP can put a leader in a challenging position because any decision affecting the MP may have to be made without providing them with due process. After all, it may be impossible for the leader to explain to an individual why they will not be permitted to run for the party, let alone give them a chance to respond to any accusations against them. Further, significant suspicion could arise from the unexplained removal of a candidate from a ballot or caucus. That said, taking action may be prudent, even if it is unfair. It all depends on the specific circumstances.

Despite all these challenges, the perceived need to inform opposition leaders has led the government to consider ways to give all party leaders access to classified information.

Offering Top Secret clearances to opposition leaders

As I discussed earlier in this chapter, in December 2020 a memorandum from the National Security and Intelligence Advisor to the Prime Minister (NSIA) included a suggestion to provide Secret level briefings to opposition leaders. This recommendation was ultimately never actioned.

In May of 2023, opposition leaders were offered the opportunity to obtain Top Secret security clearances so they could read the classified annex to the report of the Independent Special Rapporteur on Foreign Interference. Leaders with clearances were later able to read the classified version of the National Security and Intelligence Committee of Parliamentarians (NSICOP) *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* (NSICOP Report). I also note that, as per the Commission's Terms of Reference, the Governor in Council may make the classified supplements to my Initial and Final Reports available to the leaders of all recognized parties in the House of Commons who have the requisite security clearance.[28]

At the time of the Commission's public hearings, only leaders of the NDP and Green Party of Canada ("**Green Party**") had taken up the offer. However, I am aware from public reporting that the Leader of the Bloc Québécois has now received Top Secret clearance as well. The Leader of the Conservative Party has publicly stated that he will not apply for clearance. However, his Chief of Staff obtained a Top Secret clearance.

To date, briefings to opposition leaders have been provided on an *ad hoc* basis, coordinated through the NSIA and Deputy NSIA. PCO put together a package of intelligence for opposition party leaders to read, based on both general issues about the security situation and what specifically each leader needs to know. Opposition party leaders then have an opportunity to ask questions. Both the NDP and Green Party Leaders have had classified briefings.

A May 2024 memorandum to the Prime Minister from the NSIA, Nathalie Drouin, notes that PCO was preparing to share a protocol for the provision of regular classified briefings to the leaders of all the recognized parties. At the public hearings, Ms. Drouin said that PCO was finalizing the protocol for regular briefings (at least twice a year) to all parties with representation in the House of Commons at the classified level, in addition to *ad hoc* briefings. The Conservative Party Leader's Chief of Staff has received classified briefings as well.

[28] Terms of Reference, clause (a)(i)(G).

Briefings regarding specific intelligence in spring 2024

In the spring of 2024, the government had intelligence related to opposition parties that required it to provide special *ad hoc* classified briefings to party leaders.

A memorandum to the Prime Minister dated 2 May 2024, titled "Ad Hoc Classified Briefings," refers to intelligence about foreign interference activities directed at opposition parties. The intelligence indicated a foreign state was interested in influencing political processes.

The intelligence was brought to the NSIA's attention and then circulated to the Clerk of the Privy Council (Clerk), the Prime Minister and the Deputy Minister Committee on Intelligence Response (DMCIR). Some of this intelligence described allegations of a serious nature. Ms. Drouin testified that the government determined that a classified briefing to certain opposition party leaders or their representatives was necessary. She emphasized that the purpose of 2 May 2024 memorandum was to inform the Prime Minister that the other party leaders would be briefed, not to seek his authorization.

The memorandum further said that CSIS would develop briefings at the Top Secret level, which would allow the briefed parties to take action if appropriate. It also indicated that PCO and CSIS would work with the leaders to identify what information could be shared and how the parties might address issues in a way that did not jeopardize intelligence sources. Ms. Drouin explained that information in the note reflected PCO's view that these briefings were necessary despite the risks that the information could be used and shared improperly.

The challenge of opposition leaders who are not briefed

I heard that it poses a challenge for the government if a party leader does not have a security clearance.

The Prime Minister's Office (PMO) has asked government officials if it is possible to inform an opposition party of some information even if its leader does not have a security clearance. I heard there are ongoing discussions on bringing intelligence reporting about foreign interference, including disinformation, to the attention of a political party.

The Prime Minister spoke of one case where the NSIA gave him information on significant potential foreign interference involving opposition parties. The information, he said, was explosive. According to him, he told the NSIA, CSIS and others that they needed a response plan. He noted to them that it was not good for democracy for him, in his dual role as Prime Minister and leader of the Liberal Party, to use information about potential foreign interference involving opposition parties. It could be seen as being used to embarrass them.

The Prime Minister said that he has offered classified briefings to all party leaders so that they are best positioned to take action to protect their MPs, some of whom might be vulnerable or, wittingly or unwittingly, implicated in foreign interference. In the absence of the Leader of the Conservative Party having a security clearance, the Prime Minister has directed CSIS and others to try to inform the leader so that he can be warned and armed to make decisions about protecting the Conservative Party and its members. However, determining how to do so may be challenging. For example, the Prime Minister testified that chiefs of staff have more limited authorities compared to party leaders and are not accountable to the public in the same way.

Mr.Chong suggested that members of the King's Privy Council can receive classified information by virtue of their oaths and role, without having to apply for a security clearance. This would include him and the Leader of the Conservative Party.

The Prime Minister said that the title of Privy Councillor is not equivalent to a security clearance and does not grant access to classified information in general. It allows Privy Councillors to access information that is relevant to their duties and roles as Privy Councillors in the government. This is why, for instance, Marco Mendicino, who was Minister of Public Safety from October 2021 to July 2023—and is therefore a Privy Councillor—needed to obtain a new security clearance to review materials relevant to his *in camera* testimony before the Commission.

15.9 Information from the Canadian Centre for Cyber Security

Some political parties have had contact with the Canadian Centre for Cyber Security (CCCS). They found it helpful to varying degrees. At least two parties had also consulted external cyber security experts; in one case to find out best practices with respect to a specific social media platform. One party said it would benefit from additional advice and guidance to support its current IT infrastructure against foreign interference threats and would like funding for this.

15.10 The Impact of Bill C-70

Before the passage of the *Countering Foreign Interference Act* (introduced as Bill C70), CSIS was restricted in its ability to share information outside of the federal government. With its new disclosure authorities, CSIS may be able to approach the question of providing information to opposition parties or parliamentarians differently. For example, one CSIS witness explained that the new Act allows CSIS to deliver more classified briefings to entities like electoral district associations, which CSIS had considered doing because it views nomination processes as vulnerable to foreign interference.

Mr. Mendicino explained that the *Countering Foreign Interference Act* aims to address the limitation on CSIS's ability to disclose classified information in protective security briefings to MPs. In his view, the amendments will allow CSIS to declassify as much information as possible, which will allow it to provide more comprehensive briefings, share intelligence outside of the government and have a more outward-facing approach to threat reduction.

That said, the *Countering Foreign Interference Act* does not change the need to protect sources of intelligence and methods of collection. Nor does it eliminate the challenges and risks that I have identified above with regards to sharing classified information with parliamentarians and political party leaders. These difficulties continue to exist.

15.11 Conclusion

As this chapter illustrates, sharing information about foreign interference outside the government is both important and challenging. Even sharing information with actors like parliamentarians can present difficulties for the government. However, no matter the challenge, sharing information with parliamentarians is key to building resilience against foreign interference.

Parliamentarians are not, however, the only actors outside of the federal government who need access to information to better defend against the foreign interference threat. In the next chapter, I discuss some of the issues relating to sharing information with others outside of the federal government, such as other governments and the general public.

CHAPTER 16

Information Sharing Outside of the Federal Government

Information may be incomplete: *intelligence products are discussed in many areas of this public report. Please note that this report includes only relevant information that can be appropriately sanitized for public release in a manner that is not injurious to the critical interests of Canada or its allies, national defence or national security. Additional intelligence may exist.*

16.1 Introduction

The previous two chapters of this report have focused on how information is shared within the federal government, and with parliamentarians and political parties. In this chapter, I consider how the federal government shares information with entities that are entirely outside of the federal level.

16.2 Engaging with Other Governments in Canada

The importance of inter-governmental communication

Foreign interference does not only target federal institutions and processes. Foreign actors target institutions at every level in Canada. Provincial, territorial, Indigenous and municipal governments are all critical aspects of our democratic system, and it is important that as a society we work to defend them alongside federal democratic processes. Accomplishing this requires collaboration between various governments. Senior government officials told me that sharing information with other levels of government about threats that they face is important.

Responses to foreign interference—regardless of what level of government is targeted—may also require response tools in fields of jurisdiction that do not fall to the federal government under the Constitution. A prime example of this is education. I heard that building digital literacy is a key part of Canada's efforts to counter misinformation and disinformation. Yet, implementing this likely requires initiatives in public education that the federal government is neither responsible for, nor able to implement. Rather, provincial, territorial and Indigenous governments have primary responsibility in this area.

This is not to say that the federal government has no role to play, only that in responding to foreign interference, it is important to recognize and respect jurisdictional and legal boundaries imposed by the Constitution. For example, the Canadian Security Intelligence Service ("**CSIS**") might share information with a municipality or province about the dangers of using a specific technology and suggest courses of actions, but the responsibility to then mitigate the risks remains with the municipality or province. Because of this, the federal government must help and support other levels of government to exercise their authorities to build Canada's collective resilience.

Governments outside of the federal level are therefore key players in a whole-of-society response to foreign interference. There is a shared interest in building resiliency and ensuring that Canada has free and fair elections at all levels of government and a healthy democracy. Effectively countering foreign interference will require cooperation and collaboration between governments from coast to coast to coast.

Challenges in engaging with other governments

Saying that collaboration is important is one thing, but I understand that collaboration can sometimes be difficult. There are often challenges in government-to-government relations and these may arise when coordinating responses to foreign interference.

Different governments have different resources, capacities and levels of knowledge about national security issues. I heard from federal government witnesses that an important consideration for them when engaging with provinces and territories is their varying awareness and capacities about national security matters. This can make it challenging to coordinate effectively with provinces and territories for operational purposes. The same is likely true for Indigenous and municipal governments.

Different governments may also face different threats. This may mean varying priorities from one government to another, and the need for distinct approaches when the federal government is working with many levels of government.

The fact that governments operate in different ways also presents practical challenges. Federal, provincial, territorial, Indigenous and municipal governments are all structured differently. At a basic level, it can be difficult for federal officials to identify departments, offices or their counterparts and collaborators.

Issues surrounding sharing classified information, which I have discussed throughout this report, present another practical challenge for effective government-to-government cooperation.

On 31 October 2023, the Premier of Yukon, Ranj Pillai, wrote to the Prime Minister with concerns about the lack of consultation on national security incidents and the inability of security agencies to share classified information with subnational government officials. Premier Pillai mentioned the need for physical and digital security infrastructure that would enable access to sensitive information for provinces and territories. In response, the Prime Minister said the *Countering Foreign Interference Act* (Bill C-70)—which I discuss in Volume 3, Chapter 12—was intended in part to address Premier Pillai's concern about information sharing.

Several witnesses said Bill C-70 expanded CSIS's ability to share classified information outside the federal government and they expect that it will improve information flow. However, Bill C-70 does not lessen the need for security agencies to protect sources and intelligence collection methods when they share classified information outside the government.

The federal government has also invited specific provincial and territorial officials to obtain security clearances, which would give it designated contact points for national security matters. This process is ongoing.

I heard further evidence that provincial and territorial infrastructure and capacity to process and store classified information is a barrier to sharing intelligence. Currently, the government is seeking to build information-sharing networks between the federal government and the provinces and territories, and has offered to equip provinces and territories with communications systems up to the Secret level.

In the meantime, however, challenges with sharing classified information remain. Moreover, given the sheer number of Indigenous and municipal governments across Canada, and their varying levels of resources, it seems to me that information sharing may continue to present challenges in many cases.

Work to date

Notwithstanding these challenges, I heard evidence that the federal government is making efforts to engage with provinces, territories, Indigenous governments and municipalities in relation to foreign interference.

Within the Privy Council Office ("**PCO**") a number of initiatives are underway. The National Security and Intelligence Advisor to the Prime Minister is working with the national security and intelligence community to develop agendas and baseline briefings for provinces and territories, as well as tailored briefings and materials that speak to their specific needs and threat environment.

The PCO Security and Intelligence Secretariat and Public Safety Canada ("**Public Safety**") co-lead a national security table at the assistant deputy minister level with provinces and territories. This table stopped meeting during the COVID-19 pandemic, but has been restarted as a forum to address

all national security matters, including foreign interference. PCO has also been involved in several bilateral meetings with provinces. The objective of these meetings is to enable the government to share information with provinces and to enable provinces to raise concerns. This seeks to address the challenge I noted above about structural differences between governments.

The PCO Democratic Institutions Secretariat has regular contact with provincial and territorial officials. It has given the provinces and territories its guidebook on foreign interference and its compendium of best practices on foreign interference. In January 2024, it released its *Protecting Democracy Toolkit*, which it also shared with provinces and territories.

Both the Clerk of the Privy Council and Department of Canadian Heritage ("**Canadian Heritage**") have made efforts to engage with provinces and territories on building digital literacy. Canadian Heritage has also engaged with provincial governments on issues related to artificial intelligence.

Public Safety's National Counter Foreign Interference Coordinator, who I discuss in Volume 3, Chapter 11, delivered a foreign interference-related briefing to provincial members of the legislative assembly in British Columbia before its provincial election. They have offered to provide similar briefings to all provinces and territories.

16.3 Engaging with the Public

Essentially all federal agencies and departments who testified emphasized that public outreach was a key component of a whole-of-society response to counter foreign interference. For example, I heard evidence that the Canadian national security and intelligence community recognizes a need to engage with victims of cyber incidents. They have developed public engagement mechanisms, such as publications, for various audiences to do this. Some agencies, like CSIS and the Royal Canadian Mounted Police ("**RCMP**"), also have dedicated branches for this.

Most government witnesses told me that a single point of contact within government for public outreach would not be productive. While coordination is important, so government's messaging is coherent and avoids "consultation fatigue," it is also key for people to have options, according to their circumstances and needs, to engage with government. Finding the best channels to reach communities is a key part of the government's engagement efforts.

Further, although Canada bases its public engagement strategy on threat actors' behaviour and not on their targets, government tries to tailor its engagement to the needs and circumstances of particular communities. According to the government witnesses, it is therefore important that each

agency builds its own relationship with the public. In my view, this is a good approach, but it cannot obfuscate the need for the government to quickly develop a coherent and comprehensive communications strategy.

Security and intelligence and law enforcement agencies try to engage with the public, including diaspora communities, in a variety of ways:

- The Communication Security Establishment's Canadian Centre for Cyber Security ("**CCCS**") and the RCMP have recently made efforts to increase their presence on social media.
- CSIS and CCCS are trying to increasingly include specific and detailed information about foreign interference in their public-facing products.
- The RCMP, CCCS and CSIS have made efforts to translate some of their products into languages other than French or English.
- The RCMP is trying to be more present at local community events.

The above agencies also engage in more formal processes for communication. For example, Public Safety and the Department of Justice co-lead the Cross-Cultural Roundtable on National Security, a group of community representatives who educate government on their communities' concerns and are consulted on potential policy initiatives. The government also saw the two rounds of consultations that it led on Bill C-70 as a way for it to engage with the private sector, community organizations and diaspora communities.

A large part of government engagement, however, happens through informal calls, meetings and messages. Some witnesses mentioned that informal engagement is sometimes more effective in building trust and may allow more people to voice their opinions.

Tricia Geddes, then the Associate Deputy Minister of Public Safety,[29] described ongoing engagement and communication on foreign interference as one of the most effective tools the government has to disrupt foreign states' efforts that target vulnerable communities. Other witnesses agreed, adding these engagements foster greater awareness of the tools available to the public to protect themselves and the resources government has to counter foreign interference. It also encourages members of the public to report potential foreign interference. I heard that ongoing relationships enable the sharing of information with the public, which in turn may increase resilience.

Concerns or issues raised by the public can inform the government's understanding of the foreign interference threat. For example, CSIS said important aspects of its understanding and reporting on foreign interference comes from members of diaspora communities. CSIS views such relationships as critical to maintaining and supporting its operational work. Global Affairs Canada said information from individuals can inform foreign policy development. I heard that feedback from the public is important because it allows government to modify its practices where necessary.

---

[29] Tricia Geddes became the Deputy Minister of Public Safety on 31 October 2024.

The importance of rebuilding public trust was a constant theme in the evidence before me, especially in relation to diaspora communities. CSIS witnesses acknowledged that the agency must overcome distrust from members of diaspora communities, who may have been the victims of problematic treatment in the past by law enforcement or security and intelligence agencies in Canada.

Government witnesses said some community members still distrust government to some extent, but believed that, through a long process of frequent encounters and meetings, the trust gap is being bridged. They pointed to widespread support for Bill C-70 as an indicator of this.

I also heard about the impact of the *Countering Foreign Interference Act*. With its new disclosure authority, CSIS may be able to look differently at the way in which it provides information to entities or individuals outside of the federal government.

However, even with the amendments to the *Canadian Security Intelligence Service Act*, public engagement will continue to present challenges. I heard testimony about work to ensure that government produces more information at the unclassified level to facilitate this.

I heard from former and present-day senior CSIS officials that the agency had a history of defaulting to high levels of protection for classified material. However, CSIS witnesses also spoke about CSIS moving to a "sunlight" policy to be more transparent with Canadians about foreign interference. According to one witness, CSIS now understands it needs to be able to share information to better protect Canadians and build trust.

These are good intentions, but a more formal and organized plan is needed. Up until now, communication with the general public has, in my view, been lacking. Annual reports and other documents posted to government websites are not enough, particularly if the websites themselves are not user-friendly. I recognize that in a world oversaturated with information, capturing public attention is not easy. But creative solutions must be found. I will return to this in my recommendations.

16.4 Conclusion

Sharing information about foreign interference outside of the federal level presents a challenge for the federal government. But other levels of government are equally vulnerable to foreign interference and have a crucial role in combatting it, given the constitutional division of powers. Similarly, effective public engagement and communication are critical. These should be areas of focus for the government moving forward.

CHAPTER 17

Transnational Repression

Information may be incomplete: *intelligence products are discussed in many areas of this public report. Please note that this report includes only relevant information that can be appropriately sanitized for public release in a manner that is not injurious to the critical interests of Canada or its allies, national defence or national security. Additional intelligence may exist.*

17.1 Introduction

There is currently no legal definition of transnational repression in Canada. The Canadian Security Intelligence Service ("**CSIS**") describes transnational repression as foreign state activity to monitor, intimidate and harass diaspora communities in Canada to achieve its objectives. It has also been described as the practice of foreign powers reaching across borders in an attempt to intimidate, silence or harm their perceived critics, typically dissidents, refugees, human rights activists and minority groups, and exert control over them. Transnational repression threatens an individual's freedom to engage in legitimate democratic practices, and threatens to undermine democratic society and the sovereignty of states, including Canada.

I heard testimony from government witnesses recognizing the seriousness of the threat that transnational repression poses to diaspora communities, the Canadian public and Canadian society overall. I agree with them. This is a significant threat, that seems to be growing in the current geopolitical context.

Royal Canadian Mounted Police ("**RCMP**") witnesses said transnational repression was one of the most prevalent types of foreign interference related threats in Canada. David Morrison, current Deputy Minister of Foreign Affairs and former Acting National Security and Intelligence Advisor to the Prime Minister, believes the real foreign interference threat to Canada is not foreign actors targeting parliamentarians to gain influence, which garnered so much public attention, but rather transnational repression. David Vigneault, former CSIS Director, has publicly said transnational repression is one of the greatest strategic challenges to Canada's sovereignty and democracy.

In my view, it would be challenging to overstate the seriousness of transnational repression, or the impact it has on individuals and our social fabric.

17.2 Transnational Repression and the Commission's Mandate

Not all transnational repression activities were within my mandate of examining foreign interference in Canadian democratic processes. Because of this, the Commission did not investigate transnational repression directly or comprehensively; this would have been beyond its mandate and resources.

However, the Commission's Terms of Reference did direct me to examine and assess supports in place for members of vulnerable diaspora communities who may be victims of foreign interference in Canada's democratic processes. While doing so, I heard evidence on transnational repression that impacts democratic institutions. Moreover, given the importance of transnational repression as an issue, the degree of public attention that it has received, and its potential, in some circumstances, to impact our democracy, I wanted to better understand it. I therefore obtained information about transnational repression that was not directly tied to democratic institutions.

In this chapter, I describe the evidence related to transnational repression that I heard. In Volume 6, Chapter 21, I also summarize what I heard from members of the Canadian public through the Commission's public consultation process about their experiences of transnational repression and the serious impacts that it has on their lives.

17.3 Transnational Repression Threat Actors and their Tactics

I heard that assessing the extent of transnational repression in Canada is difficult. Targeted individuals are often reluctant to report their experiences. Although the RCMP monitors transnational repression, it understands that these activities are likely under-reported. People may fear reprisals against them or their relatives abroad if they speak out. They may believe that security agencies will not be able to investigate activities that originate from abroad (e.g. online harassment) or from foreign mission personnel protected by immunities (e.g. diplomats), nor will they be able to lay charges against the perpetrators of such activities. Many targeted individuals come from communities who, for both cultural and historical reasons, may distrust law enforcement and security agencies.

CSIS officials described foreign states undertaking transnational repression activities in Canada as falling into different categories based on their goals, intent and methods. Some may have an interest in interfering in Canadian democratic processes, but others do not.

States such as Iran, among others, focus on repression of dissidents and foreign nationals living in Canada. These countries have shown little interest in interfering with Canadian democratic processes. Their transnational repression activities may include information collection, digital harassment, physical threats and violence. The Canadian Centre for Cyber Security assesses that Iranian and Saudi Arabian state-sponsored cyber threat actors have almost certainly monitored diaspora populations and activists using cyber tools and judge it very likely that these actors are targeting individuals in Canada.

The People's Republic of China ("**PRC**") and India also engage in repressive activities against communities, political dissidents and human rights defenders, but also show an interest in interfering in Canadian democratic processes.

I provide further information on transnational repression carried out by some of these states below. The list of countries is not exhaustive and should not be read as indicating that no other country engages in transnational repression in Canada.

Iran

Iran is not, nor has it been historically, a significant foreign interference threat actor in relation to Canadian federal elections. However, Iran is assessed to be a significant transnational repression threat because of the intensity of its activities, which are mostly conducted with cyber tools.

Intelligence reporting indicates that officials from Iran are likely monitoring, influencing and collecting information on, harassing and intimidating the Iranian diaspora in Canada to prevent criticism of Iran. For instance, I heard that Iran sought to discourage relatives in Canada of Flight PS752 victims from criticizing it. This involved online and digital threats, contact by Iranian government officials, possible cyber intrusions to gain access to a network or device and coercion and intimidation of family members located in Iran.

Iran also relies on criminal groups to carry out many of its activities outside of Iran against Iranian dissidents.

The People's Republic of China

The PRC harasses, intimidates and seeks to sanction people throughout the world for the purpose of forced return to the PRC. The PRC uses a wide range of tradecraft to carry out its transnational repression activities. It collects human source intelligence, conducts online monitoring and cyber intrusions, controls mobility and carries out coercion-by-proxy. It also uses harassment and threats of violence, forced repatriations and physical violence. When PRC authorities have no direct means to carry out transnational repression activities, the Internet becomes their preferred tool. The PRC is effective in using existing and new technologies, namely artificial intelligence. Another strategy is using a person's family living in the PRC as leverage against the person who is in Canada.

The PRC uses a wide range of actors to engage in foreign interference. The United Front Work Department ("**UFWD**"), a department of the Chinese Communist Party, attempts to control and influence the Chinese diaspora.

The evidence shows the PRC has especially directed transnational repression, which includes harassment and other threats, to individuals affiliated with groups that the PRC has labelled the "Five Poisons," which are communities the PRC considers particularly threatening: Falun Gong practitioners, Uyghurs, Tibetans, supporters of Taiwanese independence and prodemocracy advocates focused on mainland China and from Hong Kong.

More than any other country, the PRC is good at concealing its transnational repression. To carry out these activities, the PRC uses, among others, its diplomatic missions, PRC students, community organizations and private individuals affiliated with the UFWD or the Ministry of State Security.

The PRC sometimes uses subnational government entities for both legitimate and illegitimate purposes, making it harder for Canadian security and intelligence agencies to detect its transnational repression activities.

India

India's transnational repression activities in Canada are mainly targeted at the approximately 800,000 Sikh diaspora community members.

Since the 1985 Air India tragedy, India has pressured Canada to adopt a stronger stance against Canadian Sikhs who support establishing "Khalistan," which the Canadian government defines as a separate homeland for Sikhs on the Indian subcontinent. According to CSIS, India has some legitimate basis for concerns about the security threat posed by Khalistani extremism in Canada. Some extremists have engaged in threat-related activities directed at India from within Canada, notably by coordinating and funding terrorist activities in India. However, according to CSIS, the vast majority of Khalistan supporters are peaceful.

While Canada has consistently cooperated with India to address cases of actual or threatened terrorism based on credible evidence, this issue continues to cause significant tension in Canada-India relations. Moreover, India and Canada have opposing viewpoints on peaceful pro-Khalistan protests in Canada and on what constitutes protected free speech. This has furthered tensions.

In this context, India's transnational repression activities aim to promote a pro-India and anti-Khalistan narrative in Canada.

India's transnational repression activities include information collection and monitoring of individuals of interest and undermining support for Canadian policies related to issues such as Pakistan and Khalistani extremism. India also engages in foreign interference that seeks to counter activities by diaspora communities that it views as counter to its national interests, such as lawful and public advocacy for issues such as an independent Khalistan. Information collected by India, directly or through proxies, is used to target members of the South Asian community.

The RCMP's October 2024 statement about violent criminal activity occurring in Canada with connections to agents of the Government of India is consistent with the classified evidence available to me on India's increasingly aggressive and violent activities. Further, India aspires to build a modernized cyber program. The national security and intelligence community assesses India to be an emerging cyber threat actor.

17.4 Canada's Response to Transnational Repression

Although this was not the focus of the Commission's investigation, I heard evidence about the government's attempts to respond to transnational repression. These efforts necessarily encompass transnational repression that falls outside of my mandate. However, they also encompass transnational repression that may have direct or indirect impacts on our democratic institutions. It is through that lens that I briefly discuss the government's response below.

Public Safety Canada ("**Public Safety**") is working with other government departments and agencies to develop policy advice on transnational repression.

The National Counter Foreign Interference Coordinator ("**NCFIC**") explained his mandate includes responding to transnational repression. The NCFIC told me he was bringing a transnational repression action plan to the Deputy Minister of Public Safety for consideration. He has established an Interdepartmental Working Group on Transnational Repression, which brings

together many departments, not just law enforcement or security and intelligence agencies. In his view, this is essential to combatting transnational repression given the complexity of the issue. For instance, the NCFIC explained that both Immigration, Refugees and Citizenship Canada and the Canada Border Services Agency can be involved in efforts to screen individuals who might have links to the United Front Work Department (UFWD) before they enter Canada.

In 2022, Public Safety re-established the "Cross-Cultural Roundtable." This forum was created after 9/11, bringing together different communities to discuss radicalization, but it fell into disuse at some point. Shawn Tupper, the former Deputy Minister of Public Safety, considers it an opportunity to hear the perspectives of different communities and receive advice on how Public Safety can improve its work.

In its engagement with diaspora groups, CSIS has established a hotline for anonymous reporting on foreign interference. CSIS also has protocols so that it can respond quickly in the event that it learns of a threat against an individual or community. According to CSIS, it can be difficult to assess the impact that transnational repression has on diaspora communities and, in particular, whether it impacts participation in democratic processes.

While the Communications Security Establishment ("**CSE**") does not have a domestic mandate, some of their cyber operations have repercussions for transnational repression. For example, CSE has conducted cyber operations designed to target transnational repression activities of foreign entities that have an impact in Canada.

Global Affairs Canada ("**GAC**") has made efforts to address transnational repression. One of the four Rapid Response Mechanism ("**RRM**") working groups established in 2023 was dedicated to transnational repression. In July 2023, it began working to develop a definition for transnational repression. GAC also hosted a Human Rights Forum in Ottawa focused on transnational repression by the PRC. In April 2023, GAC hosted a public event on transnational repression at Toronto Metropolitan University. GAC has also frequently raised the issue in its diplomatic engagements with certain countries, including the PRC.

In 2024, the Department of Canadian Heritage's Digital Citizen Initiative funded projects to understand the PRC's transnational repression in Canada. One project looked at how transnational repression campaigns and foreign-influenced disinformation from the PRC impact social inclusion in Canada. The tools developed under this project were eventually deployed in different languages across Canada. Another project, "Strengthening Community Resilience to Foreign Interference," focused on building a better understanding of PRC foreign interference, including its targeting of Chinese Canadians.

To protect the ability of members of diaspora communities to participate in elections, Elections Canada publishes voting guides addressed to voters available in 51 languages and engages with diaspora communities through various mechanisms. The initiatives are intended to provide information to people who may not be familiar with Canada's electoral process, and to provide information about electoral integrity, such as the secrecy of the vote and different ways of voting.

The government also works with allies to discuss global responses to transnational repression. For instance, at the June 2022 G7 Summit, leaders issued the Resilient Democracies Statement, which committed to building resilience against transnational repression that seeks to undermine trust in government, society and media.

17.5 Examples of Transnational Repression Activities in Canada

As I noted earlier in this chapter, witnesses gave several notable examples of transnational repression in Canada that, while not necessarily directly related to democratic institutions, provided valuable insight into the kinds of clandestine and threatening activities that some foreign states are engaged in within Canada. This testimony was important in its own right, and also helped contextualize other evidence I heard about foreign interference.

In this section, I discuss two examples of transnational repression that were given during the public hearings.

PRC overseas police stations

In September 2022, the Spanish nongovernmental organization Safeguard Defenders published a public report alleging that the PRC had established over 50 "overseas police stations" in 29 countries including Canada. The report said that the PRC used overseas police stations to harass, intimidate and punish individuals around the globe with the aim of returning "fugitives" to the PRC.

GAC, Public Safety, the RCMP and CSIS discussed this report. Subsequent investigations confirmed there were overseas police stations operating in Canada. CSIS shared information about these with the RCMP. The Prime Minister's Office was briefed on the issue in October 2022. It was also discussed at a deputy minister-level meeting.

The Assistant Deputy Minister for the Indo-Pacific at GAC explained that the PRC is very good at engaging in grey zone activities. These activities can have a dual purpose—both legitimate and illegitimate.

For instance, intelligence reporting indicates that overseas police stations performed a number of functions not directly related to transnational repression, including providing government administrative services like driver's licence renewals. These services may have been useful to community members during the COVID-19 pandemic when travel restrictions limited their ability to travel to the PRC.

That said, these stations were also used to carry out transnational repression. Subnational PRC officials appear to have spearheaded these stations to leverage diaspora populations to carry out UFWD strategies, gather intelligence and facilitate transnational repression—possibly without the knowledge or approval of national PRC authorities.

The overseas police stations therefore illustrated how community organizations could be used as effective tools for the PRC to engage in transnational repression under the guise of providing useful services.

GAC's Assistant Deputy Minister for the Indo-Pacific explained however that, from an international law perspective, even if they had not been involved in transnational repression, the PRC had violated its obligations under the *Vienna Convention on Consular Relations* by operating these stations in Canada. The stations were operating without Canada's agreement, which is not permitted. As such, in his view, the PRC needed to be held accountable for these stations.

The stations presented challenges to the government's ability to use traditional tools to respond. Certain operations of the stations were run by Canadian citizens. Expelling those responsible from Canada was not an option as it would have been with respect to foreign state officials.

The RCMP instead chose to respond by using disruption tactics. They deployed uniformed officers to the stations to make their presence known and engage with the local community directly and by publishing materials. The RCMP told me this disruption tactic contributed to closing the overseas police stations, despite no charges being laid. Former Deputy Minister of Public Safety Shawn Tupper said this was an example of how disruptive activities may sometimes be as effective as prosecution.

Diplomacy also played an important role in Canada's response. There were multiple senior level interactions with the PRC Embassy between October 2022 and April 2023 on foreign interference. In each interaction, GAC officials raised Canada's concerns about the overseas police stations with their PRC counterparts.

On 7 October 2022, GAC asked the PRC Ambassador for detailed information about the overseas police stations and enjoined him to end any activities not permitted by the *Vienna Convention on Consular Relations*. On October 28, GAC issued a diplomatic note to the PRC insisting that the overseas police stations be shut down. On November 30, GAC received an official notice from the PRC Embassy indicating that what the PRC referred to as the "overseas Chinese centres" were no longer in operation. However, this appears not to have been true.

Throughout 2023, GAC's RRM Canada analyzed the types of services provided by newly identified PRC stations around the world, building on the work done by Safeguard Defenders. Based on this research, on 24 February 2023, GAC again demanded that the PRC close any stations still operating in Canada.

Throughout the fall of 2022 and into early 2023, GAC liaised with like-minded countries to share information and consult on how other countries planned to respond to the stations. There were high-level engagements with certain leaders and foreign ministers at the East Asia Summit, G20 and Asia Pacific Economic Cooperation meetings to increase international awareness of the extent of PRC foreign interference.

During the public hearings, I heard a wide range of views on the RCMP's actions. A community member who participated in a Commission consultation panel described the RCMP's response as irresponsible and damaging to vital community institutions.

Conversely, one Commission Participant suggested to RCMP witnesses that the response to the overseas police stations was too "diplomatic," and therefore distinguishable from how the RCMP responds to other organized crime. The RCMP witnesses disagreed with this framing of their response. They stated that they have taken similar approaches in other investigations, also recognizing that in this case it was particularly important to build a trust relationship with members of the Chinese Canadian community, who were the victims of the criminal activities being investigated.

Given that this matter exceeds the scope of the Commission's mandate and in light of ongoing investigations, I do not consider it expedient to make any specific findings.

Assassination of Hardeep Singh Nijjar

Hardeep Singh Nijjar was assassinated on 18 June 2023 in Surrey, British Columbia.

A link between the Government of India and the killing of Mr. Nijjar

There were immediate rumours that Mr. Nijjar's death was somehow linked to the Government of India, but that was not the initial read of Canada's

intelligence and security agencies. The initial assessment was that the killing was gang or criminal related, and the Prime Minister was informed of this.

However, Canadian officials began hearing from a number of South Asian members of Parliament and other members of the South Asian community who were insistent that the killing was connected to India. A number of media articles also alleged that the Government of India was involved and that it was possible retaliation for the killing of Ripudaman Singh Malik a year earlier. Mr. Malik had been prosecuted for having contributed to financing the Air India bombing but was acquitted of the charges in 2005.

In light of what they were hearing, intelligence agencies continued to investigate the circumstances of the killing.

Over the course of the summer, intelligence revealed the Government of India's involvement in the killing. Then-CSIS Director David Vigneault briefed the National Security and Intelligence Advisor, Jody Thomas, about this. Within an hour of this briefing, she informed the Clerk of the Privy Council, John Hannaford. The Prime Minister was then promptly briefed on the updated assessment.

The government's response

The government wanted India to acknowledge its involvement in the assassination, but also needed a pragmatic approach to resolve the issue.

The Prime Minister testified that the government's immediate approach was to engage with the Government of India and communicate that it was necessary for the two countries to work together while ensuring there was accountability. Canada also reached out to its allies to ensure a collective and coherent response.

Ms. Thomas had a meeting already scheduled with her Indian counterpart, Ajit Doval, in August 2023. She and other Privy Council Office officials met with Mr. Doval, as well as the heads of India's intelligence agency and internal police bureau, and officials from their foreign affairs department. This was a formal meeting; Ms. Thomas had a script that set out what she could say about the investigation. She believed that Mr. Doval and his colleagues absolutely understood that Canada knew this was an extrajudicial killing and was calling out India for its role in killing Mr. Nijjar.

When Minister Mélanie Joly became aware of the intelligence in August 2023, she began voicing Canada's concerns to her Indian counterpart, with three primary objectives: shedding light on the nature of India's involvement, protecting the safety of Canadians and protecting Canadian sovereignty.

In September 2023, Mr. Vigneault, Ms. Thomas and Mr. Morrison went to India for the G20 Summit, which India was hosting. Canada had originally planned to take advantage of the Summit to improve bilateral relationships with India. Mr. Nijjar's assassination derailed that plan. Instead, just prior to the Summit, they met with their counterparts to try to get India to cooperate with the investigation.

Ms. Thomas said that during her second meeting with Mr. Doval, they both had scripts. She wanted to signal that Canada knew that India had been involved in the killing while still protecting the integrity of the ongoing RCMP investigation.

Mr. Morrison told his counterpart that it was highly likely the truth would eventually come out through the Canadian investigation, the unsealing of an indictment in the United States or a media leak.

Mr. Vigneault delivered his script *verbatim*. His objective was to situate this event within the broader context of previous instances in which CSIS had advised that Canada was aware of India's foreign interference activities and considered them problematic. India did not acknowledge that it was involved in killing Mr. Nijjar.

Prime Minister Trudeau described the G20 summit as a "big moment," where the government worked behind the scenes to try and continue to get India to cooperate with it. This culminated in a conversation between the Prime Minister and Narendra Modi, the Prime Minister of India, after the last session of the G20 Summit. The Prime Minister told Mr. Modi that Canada knew India was involved, and that this would likely become public. Mr. Modi responded that Canada had people that India wanted to see arrested, and asked Canada to share the intelligence it had about the killing.

Media reporting on Mr. Nijjar's assassination

Soon after the G20 Summit, the government received information that led it to believe India's involvement would soon be leaked in the media. The government determined that it should tell Canadians it was aware of allegations about India's involvement and was investigating them in the interest of public safety. Canada consulted its allies before making this declaration.

On 18 September 2023, the *Globe and Mail* published an article saying that Canadian officials had information about potential Indian involvement in Mr. Nijjar's death. Following the publication of that story, the Prime Minister announced in the House of Commons that Canadian security agencies had been actively pursuing credible allegations of a potential link between agents of the Government of India and the killing of Mr. Nijjar.

Declaring an Indian diplomat *persona non grata*

At the same time, Canada declared an Indian diplomat *persona non grata*.

India responded by declaring a Canadian official, *persona non grata* and also lifted the diplomatic immunity of 41 Canadians in India, effectively expelling them. Witnesses described India's response as extreme. As a result of the immunity of its diplomats being lifted, Canada shut down its three consulates in India.

RRM Canada also detected a disinformation campaign targeting Prime Minister Trudeau, Canada's High Commission to India, Canada's national security and intelligence agencies, Canada's Sikh diaspora and Mr. Nijjar's political beliefs. Several media outlets aligned with the Indian Prime Minister amplified this campaign. The posts included narratives that the Prime Minister and Canadian institutions were "enablers of terrorism" and "treacherous against Bharat (India)."[30]

The Prime Minister commented that this was a situation where there were clear indications that India had violated Canada's sovereignty—but when confronted, the Government of India's response was to double down and attack Canada further.

The government's continuing response

GAC said Canada continues its work to hold the individuals responsible for Mr. Nijjar's assassination accountable. An RCMP investigation into the matter is ongoing, and four individuals were arrested in May 2024.

The question of Indian foreign interference and transnational repression evolved in rather dramatic fashion during the Commission's public hearings.

On 14 October 2024, in the midst of the hearings, the RCMP publicly released findings with respect to the involvement of agents of the Government of India in serious criminal activity in Canada.

Simultaneously, GAC announced that Canada had expelled six Indian diplomats and consular officials following a campaign against Canadian citizens by agents linked to the Government of India. The six individuals were identified as persons of interest in Mr. Nijjar's assassination.

The Prime Minister said the decision to make this announcement was anchored in public safety considerations, with the objective of disrupting the chain of criminal activities with ties to India, primarily targeting the Sikh community in Canada, and the covert collection of information by Indian diplomats about Canadians opposed to the Government of Mr. Modi.

The challenge of attribution

The events described above are a good illustration of how difficult it can be to make a decision about whether, when and how to publicly attribute foreign interference activities to a particular state. There are a lot of considerations at play, and the consequences can be severe.

[30] CAN025923: Rapid Response Mechanism Canada, *Potential Foreign Information Manipulation and Interference following PM Statement on Killing of Hardeep Singh Nijjar* at p. 1.

17.6 Conclusion

As I noted above, the Commission's Terms of Reference did not direct me to conduct an in-depth study of transnational repression in Canada. Thus, the work that the Commission did in this respect likely only scratches the surface of this phenomenon.

What the Commission's work has made clear to me, however, is how serious a problem transnational repression is, how harmful its impacts are on individuals in Canada and how important it is for the government to meaningfully respond to it.

Any effective response to foreign interference must take into account the realities of transnational repression that some states carry out in Canada.

In my view, the government must look even closer at transnational repression and the serious impacts that it can have on some Canadians. It is a complex issue.

CHAPTER 18

The House of Commons Motion on the NSICOP Report

Information may be incomplete: *intelligence products are discussed in many areas of this public report. Please note that this report includes only relevant information that can be appropriately sanitized for public release in a manner that is not injurious to the critical interests of Canada or its allies, national defence or national security. Additional intelligence may exist.*

18.1 Introduction

On 3 June 2024, the National Security and Intelligence Committee of Parliamentarians ("**NSICOP**") published a redacted public version of its *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* ("**NSICOP Report**"). The impact of this report on the public discussion surrounding foreign interference was immediate. This was due in large part to the fact that it contained assertions that some elected officials were "semi-wittingly" or "wittingly" assisting foreign states. These assertions led to significant concern in the media, the public and in the halls of Parliament itself.

I was asked by the House of Commons to investigate the assertions made in the NSICOP Report. This was a particularly challenging task.

I wish to begin by emphasizing the obvious. The NSICOP Report is the culmination of a significant amount of very important work. It is an impressive and detailed synthesis of a vast amount of information. And it has made a considerable and valuable contribution to advancing public awareness of foreign interference. Nothing I say in this chapter should be interpreted as detracting from any of that.

In conducting the investigation requested by the House of Commons, the Commission reviewed the classified version of the NSICOP Report and the intelligence that NSICOP considered in drafting it. The Commission then undertook the task of producing a publicly disclosable summary of the assertions in the NSICOP Report about parliamentarians "semi-wittingly" or "wittingly" assisting foreign states. This summary was entered into evidence at the Commission's public hearings.

The Commission also reviewed considerable additional information that NSICOP did not have, including the raw intelligence and operational reporting underlying the materials NSICOP relied on. The Commission obtained further written information from the government and conducted *in camera* examinations of Canadian Security Intelligence Service ("**CSIS**") and senior Privy Council Office ("**PCO**") officials.

This aspect of the Commission's investigation proved eye-opening. What I learned was both surprising and insightful. The most important observations I made during the NSICOP Report investigation had to do with the nature of

intelligence – what it is, and what it is not, how it should be used, and how it should not.

Intelligence can evidently be extremely valuable in informing government, enabling it to develop policy and respond to threats. But there are inherent limits to what intelligence can do, and how it should be communicated. The frailties of intelligence make it dangerous to rely on unquestioningly. This is particularly true for intelligence that may suggest misconduct by individuals, such as the involvement of parliamentarians in foreign interference activities. Intelligence should never be treated, or reported, as though it were undisputed fact. And, importantly, intelligence on its own should not be used to pass judgment on individuals who have no opportunity to defend themselves.

The fact that the NSICOP Report, even the classified version, does not name the individual parliamentarians to whom it refers shows an understanding of, and regard for, these concerns.

However, the NSICOP Report nevertheless makes strongly worded and unequivocally stated allegations against individual parliamentarians. These assertions had the (perhaps unintended) effect of causing widespread public consternation, casting a cloud of suspicion over all parliamentarians (especially those from diverse backgrounds) and contributing to the erosion of Canadians' trust in their democratic institutions. This may in part be because few people are familiar with the limitations of intelligence – that is to say, what it is and what it is not, and how it should, and should not, be used.

The Commission's investigation led me to conclude that the consternation caused by the NSICOP Report, while understandable, is in some important respects unwarranted. The situation is perhaps neither as clear-cut, nor as extreme, as the fears provoked by the NSICOP Report would suggest.

In my view, some of the findings in the NSICOP Report regarding the "witting" participation of individual parliamentarians in foreign interference activities were more definitive than the underlying intelligence could support. They also sometimes contained inaccuracies, either in the way the intelligence was described, or because of inaccuracies in the intelligence itself.

To be clear, this does not mean that the conduct reported is not concerning. There are legitimate concerns about parliamentarians potentially having problematic relationships with foreign officials, exercising poor judgment, behaving naively and perhaps displaying questionable ethics. But I did not see evidence of parliamentarians conspiring with foreign states against Canada. While some conduct may be concerning, I did not see evidence of "traitors" in Parliament.

My ultimate take-away from this aspect of my investigation is that great care must be taken when using intelligence to draw conclusions about individuals, and even more when reporting this publicly.

18.2 The House Motion

On 6 March 2023, the Prime Minister asked NSICOP to complete a review to assess the state of foreign interference with respect to the 2019 and 2021 general elections. NSICOP decided to conduct a broader review into foreign interference in federal democratic processes and institutions, which included both parliamentarians and the parliamentary process.

On 22 March 2024, NSICOP produced its classified report and submitted it to the Prime Minister. On 3 June 2024, it released a redacted, public version of the Report.

The public version contained assertions that generated significant public concern. For example, it stated that "[s]ome elected officials (…) began 'wittingly' assisting foreign state actors soon after their election" and that it had "seen troubling intelligence that some Parliamentarians are, in the words of the intelligence services, 'semi-witting or witting' *participants* in the efforts of foreign states to interfere in our politics."[31] This latter assertion is followed by five examples of this type of participation.

These assertions caused widespread public outcry, which included accusations of "traitors" in Parliament and demands for the Government to identify the "witting" elected officials referred to in the NSICOP Report who assisted foreign states.

Against this backdrop, the Bloc Québécois tabled a motion in the House of Commons ("**House Motion**"). The House Motion was adopted on 11 June 2024. It called for an expansion of my mandate to address some of the findings of the NSICOP Report. The motion read:

> That the House:
>
> (a) take note of the Special Report on Foreign Interference in Canada's Democratic Processes and Institutions of the National Security and Intelligence Committee of Parliamentarians;
>
> (b) express concern that certain elected officials may be wittingly or unwittingly working in the interests of foreign powers; and
>
> (c) request the terms of reference of the foreign interference commission (the Hogue Commission) to be expanded to investigate Canada's federal democratic institutions, including members of the House of Commons elected in the 43rd and 44th Parliaments as well as Senators.[32]

[31] COM0000363: NSICOP, *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* at paras. 55, 164.

[32] Canada, House of Commons, *Journals*, 44th Parl., 1st Sess., No. 329 (11 June 2024) at pp. 4150-4152.

On 17 June 2024, the Commission took note of the House Motion and indicated that it would conduct the requested investigation. However, no change to the Commission's Terms of Reference was needed. The Commission conducted the investigation under its existing Terms of Reference.

18.3 The Commission's Investigation

The Commission's mandate

It is important to understand the Commission's specific mandate regarding the NSICOP Report.

Much has been said in the Commission's public hearings, the media and Parliament, about naming, in the public interest, the parliamentarians referred to in the NSICOP Report. I take this opportunity to explain why this would not be in the public interest, and why I am not divulging those names.

From the outset, I would like to dispel the notion that the classified NSICOP Report contained a list of names of parliamentarians who are suspected of working in the interests of a foreign state. It does not. The NSICOP Report does not name individual parliamentarians.

The classified NSICOP Report contained several statements describing the conduct or activities of unnamed parliamentarians, and footnotes referring to the intelligence products from which the information provided by NSICOP was taken. Thus, identifying the individuals to whom NSICOP referred was an exercise in "reverse-engineering," not only for the Commission, but even for CSIS when it reviewed the NSICOP Report.

As I explained in Volume 2, Chapter 3, the Commission's mandate was not to attempt to expose and identify specific individuals or organizations as alleged foreign interference agents. The mandate was to examine and assess Canada's capacity to detect, deter and counter foreign interference in its democratic institutions, including electoral processes. This involved examining the government's intelligence holdings about the potential foreign activities of various hostile state actors, including their interactions with elected officials, and assessing the government's response. It did not include passing judgment on the culpability of any elected official.

Indeed, judging culpability of an elected official or of any other person would violate the Commission's legal obligations and the requirements of procedural fairness. Section 13 of the *Inquiries Act* prohibits the Commission from making a report against a person (that is, a finding that would bring discredit on the person or be unfavourable to their reputation) unless that person has been given notice of the misconduct alleged against them and a

full opportunity to be heard in response. If the Commission investigated specific parliamentarians with the possibility of stating in its report that they had been wittingly involved in foreign interference, it would be legally required to give those parliamentarians advance notice, access to the evidence against them and an opportunity to respond. This was never my mandate.

Further, this section 13 procedure would be impossible to follow when the information is based on highly classified intelligence. Indeed, even the fact that the NSICOP Report referred to a particular parliamentarian's conduct would be classified. Disclosing this, let alone details about the allegations themselves, could potentially reveal the investigative capabilities of CSIS to adversaries and could put sources at risk. This would violate the Commission's obligation to prevent disclosure of information where this could be injurious to the critical interest of Canada or its allies, national defence or national security. It could even constitute a criminal offence under the *Foreign Interference and Security of Information Act*.

In addition, the Commission is obliged by its Terms of Reference to ensure that its work does not jeopardize any ongoing criminal investigation or proceeding, or any other investigation. The Commission's investigation pursuant to the House Motion complied with this obligation, as does my reporting of it here.

The Commission's process

Before turning to my findings, it is important to understand what the Commission did to investigate the assertions in the NSICOP Report.

The Commission's first step was to carefully review both the classified and unclassified versions of the NSICOP Report. This was done to identify assertions relevant to the House Motion, i.e. statements regarding federal parliamentarians who may be wittingly or unwittingly allegedly working in the interests of foreign powers. The Commission did not investigate other assertions in the NSICOP Report, such as assertions regarding non-federal politicians. Although the NSICOP Report did discuss this, among other important subjects, the House Motion did not ask the Commission to examine those subjects.

The Commission focused on identifying assertions that current or former federal parliamentarians "wittingly" (with knowledge) or "semi-wittingly" (with partial knowledge or willful blindness) acted in the interests of foreign states. I refer to these as the "identified assertions."

Each of the identified assertions in the NSICOP Report has a footnote reference. In July 2024, the Commission asked the government to identify the documents referred to in the footnotes, as well as any other documents already produced to the Commission that were relevant to the identified assertions. The Commission also requested and obtained the underlying intelligence reporting cited in or relied on by the documents referred to in

each footnote, as well as any additional relevant intelligence or information that had not yet been produced to the Commission. The Commission asked for the underlying intelligence, including operational reporting, because it needed to see the information in as "raw" and detailed a form as possible. This would allow it to properly assess the assertions in the NSICOP Report.

This process enabled the Commission to examine everything that NSICOP looked at when preparing the NSICOP Report, and more. As I discuss below, careful review of the intelligence resulted in the Commission identifying discrepancies between what the intelligence said and what the NSICOP Report said. In some cases, the information in the intelligence was simply wrong, or errors were made in assessing it.

After its initial review of the documents, the Commission requested additional information in writing from the government about each identified assertion. The information requested included how the intelligence was disseminated, both within and outside CSIS, and any action taken in response to this intelligence. The Commission also asked the government to identify, and produce if it had not already done so, intelligence that supported specific aspects of each identified assertion. In addition, the Commission asked the government to answer more specific questions about certain assertions and related intelligence.

The Commission then examined senior officials from CSIS and the Privy Council Office (PCO) *in camera* about the information and intelligence related to the identified statements, as well as about the investigations that generated the intelligence. Before its public hearings in September and October 2024, the Commission produced summaries containing as much information as national security considerations allowed to be disclosed publicly about these examinations. The highly classified information involved made this an enormous challenge. I am pleased that the Commission was able to meet it. This allowed the Commission and Parties to examine senior CSIS and PCO representatives on the NSICOP Report, to the extent possible, during the Commission's public hearings in October.

18.4 Observations on Intelligence

The nature of intelligence

Intelligence is an important tool that allows Canada to develop responses to national security threats. Intelligence may assist with policy development, inform diplomatic responses and guide investigations. Intelligence may provide individuals or groups with situational awareness and equip them to build resilience against threats.

However, the Commission's investigation, including its investigation of the assertions in the NSICOP Report, served as a reminder that intelligence has limits. The conclusions that can be drawn from intelligence are limited, for instance, by what has been collected and how that collection was done. As valuable as intelligence is, it has inherent frailties. These frailties make it dangerous to rely on intelligence unquestioningly, particularly when making conclusions about individuals. Intelligence should never be treated, or reported, as though it were undisputed fact.

Loss of accuracy and nuance when intelligence is summarized

One notable benefit the Commission had in reviewing the NSICOP Report was that it could trace the reporting of intelligence across multiple intelligence products. The Commission could see how information was presented in operational reporting, and how it evolved as it moved to intelligence reports, to more refined assessments, to external reviews like the classified NSICOP Report and to sanitized public documents like the unclassified NSICOP Report. This exercise gave the Commission insight into the very real challenges involved in ensuring the accuracy of information as it moves through these steps, from the classified to the public domain.

At the operational level, information is collected as a building block to add to the government's understanding of a threat actor's activities or to determine the next steps that should be taken as part of an investigation. As raw intelligence is used to build more refined intelligence products, the government can gain important context and a more complete picture can emerge. However, the evolution can also go the other way, stripping away subtlety, nuance and precision. This is the inevitable consequence of summarizing information.

As I have learned, this problem becomes exponentially worse when information goes through national security review for release to the public. As one CSIS witness testified, this process inevitably removes detail, results in a loss of context and leads to abstraction. It is not lost on me, for example, that due to security concerns I can only discuss the NSICOP Report's assertions in general, abstract terms here, without the specifics and details available to the Commission. Indeed, this is the case for many subjects discussed in this report. But it is a particular challenge here, as it limits the extent to which I can explain what I saw, and it greatly increases the risk that a reader will not be able to understand, or will misinterpret, what the evidence actually showed.

This does not make public reporting worthless. Far from it. Public reports can do much to advance public understanding of foreign interference.

But we cannot ignore the reality that, in moving from the classified to the unclassified space, detail, context and nuance can be lost. The end product is inevitably incomplete and necessarily omits relevant information. There is a very real danger that it can be misleading. This has been a concern for me throughout the Commission's proceedings, and one that the Commission has worked extremely hard to try to avoid. I can only hope, not guarantee, that we have succeeded.

Difficulties in assessing the "wittingness" of parliamentarians

When interpreting intelligence reports related to foreign interference and parliamentarians, it is critically important to understand that parliamentarians are rarely the actual subjects of the foreign interference investigations conducted by CSIS. Thus, CSIS generally collects information about a parliamentarian's potential involvement in foreign interference incidentally to its investigations of foreign threat actors. This may sound like a technical point, but it has significant consequences. I have also learned that this point is often missed in the discourse about the potential involvement of parliamentarians in foreign interference.

That parliamentarians are rarely the subjects or focus of investigation matters for at least two reasons.

First, it means that there will be gaps in what CSIS knows about a parliamentarian's potential involvement in foreign interference activities. Because parliamentarians are generally not the subject or focus of the investigation, CSIS has limited information about them. To illustrate what this means in practice, I offer an example entirely unrelated to foreign interference.

Consider a police investigation into an alleged criminal organization. The police can use a wide range of techniques to target the organization. These include wiretaps, undercover officers, confidential informants, public surveillance and social media monitoring. These techniques may show that members of the criminal organization believe a certain public official is vulnerable to being corrupted.

This would be useful intelligence about the organization under investigation. It tells the police something about the organization's nature and intent. The organization would appear to be interested in committing crimes and specifically in targeting a public official.

But what does this say about the public official? That is much more difficult to determine. Perhaps it means that the official is open to corruption. Or perhaps not. It could just as easily be that the criminals are mistaken, and that the public official is beyond reproach. Because the police are not targeting the public official, they are less likely to have information that sheds light on the public official's motives, objectives, intentions or actions. They know a lot about the criminal organization – but very little about the public official.

With intelligence about foreign interference, the targets and methods might be different, but the basic point is the same. Parliamentarians are generally not the focus of intelligence investigations, so intelligence holdings about foreign interference will have gaps about the motives and actions of the parliamentarians involved.

Second, and related to the first point, when CSIS obtains information about parliamentarians potentially engaging in foreign interference activities, it does not necessarily assess the "wittingness" of the parliamentarian. That is not the goal of the CSIS investigation. The goal is to understand the activities of the foreign threat actor. This is a very important caveat to keep in mind when considering the assertions in the NSICOP Report. In most of these cases, CSIS made no assessment whether the parliamentarian in question "wittingly" participated in foreign interference. "Wittingness" was generally NSICOP's conclusion, not CSIS's.

18.5 Discussion of the Assertions in the National Security and Intelligence Committee of Parliamentarians (NSICOP) Report

With these above observations about the nature of intelligence in mind, I move to a consideration of the NSICOP Report itself.

The "wittingness" of parliamenarians

As I noted above, CSIS does not always assess the "wittingness" of parliamentarians. Below, I describe two conclusions about a parliamentarian's wittingness in which the NSICOP Report went further than CSIS did.

In one assertion, the NSICOP Report described what it called "a textbook example of foreign interference that saw a foreign state support a witting

politician."[33] NSICOP referred to a briefing document to support this allegation. That briefing document does not refer to this incident as a "textbook example of foreign interference." Another document related to this allegation, but not footnoted in the NSICOP Report, does describe this incident as a "textbook example of foreign interference," but does not describe the member of Parliament ("**MP**") as a "witting politician."

In a written response to the Commission, CSIS said that the extent to which this MP was aware of all the details, or that they constituted foreign interference, was an intelligence gap. CSIS assessed that the politician was aware of and had accepted the assistance of a foreign state. But CSIS did not assess that the politician was wittingly engaging in foreign interference. This nuance, and the gap acknowledged by CSIS, are important.

Elsewhere, the NSICOP Report discussed what it described as examples "of members of Parliament who worked to influence their colleagues on India's behalf and proactively provided confidential information to Indian officials."[34] In discussing one such example, CSIS told the Commission that it had not actually made an assessment of the wittingness of the MP in question. CSIS witnesses emphasized that CSIS did not necessarily assess the conduct or wittingness of parliamentarians, as it was the foreign states who were being assessed. Information about parliamentarians was collected incidentally, not because the parliamentarians were being investigated as threats.

In my view, the NSICOP Report went too far in making assertions about the wittingness or complicity of parliamentarians.

I recognize that NSICOP, as a committee of parliamentarians, considered the information before it from the viewpoint of parliamentarians commenting on the behaviour of their colleagues who they considered to have crossed a line. However, in my view, these conclusions went beyond what the available intelligence could support. But I also recognize that I did not consider the information from the same perspective as NSICOP. My focus was solely on what the intelligence revealed.

Errors in the intelligence itself

It is always important to recognize the risk that the intelligence is simply wrong. This is why the Commission repeatedly heard, and has repeatedly stated, that just because something is reported in intelligence does not make it fact. Information from human sources may not be reliable. It is often hearsay at best. The possibility for human error is considerable. Moreover, sources can have motivations to fabricate or incentives to say what they think

[33] COM0000363: National Security and Intelligence Committee of Parliamentarians, *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* at para. 56.

[34] COM0000363: National Security and Intelligence Committee of Parliamentarians, *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* at para. 55.

the intelligence agencies want to hear. Even technical sources, such as intercepted private communications, are rife with the possibility of errors resulting from misinterpretation, inaccurate translation, lack of context and other factors. Intelligence professionals are, of course, trained to assess the reliability of such information, but this is easier said than done.

A clear example of inaccurate intelligence came to light in the Commission's investigation of one identified assertion in the NSICOP Report. NSICOP reported that an elected official proactively provided confidential information to Indian officials at a particular time.[35] This was an extremely grave allegation, particularly because the information in question was significant.

However, while investigating this allegation, the Commission discovered that at the time the elected official allegedly provided the confidential information, it had already been made public by the government. In other words, if the official did in fact provide the information to Indian officials, that information was not confidential at all at the time. On the contrary, it had already been shared with the public.

To be clear, this is not an error that NSICOP could have avoided. The CSIS document that NSICOP relied upon contained the same error. In the 2022-2023 CSIS classified annual report to the Minister of Public Safety, which NSICOP relied on for this assertion, CSIS described this incident and indicated that the information in question was confidential. During the course of the Commission's *in camera* hearings and follow-up communications, CSIS eventually agreed that it appeared that the information in question was not confidential at the time it was allegedly communicated, and that CSIS had no indication that the elected official shared confidential information.

Another example of inaccurate intelligence – unrelated to NSICOP's investigation –surfaced during the Commission's proceedings. As I described in Volume 3, Chapter 10, the Commission asked the government to list and describe all major instances of suspected foreign interference targeting Canada's democratic processes from 2018 to the present. As I explained in that chapter, the original list included seven suspected instances. The seventh instance was, however, eventually removed when CSIS identified publicly available, irrefutable information that disproved the central claim of this intelligence. I note that the disproven information came from sources considered to be reliable. I note this example to reinforce the crucial point that intelligence can sometimes simply be wrong.

[35] COM0000363: National Security and Intelligence Committee of Parliamentarians, *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* at para. 55.

Intelligence is a mosaic and a moving target

Intelligence is like a mosaic, a jigsaw puzzle or sometimes even a Jenga tower. It consists of individual pieces that are snapshots, moments in time – a partial conversation here, a source report there. Only when these components are put together does a fair, accurate and coherent picture emerge. One piece of intelligence may suggest one inference or conclusion, but combined with additional information, the inference that can be drawn or conclusions that can be reached may change significantly. Relying on a single piece of intelligence without a broader appreciation of the context in which it arises, risks leaving a reader with a distorted, or even misleading understanding of a situation. Much of the value that the intelligence assessment process adds for decision-makers comes from providing context to the reader. As former CSIS Director Vigneault testified, it is important to understand intelligence in its context.

Equally important is that intelligence is a moving target. It is dynamic, not static. Intelligence is collected at a point in time. How that intelligence is understood at any moment depends on what is known at the time it is being considered. As additional information comes to light, the way in which the intelligence is understood may change dramatically. Assessments can become more definitive in their conclusions, or much less so. Changes may occur over years, but they may also occur overnight. One CSIS witness told me that one day it may seem like an individual is compromised, but the next day CSIS may uncover another piece of information that changes this assessment.

I heard evidence from CSIS witnesses that, if CSIS assesses an MP's activities, this assessment occurs on a "sliding scale" as CSIS continues to collect incidental information about their activities. It can be challenging to appreciate this when reporting on intelligence at a single point in time. But this appreciation is crucial for a proper understanding of what conclusions can, and cannot, be fairly drawn.

Two situations described in this chapter demonstrate how new information can fundamentally change the understanding of previously obtained intelligence.

As explained above, the "seventh instance" of suspected foreign interference identified by the government was based on intelligence from sources that were considered reliable. Yet in this case, information readily available in the public domain resulted in a re-evaluation of the suspected instance and its removal from the list.

CSIS explained that it did not verify the intelligence in relation to the "seventh instance" because the MP was not the subject of the investigation. I note that since parliamentarians are very rarely subjects of investigation, this means that most of the information collected about them is equally likely to be unverified.

Similarly, there is the case of the parliamentarian who CSIS said had allegedly provided "confidential" information to India. This conclusion had to be re-assessed when the Commission pointed out that the information in question had already been made public at the time, and therefore was not confidential. CSIS drew inferences from the information it received and did not consult readily available open source information before concluding that the parliamentarian had passed on confidential information.

Errors in the description of intelligence

In some cases, there are errors in the NSICOP Report's description of what the intelligence actually said.

For example, the NSICOP Report describes two instances where a single MP was alleged to have assisted a specific foreign state.[36] In describing the second instance, the classified NSICOP Report states that it involved the same MP as in the first instance. As a result, NSICOP concluded that a single MP conducted the activities described in both instances.

However, based on the NSICOP Report's footnoting, as well as other intelligence available to the Commission, these two assertions do not appear to relate to the same MP. The intelligence reports related to the second instance referred to a different MP. This is noteworthy because a reasonable person would likely be more confident that an MP had engaged in misconduct if NSICOP described two distinct instances of that MP potentially aiding a foreign state.

In another example, the classified NSICOP Report states that an MP had been compromised by a particular foreign state. The report uses particular language to describe the compromise. The accompanying footnote cites an intelligence product. The intelligence product does use the particular language cited in the NSICOP Report, but it does so in reference to a different foreign state than the one the NSICOP Report identifies. In other words, NSICOP had the wrong country.

Moreover, there is a more fundamental problem in NSICOP's reporting of the intelligence about this MP. The NSICOP Report indicates that the particular language referred to above represented the assessment of the MP by CSIS – or, said otherwise, that CSIS had assessed the MP as compromised. This was not the case. Rather, in an intelligence product that NSICOP reviewed, CSIS reported the language used by a third party, not by CSIS. "Someone told CSIS the MP was compromised" is very different from "CSIS assessed that the MP was compromised."

---

[36] COM0000363: National Security and Intelligence Committee of Parliamentarians, *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* at para. 55.

In another example, the NSICOP Report describes interactions between a parliamentarian and an individual who was described as "an undeclared intelligence officer" for a foreign state. The reference to the intelligence officer as "undeclared" requires a brief explanation. A declared intelligence officer in Canada is someone occupying a legitimate posting by a foreign government with the knowledge of Canada. An undeclared intelligence officer is a spy.

When the Commission reviewed the intelligence relied on by NSICOP, it learned that the individual NSICOP described as an undeclared intelligence officer – i.e. a spy – was actually a *declared* intelligence officer, i.e. a legitimate foreign official. While the intelligence officer's status was not known by the whole world (which is normal), CSIS acknowledged that it is likely the parliamentarian did know. Thus, the NSICOP Report stated that the parliamentarian had spoken to a foreign spy, but in fact, the parliamentarian had spoken to a legitimate foreign official. This makes a difference.

Another example involves what the NSICOP Report referred to as a "particularly concerning case of a then-member of Parliament maintaining a relationship with a foreign intelligence officer." The NSICOP Report adds that, "[a]ccording to CSIS, the member of Parliament sought to arrange a meeting in a foreign state with a senior intelligence official and also proactively provided the intelligence officer with information provided in confidence." While this is not in the public NSICOP Report, the classified NSICOP Report also described the information at issue as "privileged." On its face, providing confidential, privileged information to a foreign intelligence officer does seem particularly concerning.

However, when the Commission investigated this assertion, it discovered there was no indication that the information was actually confidential or privileged. CSIS confirmed that the information was in fact unclassified, and that it was not legally privileged. Moreover, CSIS did not know whether the MP had ever been told to keep the information in confidence. This paints a rather different picture than suggested in the NSICOP Report.

CSIS witnesses said they viewed the information as sensitive and considered it a red flag that the MP chose to share this information with a foreign official. However, CSIS told the Commission that the NSICOP Report used stronger language than CSIS would have used to describe the situation.

As for the assertion that the MP sought to arrange a meeting in a foreign state with a senior intelligence official, the Commission was unable to investigate this because so little information was available about it. The Commission requested that CSIS produce any additional information on this matter. None was provided. Given that the Commission received all the reporting provided to NSICOP, the NSICOP Report's conclusion was likely based on the same limited information. This is an important consideration, given the seriousness of the allegation.

The Commission also identified newer information held by CSIS that provided additional and important context about the relationship between the MP and the intelligence officer, and why the two may have been in contact. This information was not available to NSICOP. I mention it only because it is in my view relevant to a proper appreciation of the assertions about this MP.

18.6 Intelligence and the Challenge of Due Process

As I said above, the main conclusion I drew from my investigation of the assertions in the NSICOP Report is that there are inherent limits to what intelligence can do and how it should be used.

Intelligence is evidently useful for responding to national security threats, and critically important for developing government strategies. Even if national security and intelligence agencies do not have all the information to form a complete picture of a particular threat, there may be enough information to usefully inform government. The government can then act to manage risk. Pieces of intelligence may allow a government department to put into context other information they hold or to ask different questions about the information it receives from other sources. Government agencies employ experts who know how to assess information while taking into account its limitations.

But this does not mean that all intelligence should be used for all purposes. Rather, intelligence must be used responsibly, taking into account its limitations, particularly when acting upon intelligence will have direct and significant impacts on an individual.

I return to an observation I made at the start of this chapter. In reviewing the NSICOP Report, it would have been inappropriate for me to adjudicate the guilt or innocence of particular parliamentarians. For sound reasons related to national security and due process, I could not disclose the names of those who I believe are referred to in the NSICOP Report. I could not speak with them and give them the opportunity to understand the allegations made against them. I could not obtain information from them that might support or refute other intelligence I may have seen. I could not give them a fair opportunity to be heard. In short, a fair process would have been impossible to implement.

Because of this, it would be fundamentally unfair for me to pronounce on whether a particular parliamentarian may have engaged in misconduct in association with a foreign state.

This speaks to a broader concern about fair treatment. Any time the government acts on the basis of classified information, there is a risk that its actions will impact the rights or interests of individuals. Some impacts may be minor or diffuse. Others may be profound and direct. These consequences, and the fact that individuals can be given little, if any, opportunity to defend themselves, must be taken into account when acting on intelligence.

For example, a prime minister may quite properly make decisions about who to appoint to Cabinet by relying on the kinds of intelligence identified in the NSICOP Report. No individual has a right to be a Cabinet minister. I do not say this to minimize the impact that such a decision could have on an individual's career or aspirations, but because the interests at stake on both sides of the ledger would make such a decision defensible.

That being said, I heard evidence about times when intelligence agencies provided the Prime Minister with intelligence about MPs that affected their careers, and that intelligence turned out to be completely wrong. Indeed, the Prime Minister's Chief of Staff described an instance where an intelligence agency had identified a threat linked to an MP. Officials from the Prime Minister's Office asked questions about the intelligence. After requesting further verification of the information, CSIS realized it had the wrong person and completely changed its assessment.

Examples like these demonstrate why it would be entirely unfair to rely on untested intelligence to publicly label an individual parliamentarian a traitor. This would have a profound impact on the individual, one that could not be justified in light of the frailties of intelligence and the inability to give them a fair opportunity to defend themselves.

NSICOP's reluctance to name MPs, even in its classified NSICOP Report, demonstrates commendable attention to these due process concerns. But the NSICOP Report does use language that may have been interpreted as definitive statements that numerous MPs have wittingly collaborated with foreign states against the interests of Canada. The focus is on the MPs, as if they, rather than the foreign states, are threat actors. It is written as though intelligence were proof of fact. And it does not acknowledge that the Committee has no information from the parliamentarians in question. The overall effect of this is to suggest (perhaps unintentionally) that some parliamentarians are effectively "traitors" to their country. In my view, this goes much further than the intelligence suggests.

I came away from this aspect of the Commission's investigation reflecting on the challenge faced by bodies like NSICOP, the National Security and Intelligence Review Agency ("**NSIRA**"), the Independent Special Rapporteur on Foreign Interference ("**ISR**"), and indeed, this Commission. They are asked to review, investigate and report on the conduct of individuals. None of these bodies are designed to be courts that would adjudicate on the basis of intelligence whether individuals are guilty or innocent, liable or not. To be sure, they can – and must – make judgments about the conduct of public institutions. But passing judgment on individuals is very different. Intelligence,

on its own, cannot be a basis for such a conclusion. Commissions of inquiry that do not have to deal with intelligence may be better equipped to consider the conduct of specific individuals. Because such commissions can offer greater procedural fairness, they are better positioned to reach conclusions about the conduct of individuals (though still not their liability). But bringing intelligence into the mix changes the game. Intelligence is complex, nuanced and almost invariably incomplete.

Intelligence is also inherently secret. Bodies like NSIRA, NSICOP, the ISR or this Commission can work to promote openness and transparency. But they cannot provide full disclosure or grant due process to those whose conduct intelligence has called into question. They can question and probe the conduct of intelligence agencies, their assessments and their conclusions. But they cannot purport to pass judgment on those individuals when fairness dictates that they should have a right of reply.

Review bodies are extremely important and valuable actors in Canada's national security architecture. Each one brings its distinct set of skills, authorities and abilities to the vitally important shared goal of ensuring accountability and transparency. I hope that the work of this Commission will help contribute to the enormous efforts they have made.

When conducting an investigation or writing a report, we must be mindful of our strengths, but also of our weaknesses. We must take seriously the limits of what we can accomplish. This includes ensuring that we do not try to do more than our institutional competence and capacity permit.

18.7 The Government Response

In the course of my investigation, I received and heard evidence on the government's response to the intelligence underlying the identified assertions. I am limited in what I can say about the specific actions the government took in response to individual allegations. However, the evidence indicates that, where appropriate, certain steps were taken to reduce the threat of foreign interference activities. For instance, I heard evidence regarding an allegation that Pakistan worked to support a preferred candidate's election. Relevant information about this was shared with both Elections Canada and the Office of the Commissioner of Canada Elections because the intelligence may have indicated a violation of the *Canada Elections Act*. It could also provide context to improve those bodies' understanding of the methodologies of certain states. I also heard about a specific threat reduction measure ("**TRM**"), as well as the outcomes of that TRM, that CSIS used to respond to some of the intelligence related to the identified assertions. Of course, the efficacy of such steps is difficult to measure.

That said, more can and should always be done. In particular, this part of my investigation highlighted the need for ongoing and increased communication with parliamentarians about foreign interference. The intelligence should not be overstated and must be read with significant caveats in mind. Still, it does suggest that some elected officials have maintained relationships, or had interactions, with foreign officials that may have crossed the line beyond normal diplomacy. The intelligence also indicates that some elected officials may have knowingly received support from foreign officials or proxies, although the extent to which they were aware of the foreign interference nexus was not necessarily clear.

To be clear, this does not mean that these elected officials are "traitors." But it does suggest, at a minimum, that some elected officials may not have known where or how to draw the line between foreign interference and acceptable diplomatic activity. Indeed, I heard evidence about one TRM undertaken by CSIS that clearly exposed a lack of awareness of foreign interference among Canadian politicians, and further indicated that some elected officials may not have known that foreign officials should not be undertaking certain activities.

I also heard evidence from CSIS witnesses that some elected officials know what foreign interference is but may be unsure about where the line is drawn. A November 2021 intelligence assessment further indicates that "[o]ne of the greatest challenges for MPs appears to lie in correctly identifying [foreign interference] and recognizing what to do when they believe they are being targeted," as many interactions between MPs and foreign officials fall within the grey zone between legitimate foreign influence and illegitimate foreign interference.[37] This lack of awareness may make MPs vulnerable to exploitation by foreign states.

Elected officials are not unique in facing the challenge of identifying what is and is not foreign interference. As I discuss in Volume 3, Chapter 10, different government departments and agencies can come to different conclusions about whether a set of facts constitutes foreign interference and, if it does, how serious the interference is.

In light of this challenge – one that impacts even those government officials well versed on the subject – we cannot expect elected officials to be able to easily draw the line between foreign interference and foreign influence without further guidance. As I discuss further in **Chapter 15**, one of the government's tools to counter foreign interference lies in educating parliamentarians. My investigation into the identified assertions in the NSICOP Report has shown the importance of this. Additional information for parliamentarians about the distinction between foreign interference and acceptable diplomatic activity, for example, may help bridge the gaps in knowledge and foster resiliency among them if targeted by foreign interference activities. I will return to this in my recommendations.

---

[37] CAN003712_R01: Canadian Security Intelligence Service, *CSIS Engagement with Elected Officials on Foreign Interference: An Initiative of National Significance*, CAB 2021-22/89 (3 November 2021) at p. 5.

18.8 Conclusions about the National Security and Intelligence Committee of Parliamentarians (NSICOP) Report

The NSICOP Report has made an important contribution to the public's understanding of foreign interference. It identifies legitimate areas of concern. However, the public discourse over the past several months, as well as the testimony of witnesses and submissions of Participants in the Commission's proceedings, suggest that these allegations have contributed to an erosion of public trust in elected officials and Canada's democratic institutions more broadly. This is both regrettable and unwarranted.

The scope of the problem

To be clear, the fact that I have concerns about the assertions of witting participation in foreign interference in the NSICOP Report does not mean that the conduct of individuals referred to was irreproachable. Some information in the intelligence may be cause for concern or may justify further investigation. I heard evidence from CSIS witnesses that they believe there are and have been some relationships of concern between elected officials and foreign states. As the National Security and Intelligence Advisor to the Prime Minister, Nathalie Drouin, explained, even if the conduct does not amount to an MP being a traitor, this does not mean that their behaviour should not be considered or addressed.

As I note above, parliamentarians lacking awareness of foreign interference, being unsure about where the line is drawn or showing poor judgment or poor ethics, are problems worthy of attention and concern.

However, the concern with former and current elected officials must not be overstated. While some behaviour may be concerning, I did not see evidence of "traitors" in Parliament. Former Director of CSIS David Vigneault testified that there have been very few times in CSIS's history where an MP has been suspected of posing a threat to the national security of Canada due to their ties to a threat actor. Vanessa Lloyd, CSIS's Deputy Director of Operations, emphasized that the number of individuals who understand what foreign interference is and knowingly benefit from such relationships with foreign states is very small. This level of "wittingness" is very rare. Based on what I have seen, there is nothing to suggest I should disagree.

The NSICOP Report was right to raise concerns about foreign interference targeting parliamentarians. This is unquestionably a real issue. But based on the intelligence I reviewed, and the evidence I heard, the problem is perhaps less widespread and less dramatic than the public discourse following the NSICOP Report would suggest.

The impact of the NSICOP Report

Serious public discussion about national security issues in Canada has been minimal in the past. As I said, NSICOP has made an important contribution to raising the profile of, and advancing, these issues. I agree with the Clerk of the Privy Council, John Hannaford, that having a group like NSICOP dive into issues like foreign interference is part of an important ongoing process of building collective resilience to the threat. NSICOP provided Canadians with a significant amount of information about foreign interference. Indeed, I note that most of the information in the NSICOP Report did not relate to allegations about specific parliamentarians.

Unfortunately, the comments about parliamentarians attracted the greatest public attention, with troubling consequences. This is particularly true for MPs who are members of certain diaspora communities. For instance, I heard evidence from MP Jenny Kwan – herself an alleged victim of foreign interference – that the Report has cast a cloud of suspicion on parliamentarians. She described walking by the House of Commons on her way to a committee hearing and being confronted by protestors calling parliamentarians, including her, “traitors.” As Ms. Kwan explained, the issue with the cloud of suspicion, beyond the personal ramifications, is that the integrity of Parliament itself is called into question. And undermining democratic institutions and elected officials is exactly what threat actors want.

Conclusions on the Government's Capacity to Detect, Deter and Counter Foreign Interference

The Order in Council establishing the Commission first directed me to examine and assess interference by China, Russia and other foreign states or non-state actors, including any potential impacts, in order to confirm the integrity of, and any impacts on, the 43rd and 44th general elections (the 2019 and 2021 elections) at the national and electoral district levels.

This examination was carried out mainly during the first phase of the Commission's work. As a result of this work, I concluded in my Initial Report that the 2019 and 2021 general elections were without a doubt subject to foreign interference. However, I found that this interference did not undermine the integrity of the electoral system itself, nor did it have any bearing on which party came to power. While it was difficult to ascertain whether or not this interference had any bearing on results of elections at the riding level, I acknowledged the possibility that it did, but only in a small number of ridings.

The Commission's work since the tabling of the Initial Report has not altered these conclusions. Nor has it led me to alter my conclusion that foreign interference had an impact on the electoral ecosystem as a whole and has undermined public confidence in Canadian democracy. Indeed, my work since the initial report has only reinforced this conclusion.

The Order in Council also directed me to examine and assess the flow of information to senior decision-makers, including elected officials, and between the Security and Intelligence Threats to Elections Task Force ("**SITE TF**") and the Critical Election Incident Public Protocol panel during the election periods leading up to the 43rd and 44th general elections, in the weeks following those periods and actions taken in response. I have done this.

The evidence presented to me did not reveal any particular issues with the way in which information flowed during these periods. With the exception of one report that was not passed on to the SITE TF in a timely fashion, the way in which information flowed was satisfactory.

The Order in Council also directed me to examine and assess the capacity of relevant federal departments, agencies, institutional structures and governance processes to permit the Government of Canada to detect, deter and counter any form of foreign interference directly or indirectly targeting Canada's democratic processes, including:

- the creation, sharing, assessment and distribution of intelligence and the formulation of advice to senior decision-makers, including elected officials
- the supports and protections in place for members of a diaspora who may be especially vulnerable and may be the first victims of foreign interference in Canada's democratic processes
- the mechanisms that were in place to protect the integrity of the 43rd and 44th general elections from foreign interference as compared to those in place in previous recent federal elections that I determined to be relevant.

My review has shown that some of the processes through which intelligence was supposed to be passed to senior officials had some shortcomings. Information that should have reached ministers and even the Prime Minister did not. I was unable to ascertain from the evidence exactly why this happened in each case. The evidence did show, however, that the systems in place at the time were not particularly robust. There was no way of knowing who had received a particular report, whether those who had received it had read it and whether any action had been taken as a result.

In some cases, the impression that emerges from the evidence is that the various persons involved in the process felt they had fulfilled their duties as soon as they had delivered the information, without otherwise making sure that it had been received and understood.

I have no evidence to suggest that anyone acted in bad faith. The shortcomings observed appear to have been systemic ones, the consequences of which were exacerbated by various external factors, including the COVID-19 pandemic, which required a significant reorganization of work. Clearly, this reorganization of government work was in several ways less than optimal.

Fortunately, the intelligence delivery system has since been completely redesigned. I have not been able to put this new system to the test to see how effective and resilient it is, but the evidence suggests that it is much more suitable than the previous one. In my view, the government will have to monitor the system very closely and measure its effectiveness on a regular basis.

Of course, when information did not reach the person who would have been in a position to act on it, I could not assess the adequacy of any government response to it. If information does not reach a decision-maker, it cannot be acted upon.

I was nevertheless able to examine and assess several measures taken in response to information that was received relating to foreign interference. My observation is that the significance attributed to this information has fluctuated significantly over the years, indicating that the government has been slow to fully recognize the threat posed by foreign interference to Canadian democratic processes and institutions.

The government apparatus has reacted much more swiftly in recent years, although it still has some way to go. Governments, because of their size, are not generally known for their ability to react quickly. I appreciate that. Nevertheless, foreign interference is an increasingly prevalent and rapidly evolving phenomenon. The government needs to find ways of reacting more swiftly. The restructuring the government has undertaken of its national security governance system, which has reduced the number of committees directly engaged in combating foreign interference from approximately a dozen to five, is a step in the right direction. But it is also important not to let endless discussions and consultations get in the way of action. The machinery of government must facilitate action, not paralyze it. Among the various measures put in place by the government, the establishment of a National Counter Foreign Interference Coordinator should, I hope, go a long way towards achieving this.

As part of my assessment of the government's ability to detect, deter and counter foreign interference in democratic processes, my mandate required me to examine the mechanisms in place to protect the integrity of the 43rd and 44th general elections from foreign interference, compared with those in place to protect the integrity of previous federal elections. I should mention that it was difficult to conduct this comparative review. Aside from some mechanisms to protect electoral infrastructure, there were virtually no specific measures to protect electoral processes from foreign interference prior to 2017.

Indeed, I gathered from the evidence that it was in the wake of allegations of foreign interference in the US presidential election in 2016, the UK's Brexit referendum on European Union membership in 2016 and the French presidential election in 2017, that Canada began to take a more active interest in foreign interference in democratic processes.

The government of the day acted rather swiftly back in 2017, when the Prime Minister tasked the then Minister of Democratic Institutions with leading the government's efforts to defend Canada's electoral process against cyber threats.

In 2018, the G7 countries, meeting in Charlevoix, agreed to establish the G7 Rapid Response Mechanism to strengthen coordination and better detect threats to democracies. Canada acts as its permanent secretariat.

In 2019, the Plan to Protect Canada's Democracy was announced and implemented. In my opinion, this initiative marks a significant milestone as it both recognizes the risk that our elections might be the target of foreign interference and specifically addresses that risk. The plan was not perfect, but it has since been regularly reviewed and improved, and continues to be used to protect our democratic processes and institutions from foreign interference.

My review of the resources available to the government, with a particular focus on those available to the intelligence community, also leads me to conclude that Canada has the means necessary to detect, deter and counter foreign interference. Some of these means can be improved, of course, but they do exist.

This does not mean, however, that the fight against foreign interference has been won. In fact, it is likely to be an endless fight, as the states that seek to interfere in democracies, including our own, are sophisticated actors who constantly refine their methods.

I also note from the evidence that this threat has evolved and now rears its ugly head through disinformation campaigns in the media and on social networks. This emerging trend is quite concerning because disinformation is especially challenging to combat, and efforts to regulate social media platforms to curb it have been unsuccessful so far. Canada needs to reflect on this threat and find ways of dealing with it. This will probably require a great deal of cooperation between democracies around the world.

In short, the fight against foreign interference requires relentless effort and perseverance. Trust in our democracy depends on it.

In this Final Report, I make a number of recommendations that I hope will also help improve Canada's ability to detect, deter and counter foreign interference.

Finally, I would like to reiterate what I have already said at various points in the Final Report: transnational repression is a scourge that extends beyond the Commission's mandate. It is, however, a form of foreign interference that the government must quickly address. While the government has been doing so for some time, it needs to ramp up its efforts.

ANNEX A

Glossary

Term	Acronym or Abbreviation	Definition
Artificial Intelligence / Generative Artificial Intelligence (Intelligence artificielle/Intelligence artificielle générative)	AI / GenAI (IA / IA générative)	Information technology that performs tasks that would ordinarily require human brain power to accomplish. Generative AI is a type of AI that produces various forms of content such as text, speech or audio, code, videos and images. It learns from existing content and use the patterns and structures to generate new content, based on user inputs.
Assistant Deputy Ministers' National Security Operations Committee (Comité des sous-ministres adjoints sur les opérations de sécurité nationale)	ADM NS Ops (CSMAOSN)	Committee of assistant deputy ministers from across government departments that coordinates operational responses to national security matters.
Attorney General of Canada (Procureur général du Canada)	AGC (PGC)	Chief law officer of government, also the Minister of Justice. • Conducts litigation on behalf of the Government of Canada. • Does not represent individual government departments or agencies but gives them legal advice and legislative services. • Acts in the public interest to uphold the Constitution, the rule of law and respect for independence of the courts.
Cabinet		Political decision-making body chaired by the Prime Minister. Made up of ministers appointed by the Governor General on the recommendation of the Prime Minister (i.e. Cabinet ministers). By convention, Cabinet ministers are usually members of Parliament. They head government departments.

Term	Acronym or Abbreviation	Definition
Canadian Centre for Cyber Security (Centre canadien pour la cybersécurité)	CCCS (CCC)	Part of the Communications Security Establishment (CSE). It is the unified source of expert advice, guidance, services and support on cyber security for Canadians.
Canadian Digital Media Research Network (Réseau canadien de recherche sur les médias numériques)	CDMRN (RCRMN)	Research community in Canada aimed at strengthening information resilience and safeguarding Canadian democracy. The network is coordinated by the Media Ecosystem Observatory (MEO, see definition).
Canadian Heritage (Patrimoine canadien)	PCH (PCH)	Federal government department responsible for promoting Canadian identity and values, cultural development and heritage.
Canadian Radio-television and Telecommunications Commission (Conseil de la radiodiffusion et des télécommunications canadiennes)	CRTC	Public entity in charge of regulating and supervising broadcasting and telecommunications in Canada. The CRTC operates at arm's length from the federal government and implements laws and regulations set by Parliament.
Canadian Security Intelligence Service (Service canadien du renseignement de sécurité)	CSIS (SCRS)	Federal government agency governed by the *Canadian Security Intelligence Service Act*. • Investigates activities suspected of being threats to the security of Canada and reports on these to the government. • Can also take measures to reduce threats to the security of Canada. • Can also render assistance to certain ministers in gathering foreign intelligence within Canada.
Chief Electoral Officer (Directeur général des élections)	CEO (DGE)	Head of Elections Canada. Responsible for running elections and regulatory compliance with election rules. Directly responsible to Parliament, not to the government.
Classified information (Information classifiée)		Information government declares could reasonably be injurious to the national interest if disclosed, as per the following three categories: • Confidential – Limited or moderate injury • Secret – Serious injury • Top Secret – Extremely grave injury

Term	Acronym or Abbreviation	Definition
Clerk of the Privy Council and Secretary to the Cabinet (Greffier du Conseil privé et secrétaire du Cabinet)	Clerk (Greffier)	Senior public servant in the Privy Council Office, who also serves as Secretary to the Cabinet and Deputy Minister of the Prime Minister
Client Relations Officer (Agent des relations avec les clients)	CRO (ARC)	Intelligence official responsible for providing relevant intelligence products to security-cleared officials and staff.
Commission counsel (Avocats de la Commission)		Lawyers who work for the Commissioner on the Foreign Interference Commission.
Commissioner of Canada Elections (Commissaire aux élections fédérales)	CCE (CEF)	Ensures compliance with the *Canada Elections Act* and the *Referendum Act*. Appointed by the Chief Electoral Officer after consultation with the Director of Public Prosecutions of Canada.
Communications Security Establishment (Centre de la sécurité des télécommunications)	CSE (CST)	Federal government agency that provides the government with foreign signals intelligence and is responsible for cyber security and information assurance. The Canadian Centre for Cyber Security is part of CSE.
Compartmented information (Information cloisonnée)		Classified information subject to an additional control system (an administrative framework) that sets standards for access, marking, handling and control of information.
Critical Election Incident Public Protocol (Protocole public en cas d'incident électoral majeur)	CEIPP (PPIEM)	Protocol applied during federal elections by a panel of five senior civil servants (the "Panel" or the "Panel of Five"): • Clerk of the Privy Council • National Security and Intelligence Advisor to the Prime Minister • Deputy Minister of Justice and Deputy Attorney General • Deputy Minister of Public Safety Canada • Deputy Minister of Foreign Affairs Aimed at protecting federal elections from interference, including foreign interference.

Term	Acronym or Abbreviation	Definition
Deepfake (Hypertrucage)		Artificial images, videos or audios that are digitally altered or generated using AI tools.
Defensive Briefing (Breffage sur la sécurité défensive)		See “Protective Security Briefing.”
Democratic Institutions Secretariat of the Privy Council Office (Secrétariat des institutions démocratiques du Bureau du Conseil privé)	PCO-DI	PCO Secretariat that provides policy support and advice to the Prime Minister and the Minister of Democratic Institutions on issues that impact Canadian democratic institutions.
Department of National Defence (Ministère de la Défense nationale)	DND (MDN)	Federal government department that oversees and supports the Canadian Armed Forces.
Digital Citizen Initiative (Initiative de citoyenneté numérique)	DCI (ICN)	Department of Canadian Heritage program formally established in 2020 to combat online disinformation, support democracy and promote a healthy information ecosystem through research and partnership initiatives.
Disinformation (Désinformation)		False or inaccurate information deliberately spread to deceive or mislead. See also “Misinformation”.
Elections Canada (Élections Canada)		Entity responsible for administering federal elections. Headed by the Chief Electoral Officer (CEO). Operates independently from government.
Elections Security Coordinating Committees (Comités de coordination de la sécurité des élections)	ESCCs (CCSE)	Committees of senior government and Elections Canada officials created during federal elections (deputy minister, assistant deputy minister or director general level). Co-chaired by the Privy Council Office and Elections Canada. Ensures a coordinated approach and common understanding among the national security and intelligence community, Elections Canada and the Commissioner of Canada Elections.

Term	Acronym or Abbreviation	Definition
Executive branch (Pouvoir exécutif)		One of three branches of Canada's system of government. The other two are the legislative and judicial branches. Each branch has different powers and responsibilities defined in the Constitution. Executive branch implements laws and policy. Prime Minister and Cabinet are the executive branch of government.
Five Eyes (Groupe des cinq)		Intelligence alliance made up of Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are parties to the multilateral UK-USA Agreement, a treaty for cooperation in signals intelligence. Informally, "Five Eyes" can also refer to the group of intelligence agencies of these countries.
Foreign Interference (Ingérence étrangère)	FI (IE)	For the purpose of the Commission, foreign interference means clandestine, deceptive or threatening activity by a foreign state, or those acting on a state's behalf, that is detrimental to the interests of Canada.
Foreign Interference Commission (Commission sur l'ingérence étrangère)	Commission	Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions.
G7 Rapid Response Mechanism (Mécanisme de réponse rapide du G7)	G7 RRM (MRR du G7)	G7 (Canada, France, Germany, Italy, Japan, the United Kingdom and the United States) mechanism for identifying and responding to foreign threats to democracy. The G7 RRM is coordinated by the G7 RRM Secretariat, which is a part of Global Affairs Canada.
Global Affairs Canada (Affaires mondiales Canada)	GAC (AMC)	Federal government department that manages diplomatic relations, promotes international trade and provides consular assistance. Also leads international development, humanitarian, peace and security assistance efforts as well as contributes to national security and the development of international law.

Term	Acronym or Abbreviation	Definition
Governor in Council (Gouverneure en conseil)	GIC (GEC)	Governor General acting with the advice of the King's Privy Council for Canada. By convention, the Governor General exercises their powers only on the advice of members of the King's Privy Councill which includes members of Cabinet (see definition of "King's Privy Council for Canada"). In practice, the "Governor in Council" is the federal Cabinet and the Governor General. Governor in Council decisions are often formally issued as orders in council.
In camera (Huis clos)		Legal term meaning "in private." For example, *in camera* hearings are hearings without the presence of the public or press.
Intelligence Assessment Secretariat (Secrétariat de l'évaluation du renseignement)	PCO-IAS (SER du BCP)	Strategic intelligence analysis and assessment unit within the Privy Council Office for intelligence collected by security and intelligence agencies. Provides analysis and assessments to the Prime Minister, Cabinet, the Clerk of the Privy Council and Secretary to the Prime Minister and senior government officials.
Inter-departmental Committees (Comités interministériels)		Committees made up of high-ranking officials from different agencies and departments to enhance coordination efforts. Generally exist at the deputy minister, assistant deputy minister and director general levels.
Intervener (Intervenant)		Entity with "standing" (see definition) at the Foreign Interference Commission with limited participatory rights. An intervener is also a Participant. Entitled to notice of the Commission's public hearings and to attend them as a Participant, to make submissions, receive exhibits from the public hearings and other rights if specifically granted by the Commissioner.

Term	Acronym or Abbreviation	Definition
Judicial branch (Pouvoir judiciaire)		One of three branches of Canada's system of government. The other two are the legislative and executive branches. Each branch has different powers and responsibilities defined in the Constitution. The judicial branch interprets and applies the law. The judicial branch is made up of Canada's courts and is independent of government.
King's Privy Council for Canada (Conseil privé du Roi pour le Canada)		Group appointed by the Governor General to advise the King: Cabinet ministers, former Cabinet ministers, the Chief Justice of Canada, former chief justices, former speakers of the House of Commons, former speakers of the Senate, former governors general and distinguished individuals.
Legislative branch (Pouvoir législatif)		One of three branches of Canada's system of government. The other two are the executive and judicial branches. Each branch has different powers and responsibilities defined in the Constitution. The legislative branch makes laws. Parliament (the Senate and House of Commons) is the legislative branch of the federal government.
Media Ecosystem Observatory (Observatoire de l'écosystème médiatique)	MEO	Organization arising from an interdisciplinary collaboration between McGill University and the University of Toronto that studies the health of the media ecosystem. It is the coordinating body of the Canadian Digital Media Research Network (see definition).
Memorandum to Cabinet (Mémoire au Cabinet)	MC	A written document outlining a legislative or policy initiative, used to seek Cabinet approval.
Misinformation (Mésinformation)		False or inaccurate information (not intended to mislead). See also "Disinformation."

Term	Acronym or Abbreviation	Definition
National Counter Foreign Interference Coordinator (Coordonnateur national de la lutte contre l'ingérence étrangère)	NCFIC (CNLIE)	Position created in 2023 to coordinate the government of Canada's policy response to foreign interference. This includes work to enhance transparency in the government's response through public engagement with all Canadians, including diaspora groups, academia, non-governmental organizations as well as other domestic and international partners.
National Security Council (Conseil de la sécurité nationale)	NSC (CSN)	Cabinet committee created in 2023 and chaired by the Prime Minister for strategic decision-making on Canada's interests related to public safety, national security, foreign policy and intelligence issues.
National Security and Intelligence Advisor to the Prime Minister (Conseiller à la sécurité nationale et au renseignement auprès du premier ministre)	NSIA (CSNR)	Senior official who provides policy and operational advice to the Prime Minister and Cabinet on national security matters to ensure coordination of government responses to threats. Receives information from its Secretariats and from the security and intelligence community. Currently has the status of a deputy clerk within the Privy Council Office and reports to the Clerk of the Privy Council and Secretary to the Cabinet.
National Security and Intelligence Committee of Parliamentarians (Comité des parlementaires sur la sécurité nationale et le renseignement)	NSICOP (CPSNR)	Statutory committee composed of members of Parliament and senators governed by the *National Security and Intelligence Committee of Parliamentarians Act*. Reviews government intelligence operations, including the legislative, regulatory, policy, administrative and financial framework for national security and intelligence. Also reviews the activity of any government department relating to national security or intelligence (unless it is an ongoing operation, and the minister determines a review would be injurious to national security) and investigates any matter a minister refers to it about national security or intelligence.

Term	Acronym or Abbreviation	Definition
National Security and Intelligence Review Agency (Office de surveillance des activités en matière de sécurité nationale et de renseignement)	NSIRA (OSSNR)	Statutory review body, external to government, created by the *National Security and Intelligence Review Agency Act* and which reports to Parliament. Reviews and investigates government national security and intelligence activity to ensure it is lawful, reasonable and necessary. Also investigates complaints about key national security agencies and activities.
National security confidentiality (Confidentialité à des fins de sécurité nationale)	NSC (CSN)	Purpose is to restrict access to certain government information and prevent its disclosure in order to protect national security interests.
" Need-to-know " (« Besoin de savoir »)		Term describing a condition that must be met to access to classified information. Even if someone has the necessary security clearance to access a piece of information, they can only access it if it is necessary in the performance of their official duties.
Office of the Chief Electoral Officer (Bureau du directeur général des élections)	OCEO (DGE)	Independent agency made up of Elections Canada and the Office of the Commissioner of Canada Elections (OCCE).
Office of the Commissioner of Canada Elections (Bureau du commissaire aux élections fédérales)	OCCE (BCEF)	Organization led by the Commissioner of Canada Elections (CCE) within the Office of the Chief Electoral Officer (OCEO). In its compliance and enforcement responsibilities under the *Canada Elections Act*, the OCCE acts independently from the OCEO.
Open source (Sources ouvertes)		Information that is publicly available.
Order in council (Décret)	OIC	Legal instrument made by the Governor in Council under statutory authority (or less frequently, the royal prerogative). Always made on the recommendation of the responsible minister of government and only has legal effect when signed by the Governor General.

Term	Acronym or Abbreviation	Definition
Panel of Five or Panel (Panel des cinq)		See "Critical Election Incident Public Protocol."
Participant		Individual or entity with "standing" (see definition) at the Foreign Interference Commission, either a Party or Intervener.
Party (Partie)		Individual or entity with "standing" (see definition) at the Foreign Interference Commission with full rights to participate, including a right to access documents in advance of the hearings and to question witnesses. A Party is also a Participant.
Persona non grata	PNG	Latin term meaning "unwelcome person." In diplomacy, it refers to the practice of a host state requesting a foreign diplomat to leave its territory. When a host state declares a diplomat "persona non grata," it is essentially expelling them from the country.
Prime Minister's Office (Cabinet du premier ministre)	PMO (CPM)	Office responsible for assisting the Prime Minister in carrying out his responsibilities as head of government, leader of a political party and as a member of Parliament. It is made up of political staff and not career public servants.
Privileges		
— Cabinet confidences privilege (Privilège relatif aux renseignements confidentiels du Cabinet)		Protects the confidentiality of discussions taking place within Cabinet. Protection of Cabinet confidences is a common law rule as well as a statutory rule set out in section 30 of the *Canada Evidence Act* and recognized by the *Access to Information Act*. Applies to anyone involved in Cabinet meetings, even if not ministers.
— Litigation privilege (Privilège relatif au litige)		Protects communications (including documents) between a lawyer, their client or a third party created for the dominant purpose of preparing for existing or anticipated litigation.

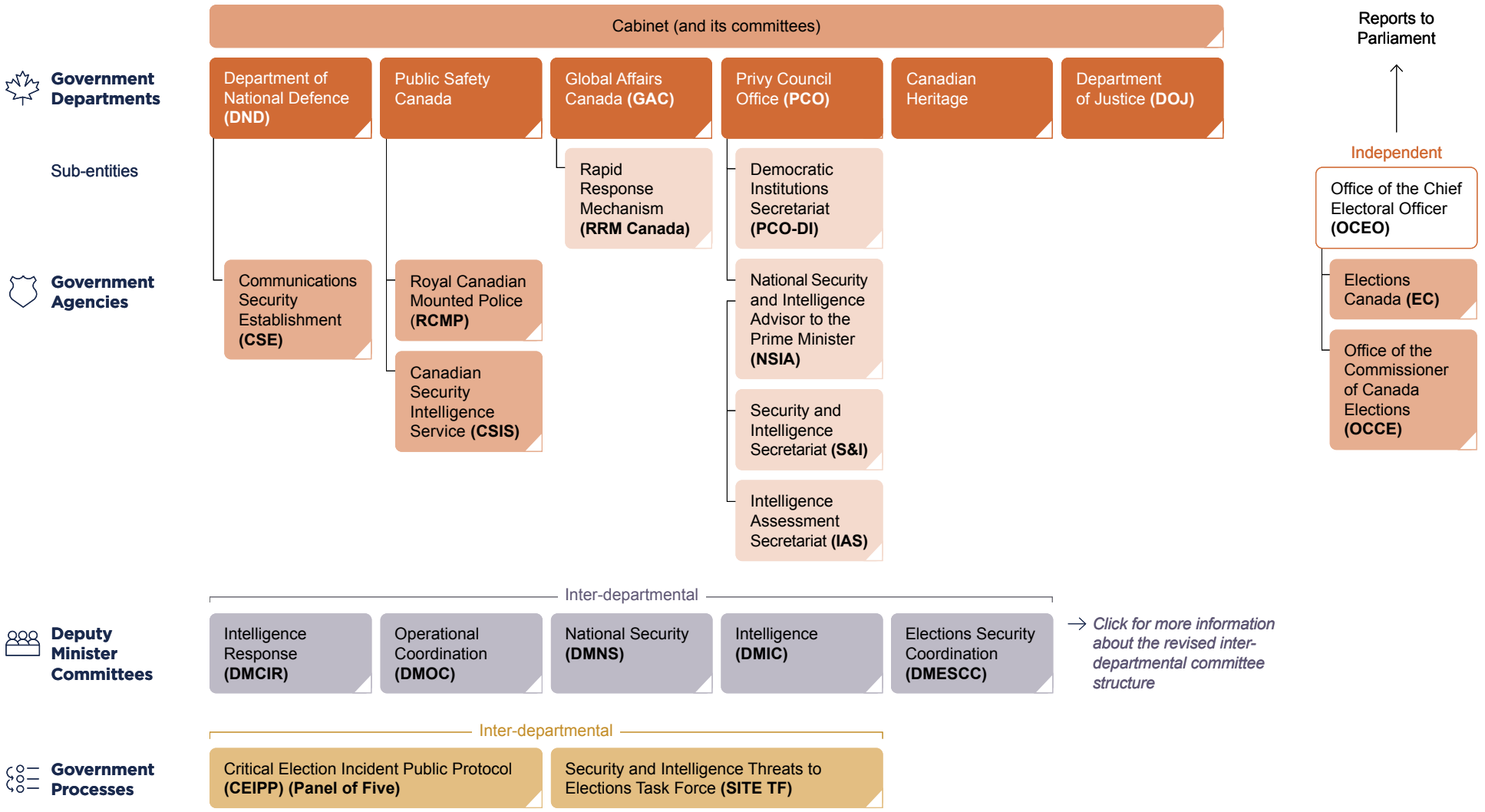
Term	Acronym or Abbreviation	Definition
— Parliamentary privilege (Privilège parlementaire)		Rights and immunities deemed necessary for the House of Commons and the Senate and their members to fulfill their functions. For example: freedom of speech in the House and in committees of the House, and exemption from subpoenas to attend court as a witness. Also, power of the House of Commons and Senate to protect themselves, their members and their procedures from undue interference so they can carry out their principal functions effectively.
— Section 38 of the *Canada Evidence Act* privilege (Privilège en vertu de l'article 38 de la *Loi sur la preuve au Canada*)		Protects information that, if disclosed, could cause injury to Canada's international relations, national defence or national security. Protection of the latter is also called "national security privilege." Information protected by section 38 privilege can only be disclosed if a court so orders or the Attorney General of Canada allows it.
— Solicitor-client privilege (Privilège du secret professionnel de l'avocat)		Protects communications (including documents) between a lawyer and their client created for the purpose of seeking or giving legal advice and intended to be kept confidential. This privilege belongs to the client, who is the only person who can waive it.
— Public interest privilege (section 37 of the *Canada Evidence Act*) (Protection des renseignements d'intérêt public, [article 37 de la *Loi sur la preuve au Canada*])		Protects information based on specified public interests. Any sufficiently compelling public interest can justify non-disclosure. Has been held to protect the identity of confidential informants, information about ongoing criminal investigations, information about sensitive investigative techniques and information that, if disclosed, would endanger the safety of public officers or the public. Also called "specified public interest immunity."

Term	Acronym or Abbreviation	Definition
Privy Council Office (Bureau du Conseil privé)	PCO (BCP)	Government department with the principal role to coordinate government administration. Often described as the Prime Minister's Department. Provides non-partisan advice to the Prime Minister, Cabinet and Cabinet committees on matters of national and international importance. Supports Cabinet decision-making and ensures implementation of the government's policy and legislative agenda across all federal departments and agencies.
Protected information (Information protégée)		Information that the government has decided could reasonably be expected to injure an interest, other than the national interest, if publicly disclosed. There are three categories: • Protected A (limited or moderate injury). • Protected B (serious injury). • Protected C (extremely grave injury).
Protective Security Briefing (Breffage préventif de sécurité)	PSB (BPS)	Type of unclassified briefing provided by the Canadian Security Intelligence Service (CSIS) to sensitize an individual with respect to a threat. Also known as a "defensive briefing."
Public Safety Canada (Sécurité publique Canada)		Federal government department responsible for public safety, national security and emergency management.
Royal assent (Sanction royale)		When the Governor General approves a bill passed by Parliament making it an Act of Parliament.
Royal Canadian Mounted Police (Gendarmerie royale du Canada)	RCMP (GRC)	Canada's national police service. Prevents and investigates crime, maintains peace and order, enforces laws, contributes to national security, ensures the safety of designated government officials and foreign dignitaries and the diplomatic community, and provides operational support to other police and law enforcement agencies within Canada and abroad.
Security and Intelligence Community (Communauté de la sécurité et du renseignement)	S&I Community	Government of Canada departments and agencies working on national security and intelligence gathering: CSE, CSIS, DND, GAC, PCO, Public Safety Canada and the RCMP.

Term	Acronym or Abbreviation	Definition
Security and Intelligence Secretariat of the Privy Council Office (Secrétariat de la sécurité et du renseignement du Bureau du Conseil privé)	PCO-S&I (S et R duBCP)	PCO Secretariat that gives policy advice and supports the National Security and Intelligence Advisor to the Prime Minister, briefing them and Cabinet on key national security issues. Has a coordination role when national security or intelligence issues are before Cabinet. Works with Public Safety Canada and other government departments to convene and support regular senior governance meetings on foreign interference threats and responses.
Security and Intelligence Threats to Elections Task Force (Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections)	SITE TF (Groupe de travail)	A governmental task force with representatives from: • Canadian Security and Intelligence Service (CSIS) • Communications Security Establishment (CSE) • Global Affairs Canada (GAC) • Royal Canadian Mounted Police (RCMP) Created to safeguard federal elections from foreign interference.
Sergeant-at-Arms (Sergent d'armes)	SAA	Performs many ceremonial duties in the House of Commons and is also responsible, as Corporate Security Officer, for the security of the House and its members off Parliament Hill.
Spamouflage (Camouflage de pourriels)		Tactic that uses networks of new or hijacked social media accounts to post and amplify propaganda messages across multiple platforms.
Standing (Qualité pour agir)		Opportunity to participate directly in proceedings (i.e. in court or before administrative tribunals) with certain rights. The Foreign Interference Commission's *Rules of Practice and Procedure* govern who can have standing as a Party or Intervener (collectively, "Participants") in the Commission's proceedings.

Term	Acronym or Abbreviation	Definition
Standing Committee on Access to Information, Privacy and Ethics (Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique)	ETHI	Made up of members of the House of Commons. Studies matters related to: • the Office of the Information Commissioner of Canada • the Office of the Privacy Commissioner of Canada • the Office of the Commissioner of Lobbying of Canada. Also studies certain issues related to the Office of Conflict of Interest and Ethics Commissioner.
Standing Committee on Procedure and House Affairs (Comité permanent de la procédure et des affaires de la Chambre)	PROC	Made up of members of the House of Commons. Studies and reports on: • the rules and practices of the House and its committees • electoral matters • questions of privilege • member of Parliament conflicts of interest.
Terms of Reference (Mandat)	ToR	The Foreign Interference Commission's mandate as set out in Order in Council P.C. 2023-0882 (which creates the Foreign Interference Commission and appoints the Commissioner).
Threat reduction measure (Mesure de réduction de la menace)	TRM (MRM)	Operational measure taken by the Canadian Security Intelligence Service (CSIS) to reduce threats to the security of Canada, under section 12.1 of the *CSIS Act*, which requires that the measure be reasonable and proportional to the severity of the threat.
Transnational repression (Répression transnationale)	TNR (RTN)	For the purpose of the Commission, transnational repression is when countries employ measures beyond their borders to intimidate, silence, coerce, harass or harm individuals, primarily members of diaspora communities in Canada.

Main Federal Entities Involved in Responding to Foreign Interference



Public Inquiry Into
Foreign Interference
in Federal Electoral
Processes and
Democratic
Institutions