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

The Honourable Marie-Josée Hogue,
Commissioner

VOLUME 3 CHAPTERS 10-13

The Government's Capacity to Detect, Deter and Counter Foreign Interference (Facts and Analysis 1/2)

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 3: The Government's Capacity to Detect, Deter and Counter Foreign Interference (Facts and Analysis 1/2).

Cette publication est également disponible en français :
Volume 3 : La capacité du gouvernement à détecter, prévenir et contrer l'ingérence étrangère (faits et analyse 1/2).

CP32-169/2-2025E-3-PDF
ISBN 978-0-660-75081-1

(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 10

The Foreign Interference Threat

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.*

10.1 Introduction

In order to understand the government's capacity to respond to foreign interference, it is essential to understand the nature of the foreign interference threat itself. This includes appreciating the range of actors who engage in it and the tactics that they use.

Understanding the foreign interference threat can be challenging for a number of reasons. One challenge that I learned about in the course of my work is the grey zone of activity that exists between foreign interference on the one hand, and legitimate state activity on the other.

A second challenge arises from the fact that much of what we know about foreign interference comes from intelligence, which is, as I have discussed earlier in this report, a source of information with unavoidable limitations.

In this Chapter, I provide a high-level overview of the foreign interference threat as it currently exists.

10.2 Foreign Interference Beyond the Commission's Mandate

As discussed in Volume 2, Chapter 3, foreign interference has many aspects, but the scope of my inquiry is set by the Commission's Terms of Reference. My mandate is to focus on a subset of foreign interference – that targeting democratic institutions and processes. Much is not included, such as foreign interference with Canada's economy, industry, military and academia, espionage and many forms of transnational repression.

However, foreign interference activities do not exist in watertight compartments. For example, transnational repression involving a politician could also constitute interference in a democratic process. Furthermore, some transnational repression tactics targeting diaspora community members can interfere in Canada's democratic processes. I have taken this into account when pursuing my mandate.

As an example, the Commission requested information regarding certain current, publicly known examples of foreign interference, such as the assassination of Hardeep Singh Nijjar. The Commission also met with Canadians from diaspora communities to hear their experiences with transnational repression. These issues are not fully within the Commission's mandate, but this information has enhanced my understanding of the foreign interference threat and Canada's response to it. It has also helped inform my recommendations.

10.3 Threat Actors Targeting Canada

The threat landscape is influenced by historical forces, contemporary realities, complex relationships and Canada's strategic goals and interests. For this reason, confronting threat actors requires understanding our historical relationships and more recent events and their effects. It also requires appreciating Canada's strategic interests in a range of foreign states, as well as their interests in Canada.

People's Republic of China (PRC)

The People's Republic of China ("**PRC**") is, at the time of writing this report, the most active perpetrator of state-based foreign interference targeting Canada's democratic institutions.

The PRC is also a critical actor on the global stage. The PRC focuses on promoting its national interest and protecting the legitimacy and stability of the Chinese Communist Party ("**CCP**"). Its values and interests increasingly differ from those of Canada. Nevertheless, the PRC is an essential partner for Canada in addressing issues important to both states. Canada's ability to work with the PRC on joint issues and raise objections and concerns requires Canada and the PRC to maintain functioning channels of communication.

The PRC views Canada as a high-priority target. Canada is an important member of alliances like the Five Eyes (Canada, the United Kingdom, the United States, Australia and New Zealand). We have a robust international reputation that the PRC may want to use to advance PRC interests. And we are a reliable and open trading partner with an advanced economy that can support PRC development objectives. Canada is also home to one of the largest Chinese diaspora communities. The Canadian Security Intelligence Service ("**CSIS**") reports that the PRC wants to see Canada support PRC interests, portray the PRC positively and be deferential to PRC authority.

Canada's relationship with the PRC changed dramatically in December 2018 when the PRC arbitrarily detained Canadians Michael Spavor and Michael

Kovrig (“**Two Michaels**”). Until their release in September 2021, Canada’s relations with the PRC centred on their detention.

This was also a significant event from the PRC’s perspective. Historically, the PRC focused on political engagements with the executive branch in Canada. However, Deputy Minister of Foreign Affairs David Morrison explained that the PRC’s detention of the Two Michaels led Canadian public opinion about the PRC to plummet and increased activity critical of the PRC in the legislative branch. This may have caused the PRC to develop an interest in members of Canada’s legislative branch – an interest it did not see as necessary before. This is important context for the PRC’s interest in Canadian members of Parliament (“**MPs**”), a topic I discuss in greater detail in Volume 4, Chapter 14 as part of my review of the document known as the “Targeting Paper.”

Since the release of the Two Michaels in 2021, Canada and the PRC have been attempting to come to terms with their damaged relationship. For Canada, this has included raising concerns about PRC foreign interference activities here.

PRC foreign interference is wide-ranging. It targets all levels of government in Canada. Canadian security and intelligence officials view the PRC as generally “party agnostic,” that is, supporting those it believes helpful to its interests at the time, and those it believes are likely to have power regardless of political party.

According to intelligence, the PRC uses a wide range of actors for foreign interference. Among its national-level institutions, both the Ministry of State Security and the Ministry of Public Security operate covertly internationally. The PRC also acts through its diplomatic officials.

The United Front Work Department, formally a department of the CCP, tries to control and influence the Chinese Canadian diaspora community, shape international opinions and influence politicians to support PRC policies.

Beyond formal state and party institutions, the PRC relies on proxies, which are individuals or organizations taking explicit or implicit direction from the PRC to engage in foreign interference. It tries to leverage Chinese Canadians, networks developed by embassies and consulates, as well as other actors (whether or not ethnically Chinese).

The PRC also poses the most sophisticated and active cyber threat to Canada.

CSIS further assesses that the PRC has increasingly used social media and the Internet for disinformation campaigns involving elections.

Despite increased scrutiny of foreign interference efforts in Canada, Canadian security and intelligence agencies have concluded that the PRC still has the capacity and intent to interfere in elections.

India

India is the second-most active state actor engaging in electoral foreign interference in Canada.

Like the PRC, India is a critical actor on the world stage. It is an increasingly significant global player and is in a position to challenge the PRC's hegemony in Asia. Canada and India have worked together for decades, but there have been challenges in the relationship. Recently, these challenges have become more acute. Many of the difficulties are long-standing and they inform India's foreign interference activities.

Since the 1985 bombing of an Air India flight from Canada, India has perceived Canada as not taking India's national security concerns about Khalistani separatism (the goal of an independent Sikh homeland in northern India called "Khalistan") sufficiently seriously. A fundamental tension exists between India's perspective that certain activities are terrorism, and Canada's perspective, which protects fundamental freedoms of expression and association. India does not appear to differentiate between lawful pro-Khalistan political advocacy and the relatively small number of Canada-based Khalistani violent extremists.

India has tried to pressure Canada to go beyond the parameters of Canadian law to counter supporters of an independent Khalistan. India's foreign interference activities attempt to have Canada's position align with its own about key issues, particularly about supporters of Khalistani separatism.

India focuses its foreign interference activities on the Indo-Canadian community and on prominent non-Indo-Canadians to achieve these objectives. This interference has targeted all levels of government.

Like the PRC, India conducts foreign interference through its state officials in Canada and through proxies. A body of intelligence indicates that Government of India proxy agents may have provided, and may continue to be clandestinely providing, illicit financial support to various Canadian politicians in an attempt to secure the election of pro-Indian candidates or gain influence over candidates who take office. The Canadian intelligence community has observed Government of India interference seeking to influence nomination processes and decisions made in Parliament. The intelligence does not necessarily indicate that the elected officials or candidates involved were aware of the interference attempts, nor were the attempts necessarily successful.

India also uses disinformation as a key form of foreign interference against Canada, a tactic they are likely to use more often. India continues to develop its cyber capabilities. CSIS assesses that India will likely seek to promote a pro-India and anti-Khalistan narrative in Canada using cognitive warfare techniques.

Until recently, Canada was trying to improve its bilateral relationship with India as part of its broader Indo-Pacific Strategy. The assassination of Hardeep Singh Nijjar in June 2023 derailed these efforts.

In September 2023, Prime Minister Trudeau announced that Canadian security and intelligence agencies had credible allegations of a potential link between agents of the Government of India and Mr. Nijjar's death. India has repeatedly denied these allegations. India's reaction was extreme and the relationship between Canada and India has remained strained since that time. I discuss the events surrounding Mr. Nijjar's assassination in more detail in Volume 4, Chapter 17.

More recently, in October 2024, Canada expelled six Indian diplomats and consular officials in reaction to a targeted campaign against Canadian citizens by agents linked to the Government of India.

Russia

Canada has an adversarial relationship with Russia.

In the aftermath of the Cold War, Canada progressively engaged with Russia. This changed after the 2014 Russian invasion of Crimea, when Canada's diplomatic engagement with Russia decreased significantly. Canada suspended virtually all official contacts following Russia's invasion of Ukraine in 2022. Diplomatic relations are generally limited now to Canada expressing dissatisfaction with Russian behaviour. Canada has imposed economic sanctions on more than 3,000 Russian-affiliated entities and individuals supporting the war against Ukraine.

Russia's relationship with many other Western states is equally adversarial.

Russian foreign interference activities seek to destabilize or delegitimize democratic states. Russia attacks democracy through misinformation and disinformation campaigns and, increasingly, through generative artificial intelligence ("**AI**"). It also has sophisticated cyber capabilities. For the last two years, Russia's war in Ukraine has driven much of its disinformation effort.

The government currently assesses Russia as having the capability to engage in significant foreign interference against Canada. However, it appears to lack intent, as Russia does not perceive Canada as an existential threat. Until now, the government has not observed Russian interference specific to Canada's democratic processes. Still, Russia has run a long-standing campaign to discredit Western democracies in general, and the United States and its allies in particular. For example, RT – a Russian state-controlled media outlet – is alleged to have covertly funded and directed a United States company to publish English language videos on multiple social media platforms in an effort to amplify divisions among Americans.

The Communications Security Establishment ("**CSE**") has observed Russian cyber threat activity in Canada, but not against Canadian democratic institutions. CSIS witnesses noted that Canada's strong support of Ukraine could affect whether Russia tries to influence the next federal election. Russia's significant efforts to interfere in elections in Europe demonstrate its continuing capacity to interfere.

Pakistan

Pakistan's foreign interference activities are opportunistic and relate to the poor relationship between Pakistan and India. Pakistan engages in foreign interference in Canada to promote stability in Pakistan and to counter India's growing influence. Its activities target various facets of Canadian society and all levels of government. For now, Pakistan is more likely to rely on local community elements, rather than cyber measures or AI, to facilitate its foreign interference.

Iran

Canada's relationship with Iran is severely limited. Diplomatic relations were severed in 2012 when Canada closed its embassy in Tehran and expelled all Iranian diplomats in Canada due to concerns about Iran's human rights record and support for terrorism. There is currently almost no official government-to-government contact between Canada and Iran.

Iran is not currently, nor has it historically been, a significant foreign interference actor in Canadian federal elections or other democratic institutions. Iran instead focuses on transnational repression to prevent criticism of its government.

Iran relies on criminal groups to carry out its interference activities and conducts psychological harassment online. CSIS acknowledged that such tactics may very well prevent people from participating in Canadian democratic processes, though this is difficult to determine with certainty.

CSIS witnesses also noted that Canada recently listed Iran's Islamic Revolutionary Guard Corps as a terrorist entity. This could result in increased foreign interference activity leading up to an election, among other potential reactions.

Other threat actors

The Commission heard evidence and received information about other threat actors potentially engaging in transnational repression. These countries have very little interest in Canada's democratic institutions and instead are primarily interested in controlling diaspora members and silencing dissidents. In Volume 4, Chapter 17, and Volume 6, Chapter 21, I discuss what I heard about transnational repression in Canada.

10.4 Tactics Common in Foreign Interference

Foreign states use interference to sow discord, bias policy development and decision-making and influence public opinion to support their agendas. The tactics used and targets chosen may vary.

Long term cultivation

Threat actors spend significant resources to cultivate deep, long-lasting relationships with targets like parliamentarians or candidates for election, often using proxies or co-optees who hide their affiliation with a foreign state. Intelligence indicates that foreign states seek to cultivate and assist politicians who these states believe will have power or influence in government. Assistance can come in many forms, including resources, advice and disinformation campaigns that may help a candidate at another's expense. Getting close to policymakers enables foreign states to support or suppress specific policy positions.

Eliciting information

Threat actors may try to manipulate individuals into sharing valuable information. A threat actor might share confidential information hoping the individual will reciprocate. Here too, politicians can be attractive targets. Campaign officials, political staffers and others can also become targets because of their access to confidential information.

Covert financing

Intelligence agencies have seen political parties and candidates receive donations that appear to be from a Canadian, but that in reality originate from a foreign threat actor. The clearest reason for doing this is to support candidates seen as receptive to the interests of the foreign state, or to help defeat opposing candidates regarded as hostile to the foreign state. In some cases, the candidate may not even know that they are receiving financial support from a foreign state.

Other times, funding may be used to help foster a sense of obligation between a candidate and the foreign state or its proxies. Funding provided through a proxy may help solidify the perception of the proxy as a gatekeeper for community support. Funding may help to build a durable bond between the threat actor and the candidate or office-holder. Of course, for this to be the case, the candidate must be aware they have received financial support.

Mobilizing and leveraging community organizations

Some threat actors use local community networks to facilitate foreign interference activities. For example, the People's Republic of China (PRC) relies on members of diaspora communities and on networks developed by their embassies and consulates. Foreign state officials can also covertly direct or intimidate community groups to lobby on their behalf or covertly identify and marginalize candidates or politicians who do not support the foreign state. In this way, community organizations may be both victims of foreign interference and the vehicle for conducting that interference. We therefore have to be careful not to automatically hold community organizations responsible for foreign interference, keeping in mind that most are victims, not active participants.

Exploiting opportunities in political party processes

Each political party has its own process for candidate nomination and leadership selection. These processes are mainly unregulated. They are largely within the control of the parties.

The Security and Intelligence Threats to Elections Task Force (see Volume 3, **Chapter 11**) has assessed candidate and leadership processes as potentially vulnerable to hostile state actors. For example, ridings thought of as "safe seats" may be attractive to states seeking to influence politics. Helping someone win the party's nomination in such a riding likely assures their election success.

I discuss the role that political party rules and processes may play in foreign interference in more detail in Volume 3, **Chapter 13**.

Blackmail and threats

States may use more aggressive interference tactics, such as blackmail or threats. These are often used as tools of transnational repression. For instance, a foreign state may coerce someone by threatening their family members who live in that state. States may also try to blackmail or threaten elected officials to influence their official activities.

Cyber threats

The security and intelligence community assesses that cyber threats to Canada's democratic institutions are increasing in number and sophistication. CSE's Canadian Centre for Cyber Security ("**CCCS**") sees foreign state cyber activity not only against federal government infrastructure, but also against provincial, territorial and municipal infrastructure, and non-governmental infrastructure.

Threat actors can gain access to a network by hacking into it directly or by tricking a user into giving access. Once a threat actor gains access, their aim is usually cyber espionage (stealing intellectual property or collecting other information). In other cases, the threat actor may not immediately exploit the access, but instead position itself for some future cyber activity.

CCCS has identified various attempts to probe Canada's electoral infrastructure, but foreign state actors have been unsuccessful in compromising it. However, the growing power of technology increases the threat of cyber attacks on infrastructure, as well as, I would add, the risk that these cyber attacks would ultimately be successful.

Media influence, misinformation and disinformation

Foreign state influence over media can be a powerful tool for foreign interference. CSIS has described a PRC "takeover" of Chinese-language media in Canada that occurred over decades. CSIS believes the Chinese Communist Party (CCP) tries to shape its preferred narrative through media. In this way, space for dissenting voices may become limited, economic incentives may be given to media to support CCP positions and self-censorship may increase.

Foreign threat actors manipulate both social and traditional media to spread disinformation, amplify a particular message or provoke users. People unaware of the origins of the content or the intent of the threat actor may unintentionally spread disinformation to others. This is misinformation.

This can be particularly impactful when threat actors use social media. For example, in May 2023, the Rapid Response Mechanism ("**RRM**") Canada

found that a network of accounts was amplifying a large volume of false or misleading narratives about MP Michael Chong, including spreading false narratives about his identity as well as commentary and claims about his background, political stances and family heritage. In total, RRM Canada assessed that between two and five million WeChat users viewed the false or misleading content. RRM Canada had a high level of confidence that the disinformation campaign was linked to the PRC.

Advances in generative artificial intelligence (AI) and deep fake technology (AI-generated impersonations) represent a significant change since the past two general elections. CCCS has seen more synthetic online content (manipulated or fabricated videos, audios and imagery) around election periods. Generative AI makes it easier to manipulate information. It also makes creating and spreading content faster and easier and, I would add, more effective.

I heard evidence about an instance in which RRM Canada learned about a bot network that, as part of a spamouflage campaign, circulated three YouTube videos, believed to be deep fakes of Xin Liu, a well-known critic of the CCP. The videos depicted Mr. Liu making particularly strong allegations and vilifying the Canadian Prime Minister. RRM Canada assessed the impact on Mr. Liu was likely very high. He probably received hundreds of thousands of alerts from Facebook, Twitter and YouTube with false claims that he libelled dozens of parliamentarians.

RRM Canada concluded that the use of sophisticated deepfake technology in a spamouflage campaign was significant, suggesting a new tactic by the PRC and increasing the likelihood that spamouflage could be more persuasive to a wider audience.

10.5 The Six Identified Major Instances of Suspected Foreign Interference in Canada's Democratic Processes

Preparing the list

As part of its investigation, the Commission asked the Government of Canada to list and describe all major instances of suspected foreign interference targeting Canada's democratic processes from 2018 to the present, including the actions, dates, targets, countries, key players, information flow and any responses.

In response, the Privy Council Office led a series of consultations with senior officials from CSIS, Global Affairs Canada ("**GAC**"), CSE and Public Safety Canada.

The government stated that it typically monitors patterns of behaviour over time rather than focusing on specific incidents. For this reason, the government first had to decide what constituted an "instance" of foreign interference. It concluded that, among other criteria, an instance had to meet the *Canadian Security Intelligence Service Act* definition of a foreign influenced activity that was a threat to the security of Canada[1] and government had to have intelligence about the impact of the activity. The activity also needed to be circumscribed in time, as opposed to less discrete events like the ongoing nurturing of relationships with an individual.

The requirement that an instance satisfy these criteria meant that the list was not an exhaustive catalogue of potential foreign interference in Canada's democratic institutions, including electoral processes. These criteria may have resulted in certain foreign interference activities or actions being excluded or discarded from the list.

Developing the list involved discussions within the national security and intelligence community. CSIS developed a preliminary list. Senior government officials then identified which instances met the definition of foreign interference and whether they had a tangible impact on democratic processes or institutions. Instances viewed as legitimate diplomatic activity were excluded.

The final list represented the consensus view resulting from those discussions.

The list of six suspected instances

The government gave the Commission a list of six major instances of suspected foreign interference.

Four of the six instances relate to suspected foreign interference in the 2019 or 2021 elections and are discussed in Volume 2, Chapters 7 and 8. These four instances are as follows:

- Reporting indicates that officials from the Government of Pakistan tried to influence Canadian federal politics clandestinely before the 2019 federal election to further Pakistan's interests in Canada.
- A foreign government official is suspected of foreign interference directed at a Liberal Party of Canada ("**Liberal Party**") candidate.

[1] *Canadian Security and Intelligence Service Act*, s. 2. Foreign influenced activities are defined in paragraph (b) of the definition of "threats to the security of Canada."

- Reporting indicates that the PRC actively supported a Liberal Party candidate's 2019 federal nomination race in the riding of Don Valley North, Ontario, including by using a proxy agent.
- The Government of India is suspected of leveraging proxy agents to provide clandestine financial support to specific candidates from three political parties in a federal election.

The Commission investigated the other two instances identified on the government's list and received and reviewed CSIS's intelligence reporting about them.

The Commission also examined CSIS and other government officials *in camera* about the suspected instances. As the suspected instances are based on highly classified information, the descriptions below represent as much information as I can publicly disclose. I discuss both suspected instances in further detail in the classified supplement to this report.

The first instance involved reporting that a foreign government undertook several actions, including interference, to reduce the election chances of a specific federal Liberal Party candidate. It is suspected that the foreign government did this because of the candidate's support for issues perceived to be contrary to the state's interests.

The activities of the foreign government likely extended beyond the election campaign and likely had a negative impact on the individual's political career. This information was disseminated to alert Canadian public servants of the foreign government's aggressive efforts to thwart the candidate's campaign.

The evidence suggests that no information about this was given to the political level of government until the Commission requested the list of instances. The Prime Minister said he was astonished that he had not been informed of the events, since they involved his party, and the information would have been relevant for him as party leader. The Prime Minister expressed concern that he was not briefed, despite his ongoing engagement with government officials about foreign interference. However, he was confident that he would have been told of the incident if current information flow processes had been in place. I share the Prime Minister's astonishment that he was not advised of this at the time or, indeed, until this Commission's proceedings.

The second instance involved a former opposition parliamentarian who is suspected of having worked to influence parliamentary business on behalf of a foreign government. It is suspected that a foreign government official asked the parliamentarian to take a particular action, which the parliamentarian then took.

All six instances mentioned above were assessments based on intelligence reporting, not proven fact. Elements of the picture may be missing. CSIS witnesses said that their investigations are generally focused on threat actors, not on candidates or elected officials who engage with them. This often leaves

intelligence gaps about the activities, level of knowledge, and motivations of those candidates or elected officials. Moreover, these assessments were based on the information before government at the time. Assessments can evolve, sometimes drastically, over time.

The seventh instance

The list initially produced to the Commission in July 2024 contained a seventh instance of suspected foreign interference. The intelligence underlying the seventh instance indicated that a foreign government official engaged an MP to take a particular action in their role as a parliamentarian that would support the foreign government's interests. The reporting further indicated that coercive tactics were used for the parliamentarian to act in the interest of the foreign government.

In early September 2024, CSIS reviewed public records related to the seventh instance for reasons said to be unrelated to the Commission's investigation. CSIS learned public information that directly contradicted a significant element of the intelligence underlying the alleged instance. The MP had not, in fact, undertaken the actions indicated in the intelligence. A CSIS witness explained that CSIS had not verified public information about whether the MP in fact took the actions suggested in the intelligence because the MP was not a subject of investigation.

I note that the intelligence underlying this alleged instance of foreign interference initially stated that it had been collected from sources considered reliable. Nonetheless, the information provided by these sources was shown to be inaccurate.

CSIS later evidently updated its assessment based on the publicly available information about the MP's actions. CSIS gave its updated assessment to senior government officials, and they agreed that the instance should be removed from the list. The government informed the Commission shortly thereafter. However, CSIS continued to view the events as a suspected instance of the foreign government attempting to interfere in Canada's democratic processes.

The discovery of public information directly contradicted a significant element of the intelligence underlying the suspected seventh instance and ultimately changed CSIS's assessment. This illustrates both the limits and the frailty of intelligence.

In this case, CSIS had reporting of conversations between the foreign official and the MP and between the foreign official and another foreign official. However, it did not have direct information about whether the MP in fact undertook the action they were instructed to take. Indeed, CSIS did not verify publicly available information on whether the MP had actually taken the alleged action, as the MP was not the subject of the investigation. This led to a

gap that should have been filled before any conclusions were drawn about the MP's behaviour. The failure to verify the information led to an erroneous conclusion.

This situation also illustrates the frailty of intelligence. Frailty exists even when the information is collected from sources considered reliable. For example, in this instance, the "new" information discovered several years later (but available at the time) completely changed the government's understanding of what happened and the conclusions to be drawn from it.

Ultimately, the limits and frailty of intelligence mean that considerable care must be taken when relying on it to draw conclusions or make allegations about the actions of an individual. This care is especially needed where the conclusions or allegations can have significant consequences for the individual and for public faith in Canadian institutions.

10.6 Perspectives about Foreign Interference

"Foreign interference" is much easier to define than to apply in specific circumstances. In this section, I discuss difficulties in determining what conduct constitutes foreign interference, and how these difficulties present real challenges for government in seeking to respond.

The line between foreign interference and legitimate foreign influence can be difficult to draw

Government decisions can have consequences beyond national borders – for example, on climate, development and defence. As a result, countries attempt to influence each other to protect their own interests. Even aggressive attempts at influence may be legitimate.

For example, within appropriate boundaries, states can use diplomats to pressure foreign governments, politicians and citizens. Diplomats may act directly or through intermediaries. Depending on the laws of their host state, they may lobby, attend events, take out advertisements and fund research. States also engage in many other legitimate activities to influence other countries such as at international meetings like the G7.

These activities are legitimate because they take place openly and do not involve threats to individuals or groups. Foreign interference is different because it is covert or threatening.

It may seem that the line between (legitimate) foreign influence and (illegitimate) foreign interference is easy to draw. In practice it is not. Some witnesses before the Commission referred to a "grey zone" between clearly

legitimate foreign influence and clearly illegitimate foreign interference. In other words, foreign interference and foreign influence exist along a continuum. The situation becomes even more complicated when countries engage in influence and interference at the same time.

An example provided in a Global Affairs Canada (GAC) document illustrates the difficulty in distinguishing legitimate influence from illegitimate interference:

> A diplomat of country X, stationed in Canada, asks a prominent Canadian academic to write an op-ed opposing the Government of Canada's approach to a particular international issue, and urging Canadians to likewise disagree. The academic writes the op-ed and it is published in a widely circulated national newspaper. [...] The academic does not disclose their relationship with the individual employed by the foreign government.[2]

There is nothing wrong with a diplomat discussing government policy with an academic. There is nothing wrong with a diplomat trying to convince influential Canadians to agree with them. There is nothing wrong with academics writing op-eds critical of Canada.

However, if the diplomat asks the academic to hide their relationship, this secrecy would change the activity into foreign interference. And what if the diplomat did not expressly ask them to hide their relationship, but the academic implicitly understood that they should? This complicates the task of distinguishing between legitimate influence and illegitimate interference. Moreover, an outside observer would likely never become aware of this relationship, making it difficult to conclude that the resulting activities were foreign interference by a given state.

It is also important to recognize that there is no common international definition of foreign interference. Indeed, GAC witnesses indicated that such a definition would not be feasible in the current geopolitical context. Canada may view certain activities as foreign influence or foreign interference, while adversaries may take the opposite view.

For example, the People's Republic of China (PRC) maintains that it is foreign interference for other countries to criticize it as failing to adhere to international human rights obligations. GAC views such criticism as a legitimate way to hold the PRC accountable as a member of the international community. GAC said such criticism is distinguishable from the covert activities of PRC officials or agencies in Canada. I heard that this difference could present challenges when GAC engages with the PRC about foreign interference.

---

[2] CAN008822: Global Affairs Canada, *Influence and Interference: Distinctions in the context of diplomatic relations and democratic processes* at p. 6.

Deputy Minister of Foreign Affairs David Morrison testified that differing interpretations of foreign interference mean that GAC should do more to ensure that foreign officials in Canada know what Canada considers acceptable diplomatic activity versus foreign interference. Canada can, for example, clearly communicate where the lines are, and that Canada will react when those lines are crossed. I agree with him and will return to this in my recommendations.

A concept viewed through different lenses

This working definition of foreign interference is substantially similar across government departments and agencies. It includes foreign influenced activities within, or relating to, Canada that are detrimental to the interests of Canada and that are clandestine, deceptive or that involve a threat to someone.

However, different departments and agencies can differ about whether a set of facts amounts to foreign interference and, if it does, how serious the interference is.

This is not surprising. Departments and agencies apply this definition through the lenses of their respective mandates and authorities. These lenses may, in turn, lead people to differ from colleagues elsewhere in government in how they view a set of facts.

For example, outside an election period, foreign consulate staff might ask a Canadian community member to pressure an MP to vote a certain way. CSIS may view this as a state covertly using a proxy for foreign interference. But GAC may, from its foreign policy perspective, consider the request to be legitimate diplomatic activity as long as intelligence does not suggest the request was intended to be covert, clandestine, deceptive or threatening.

Different perspectives do not necessarily create vulnerability

As long as it does not paralyze decision-making, debate within government about whether something constitutes foreign interference can be positive. Tensions between departments or agencies exist in all government work, not just work relating to foreign interference.

Discussion and debate are necessary for good government. Former CSIS Director David Vigneault, speaking about foreign interference, said that it is healthy in a democracy that intelligence agencies do not always have the final say in national security discussions because it is dangerous to accord too much weight to any one view. Different views facilitate a coordinated response that takes into account all relevant risks, priorities, values and

interests, and generally, leads to a better outcome. That being said, debate and discussion cannot be permitted to continue indefinitely without any decision being taken.

Government sometimes expressly recognizes in legislation the need for different perspectives in decision-making. For example, the *Communications Security Establishment Act* allows the Minister of National Defence to issue an active cyber operation authorization to counter the activities of a foreign state or other specific threats only if the Minister of Foreign Affairs has requested or consented to it.[3] The *Canadian Security Intelligence Service Act* requires that, before taking a threat reduction measure ("**TRM**"), CSIS consult, as appropriate, other departments or agencies about whether they are in a position to reduce the threat.[4]

Additional checks are sometimes implemented as a matter of policy, even if the legislation does not require it. For example, ministerial directives require CSIS to consult other departments such as GAC, the Department of Justice and Public Safety Canada to assess the risk level of a TRM in four areas – legal, foreign policy, operational and reputational. If the TRM is high-risk and has a foreign nexus, CSIS can proceed only with approval of the Deputy Minister or Minister of Foreign Affairs.

Inter-departmental committees at the deputy minister, assistant deputy minister and director general levels are designed to help government benefit from hearing different views. Similarly, the Security and Intelligence Threats to Elections Task Force and Panel of Five (see Volume 3, **Chapter 11**) are forums where government deliberately brings different perspectives to bear about foreign interference issues.

In deciding whether and when to respond to a foreign interference threat, government should have a 360-degree perspective, not simply a threat, foreign policy or law enforcement perspective. It is essential for agencies and departments to bring their own perspectives when addressing potential foreign interference. Working through varied viewpoints promotes more informed decisions. This is especially important in the foreign interference context where intelligence, which can vary greatly in its quality and reliability, is being considered and where foreign interference tactics are always evolving. Of course, where there is credible and reliable information about a threat requiring immediate action such as a threat to the physical integrity of an individual, the considerations are different. In this case, the priority should be to act as quickly as possible.

I heard that increased discussion over the past three to four years has led to greater agreement and better understanding of differing views across government about what constitutes foreign interference. Mr. Vigneault pointed to CSIS and political leadership's current understanding of foreign interference in nomination processes as an example. As I heard that the

---

3 *Communications Security Establishment Act*, s. 30(2).
4 *Canadian Security and Intelligence Service Act*, s. 12.1(3).

government is currently working on a whole-of-government understanding of foreign interference, I expect agreement to increase in some areas, but I also expect healthy debate to continue. It is a feature of the system, not a bug. However, healthy debate becomes unhealthy when it unduly impacts decision-making.

10.7 Conclusion

In this chapter, I have outlined at a high level the nature of the foreign interference threat facing Canada. In the next chapter, I will examine how Canada responds to this threat.

CHAPTER 11

How Canada Protects Against Foreign Interference

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.*

11.1 Introduction

In Volume 2, Chapter 6, I discussed various federal entities that were relevant to foreign interference. In this Chapter, I go into more detail about the specific powers and authorities that these entities have in responding to foreign interference. I also address the question of how coordination is maintained across these entities.

11.2 The Intelligence Cycle

The government's national security and intelligence community has producers and consumers of intelligence. Producers collect and assess intelligence and share products with consumers. Consumers receive intelligence products from the collectors.

Intelligence products are created through a process called the "intelligence cycle," which seeks to ensure that intelligence is relevant to policy and decision makers and Canada's national interests. Collection and assessment of intelligence are guided by the government's intelligence priorities, as well as its capabilities and resources. The intelligence cycle is discussed in more detail in Volume 2, Chapter 5.

Cabinet sets intelligence priorities every two years, with priorities developed by consulting across government. The Privy Council Office ("**PCO**") oversees this process through its Security and Intelligence Secretariat.

The Cabinet Committee on Global Affairs and Public Security governs and monitors intelligence priority implementation with the support of committees made up of senior public servants. Cabinet has given these committees the responsibility to set specific intelligence requirements, oversee performance measurement and recommend new intelligence priorities to Cabinet.

Once intelligence priorities are approved, the Ministers of Foreign Affairs, National Defence and Public Safety and Emergency Preparedness issue ministerial directives to the departments and agencies under their responsibility.

At the operational level, each department develops intelligence requirements based on Cabinet's intelligence priorities. Requirements outline specific needs related to the priorities. They help inform operational planning by security and intelligence producers. While intelligence priorities are broad and in place for two years at a time, requirements are more specific and can be changed at any time.

During the two-year intelligence cycle, Cabinet receives two updates. The first update comes one year into the cycle. Feedback is gathered from intelligence consumers about how much intelligence support they received for their requirements. The end-of-cycle update is similar and given to Cabinet when it begins updating priorities for the next intelligence cycle.

11.3 Key Players in the National Security and Intelligence Community

The Canadian Security Intelligence Service (CSIS)

The Canadian Security Intelligence Service ("**CSIS**") is Canada's domestic intelligence service. Its primary mandate, set out in section 12 of the *Canadian Security Intelligence Service Act* ("***CSIS Act***"), is to collect, analyze and retain information and intelligence about activities that may reasonably be suspected of being threats to the security of Canada.

CSIS then reports to and advises the government about these threats. Foreign interference is considered a threat to the security of Canada. CSIS can investigate threats within or outside Canada.

In addition to its mandate regarding threats to the security of Canada, CSIS also has a limited foreign intelligence mandate. Under section 16 of the *CSIS Act*, CSIS may collect foreign intelligence at the request of the Minister of Foreign Affairs or National Defence, and with the consent of the Minister of Public Safety., CSIS may collect foreign intelligence.[5] This essentially means that these ministers can ask CSIS to help them by collecting foreign intelligence. However, CSIS can only do so within Canada.

Prior to the *Countering Foreign Interference Act* (introduced as Bill C-70), CSIS's collection under section 16 was also limited to information located within Canada. The *Countering Foreign Interference Act* changed this by adding section 16(1.1) to the *CSIS Act*, which says that the assistance

[5] Foreign intelligence is defined as intelligence in relation to the defence of Canada, or the conduct of the international affairs of Canada relating to the capabilities, intentions or activities of foreign states or groups of states, or any person other than a Canadian citizen, permanent resident or corporation incorporated by or under an Act of Parliament or a province.

provided under section 16(1) "may include collection, from within Canada, of information or intelligence that is located outside of Canada if the assistance is directed at a person or thing in Canada or at an individual who was in Canada and is temporarily outside of Canada."

Intelligence collection

Intelligence is collected by CSIS regional offices based on Cabinet's intelligence priorities and departmental requirements. Regional offices and Headquarters work together to try to ensure regions collect the information most useful to government clients.

CSIS also collects intelligence in relation to emerging global threats.

CSIS collects information from various sources, including human and technical sources, as well as open-source materials.

CSIS uses its legislated authorities to investigate specific threats by using different operational tools and techniques that require various levels of internal approval.

CSIS can also acquire a warrant, which allows for more intrusive investigations. CSIS can get a multiple use warrant (for example, for ongoing surveillance), or, since the passage of the *Countering Foreign Interference Act*, a single use warrant (for example, for copying a single electronic device).

Finally, CSIS can partner with others to further its investigations. For example, CSIS works with Canadian agencies and a large number of foreign intelligence services to leverage their operational and technical expertise and capabilities.

Intelligence assessment and analysis

Once collected, CSIS assesses and analyzes intelligence and produces a variety of intellience products that are shared with government. Until the fall of 2023, CSIS shared its products via email over the Canadian Top Secret Network ("**CTSN**"). As will be discussed in Volume 4, Chapter 14, I heard evidence that this was often not an effective way of transmitting intelligence. CSIS now uses the Communications Security Establishment's ("**CSE's**") updated centralized database system to share information.

CSIS intelligence products are intended to inform government policy development and the broader national security environment.

CSIS intelligence can also inform government decisions at an operational level. For instance, if CSIS has intelligence that an individual applying for a diplomatic posting in Canada is involved in espionage, the government might deny them entry into Canada. CSIS also does security assessments for individuals who need access to classified information within government. These are done both for public servants and for politicians being considered for a parliamentary or Cabinet role. The Prime Minister's Office identified this vetting process as a significant context in which they receive intelligence.

Response toolkit

Threat reduction measures

Since 2015, CSIS has had the authority to implement threat reduction measures ("**TRMs**") to mitigate threats to the security of Canada, including by sharing classified information with individuals who are not security-cleared and are outside the federal government.

To implement a TRM, CSIS must have reasonable grounds to believe that the activity the measure addresses constitutes a threat to the security of Canada, and the TRM must necessarily serve to reduce it. This threshold means that CSIS may not use its TRM authority to provide classified information to anyone, including elected officials, unless the purpose of providing that information is to reduce a threat.

CSIS has three types of TRMs:

- **Messaging TRMs.** CSIS pushes information, directly or indirectly, to the subject to influence their behaviour. This could involve meeting the associate of a threat actor and telling them that CSIS knows about the threat actor's activities, with the aim of having the associate report this conversation to the threat actor.
- **Leveraging TRMs**. CSIS discloses information to a third party (for example, an online platform) to enable them to act against the identified threat-related activity (for example, misinformation). The intent is to impede the threat-related activity, but the means are at the discretion of the third party.
- **Interference TRMs**. CSIS directly affects the ability of someone to do something (for example, prevents someone from meeting a target). The intent is to impede the threat-related activity.

TRMs must be reasonable and proportional to the nature and seriousness of the threat.

Before implementing a TRM, CSIS consults other departments such as Global Affairs Canada ("**GAC**"), the Department of Justice, the Royal Canadian Mounted Police ("**RCMP**") and Public Safety Canada ("**Public Safety**") on the risks of the proposed action. CSIS assesses proposed TRMs under four risk pillars:

- operational risk
- foreign policy risk assessed in consultation with GAC
- legal risk assessed in consultation with the Department of Justice
- reputational risk assessed in consultation with Public Safety.

The risks are ranked on a scale of low, medium or high, which determines the level of approval required for the TRM.

Under section 12.1 of the *CSIS Act*, if a TRM would limit a *Charter of Rights and Freedoms* right or freedom, CSIS must get a warrant before taking any measures. Since 2015, CSIS has undertaken 20 TRMs related to foreign interference that did not require warrants. It has not undertaken any foreign interference TRMs requiring warrants.

As an example, in 2021, CSIS implemented a TRM about foreign interference activities by India. The objective was to safeguard democratic institutions by telling current and former members of Parliament ("**MPs**") about India's foreign interference activities in Canada. This involved both classified and unclassified briefings and interviews with the MPs.

All briefings provided a general awareness of foreign interference and Indian efforts, while some included targeted information on India-related foreign interference issues, including the covert promotion of a pro-Government of India agenda and covert funding of political candidates, including through the use of proxies.

Information sharing to build resilience

In July 2024, the *Countering Foreign Interference Act* expanded CSIS's information-sharing capabilities. It can now share information obtained in the performance of its duties and functions with any person or entity for the purpose of building resilience against threats to the security of Canada if the following conditions have been met:

- The information has already been provided to a federal department or agency for which the information is relevant.
- The information does not contain personal information other than that of the individual receiving the information.
- The information does not contain the name of a Canadian corporation other than that to which the information is disclosed.

This new power allows CSIS to share classified information with persons who do not hold security clearances, and who are outside the federal government. The manner and extent to which this will be done remains to be seen.

Protective security briefings

CSIS can also share unclassified information by providing individuals with a protective security briefing ("**PSB**"). PSBs aim to sensitize someone to the nature of the threat they might be facing. They are almost always unclassified briefings, derived from classified information. CSIS delivered PSBs to MPs ahead of the 2021 election. I discuss PSBs in more detail in Volume 4, Chapter 15.

Sharing information on physical treats to an individual

When CSIS has information regarding a physical threat to an individual, CSIS can share that information with law enforcement, who can then warn the individual of the threat, under their duty to warn, or take other steps to address the threat. In sharing this information, CSIS may suggest a way in which an individual could be warned about the threat without disclosing classified information to the individual, including by giving police an unclassified script to use when warning the individual about the threat.

CSIS does not have a specific policy on sharing threat-to-life information with police. However, CSIS witnesses said that when it has information of a threat of physical harm or a threat to the life of an individual, CSIS immediately engages police authorities to ensure the individual is physically protected, while also taking measures to protect the source of the information. The witnesses explained that there are communication channels with law enforcement and CSIS is able to share the information quickly.

For instance, under the One Vision Framework governing information sharing between CSIS and the RCMP (which I discuss in more detail in Volume 4, Chapter 14), the RCMP can act on oral disclosures from CSIS about an imminent threat to life or threat of serious bodily harm. This is an exception to the normal course, where the RCMP is restricted from acting on information received from CSIS until CSIS provides a formal "use letter." The One Vision Framework also emphasizes cooperation at the earliest possible stage and that public safety is the highest priority for both organizations.

The Communications Security Establishment (CSE)

The Communications Security Establishment (CSE) is Canada's foreign signals intelligence ("**SIGINT**") agency, and technical authority for cyber security and information assurance. Its mandate has five aspects, set out in sections 16-20 of the *Communications Security Establishment Act*:

- Foreign intelligence, which enables CSE's SIGINT activities.
- Cybersecurity and information assurance, which enables the provision of cybersecurity advice, guidance and services to protect federal and designated non-federal systems.
- Defensive cyber operations, which allow CSE to take online actions to protect federal and designated non-federal systems from foreign cyber threats.
- Active cyber operations, which allow CSE to take online action to disrupt the capabilities of foreign threat actors.
- Technical and operational assistance, which allows CSE to help federal law enforcement and security agencies, the Canadian Armed Forces and the Department of National Defence.

CSE collects foreign SIGINT by intercepting electronic communications and information, including from the Internet. It works to determine capabilities, , intentions or activities of foreign entities in accordance with the government's intelligence priorities. CSE cannot direct its SIGINT activities at Canadians or at anyone in Canada.

CSE analyzes foreign SIGINT to inform the government about foreign threats to Canadian security, including foreign interference, and to support foreign policy and decision-making.

CSE also provides advice and assistance to defend against cyber attacks, engages in defensive and active cyber operations and can provide technical assistance to various federal entities.

When CSE assists federal security and law enforcement agencies, including CSIS and the RCMP, it is subject to the requesting agency's authorities. When a requesting agency has authority to target persons in Canada, including Canadians, CSE may assist that agency by collecting SIGINT about those persons. Any information gained by CSE belongs to the requesting agency and not to CSE.

Intelligence collection

CSE currently uses ministerial authorizations for three types of foreign intelligence collection:

- **Passive access activities**. CSE deploys equipment to covertly collect copies of information or transmissions transiting the global information infrastructure. Passive access is the building block for the majority of CSE's foreign intelligence activities.
- **Network operations activities**. CSE makes targeted modifications to, or takes advantage of vulnerabilities in, portions of the global information infrastructure. Network operations are CSE's main source of intelligence. In 2023, they accounted for most of its reporting on Canadian intelligence gathering.
- **Other foreign intelligence activities.** The third mode of foreign intelligence collection is not public and is described in the classified supplement to my report.

In undertaking its foreign intelligence mandate, the Chief of CSE (the agency head) seeks ministerial authorization to allow CSE to collect foreign intelligence in ways that would otherwise violate the laws of Canada and may inadvertently breach the reasonable expectation of privacy of Canadians or persons in Canada.

Intelligence assessment and analysis

CSE reporting is fact-based and does not include assessments or analysis of intelligence. Recipients of CSE intelligence assess its relevance and significance. CSE has started taking steps to make its products more accessible to clients, notably by prefacing them with a short summary. It has also combined several of its reports and Five Eyes' reports into standalone products and created a new line of reporting called "Tailored Intelligence Products."

These initiatives will certainly help different actors exchange views and should enable decision-makers to grasp the importance of some intelligence more easily and more quickly.

Response toolkit

Sensors on government systems

CSE's Canadian Centre for Cyber Security ("**CCCS**") has a variety of sophisticated automated sensors to defend federal government systems. These monitor information to and from government systems. They help detect suspicious activity and cyber attacks. The program has been rolled out over a number of years and now covers most federal departments. CCCS has recently begun installing these sensors on government laptops, which has increased its ability to detect and deter threats.

CCCS's cyber program is effective. It stops nearly six billion (6,000,000,000) malicious cyber incidents against the federal government each day. Each incident is an opportunity for CSE to discover information about the threat activity.

Since 2015, CCCS has worked with Elections Canada to reinforce Canadian electoral infrastructure. Since 2019, it has used sensors on Elections Canada infrastructure.

CCCS also works on request with provincial and territorial governments, including using sensors within their systems. It does this under a ministerial authorization.

Active cyber operations (ACOs)

Active cyber operations ("**ACOs**") degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of foreign states, individuals or groups that may pose a threat to Canada's national security. CSE relies on ministerial authorizations to carry out its ACOs.

CSE currently has ACOs aimed at foreign entities. For example, CSE recently implemented an ACO to counter the activities of a foreign entity that impacted Canada's security interests. In conducting these operations, CSE leverages various techniques, including activities that allow it to access online accounts or networks.

Defensive cyber operations (DCOs)

Defensive cyber operations ("**DCOs**") allow CSE to take online actions to disrupt foreign cyber threats in order to protect federal infrastructure or systems of importance to the government. CSE was ready to conduct DCOs to protect Elections Canada's systems during the 2019 and 2021 general elections. Fortunately, it was not necessary to do so.

Attributing cyber attacks

CSE uses its technical expertise to identify those responsible for a cyber event. Public attribution tied to a foreign actor is ultimately Global Affairs Canada's (GAC's) decision (see further below where GAC's Cyber Attribution Framework is described).

It is not always possible for CSE to attribute a cyber attack. Attributing cyber events is challenging, and the majority of cyber threat activity is unattributed. However, the more information CSE has on the threat landscape, common techniques and a specific cyber incident, the better able it is to attribute the activity. Novel behaviour may take CSE longer to attribute it to a particular foreign entity.

Attribution of misinformation and disinformation campaigns is more challenging. When attempting to attribute a cyber incident, CSE often obtains foreign intelligence and technical details about the incident, which assist with attribution. When it comes to misinformation and disinformation campaigns, CSE generally cannot get the technical information to make an attribution because the information does not exist, or the social media company has not provided it.

I also note that because of its mandate, CSE is only involved in attempts to attribute misinformation and disinformation campaigns if there is a "foreignness" element because CSE cannot collect signals intelligence on Canadians or individuals within Canada. Accordingly, where foreign entities use proxies in Canada to spread misinformation and disinformation, CSE's role in attempts to attribute that activity is limited.

Guidance and advice to political parties

The Canadian Centre for Cyber Security (CCCS) has produced a security guide for campaign teams and, on request, CSE advises political campaigns and parties about cyber security. Available services include:

- network architecture review and advice
- security review of information technology requests for proposals
- guidance on, and assessment of, third party cyber security service providers that meet key IT security standards.

CSE also has a Cyber Hotline for political party members. Only one issue was reported during the 2019 election period. None were reported during the 2021 election. I note that this does not mean no such issues occurred. This is especially true since the existence of the Hotline is not widely known. The political parties seem equally unfamiliar with the technical advice and services available through CSE.

Global Affairs Canada (GAC)

GAC is Canada's international relations department. It is one of the largest consumers of intelligence within the federal government. Its focus is intelligence about the capabilities, intentions and activities of foreign states. It receives intelligence from government agencies like CSIS and CSE, as well as from foreign counterparts.

Intelligence collection

GAC is primarily a consumer, not a producer of intelligence, but it nevertheless does collect some intelligence.

GAC Intelligence Liaison Officers work openly at Canadian consulates and embassies and receive information from host countries aware of their role. GAC also reports on confidential information diplomats learn from their local contacts. This includes information received through the Global Security Reporting Program, which provides specialized diplomatic reporting on security issues. This involves sensitive information that may be classified or unclassified.

Also, as explained above, the Minister of Foreign Affairs can ask CSIS to collect foreign intelligence within Canada under section 16 of the *CSIS Act*. This authority has been exercised to collect intelligence relating to certain countries and foreign interference.

Intelligence assessment and analysis

GAC's Intelligence Bureau assesses intelligence and shares it internally and externally. The Intelligence Bureau was a small team until 2019 when funding increased, allowing the Bureau to increase its assessment capacity. GAC assessments of intelligence apply a foreign policy or international relations lens. They serve two main purposes: evaluating the threat to Canadian missions and assets abroad, and informing and supporting foreign policy development.

Response toolkit

Canada engages in international relations in accordance with two international conventions, the *Vienna Convention on Diplomatic Relations* and the *Vienna Convention on Consular Relations* ("**VCCR**"). Deputy Minister of Foreign Affairs David Morrison described these as the "rules of the road" for state interactions, including with respect to embassies and consulates. If countries do not abide by the VCCR or otherwise present a threat to Canadian security, GAC can use its diplomatic toolkit.

Moreover, GAC's Rapid Response Mechanism Canada (see further below) contributes to Canada's foreign interference response by monitoring publicly available online information for misinformation and disinformation during federal elections periods and, as mentioned above, GAC also works with CSE on attributing responsibility for cyber attacks against the federal government.

Diplomatic response tools

GAC has many diplomatic tools to detect, deter or counter foreign interference. These tools are used in coordination with the rest of government.

Government decisions about which diplomatic tools to use in different situations depend on various factors, including the issue, affected interests, impact on bilateral or multilateral relationships and availability and effectiveness of other remedies. Thus, diplomatic responses are tailored. They range from quiet diplomacy to severing diplomatic relations entirely.

Diplomatic efforts will often start quietly and then increase as needed. For example, the repeated raising of an issue with a state and raising it at higher levels of seniority can communicate a warning, while denying visas to diplomats communicates a consequence.

GAC's primary tools are bilateral responsive actions. These can include communications with foreign governments through diplomatic notes or demarches. Demarches are formal state-to-state communications through diplomatic channels that convey information, a request or a position on an issue.

Demarches have a hierarchy. A phone call from a mid-level official to a foreign mission carries less weight than a call from the Minister of Foreign Affairs. Moreover, a phone call may be less significant than a diplomatic note or a face-to-face meeting.

Another example of diplomatic communications occurred before the 2019 and 2021 elections when GAC sent a circular reminding foreign missions of their duties under the VCCR to respect Canadian laws and regulations and not interfere in Canada's internal affairs. The media also reported that GAC recently briefed foreign diplomats about foreign interference.

Other bilateral responsive actions include cancelling a visit, deal or agreement; withdrawing from an event; denying diplomats visas or visa extensions; denying new diplomatic positions or missions; recalling Canada's ambassador to a country; closing foreign missions in Canada and Canada's missions abroad; and breaking diplomatic relations.

GAC can also declare diplomatic or consular staff *persona non grata* ("**PNG**"). PNGs are often public but can be done privately. A country does not have to give a reason for making such a declaration, and the declaration is not necessarily a response to the actions of the specific person declared PNG.

Additionally, GAC can impose sanctions on companies or individuals. Thus far, GAC has not used sanctions to counter foreign interference targeting democratic institutions and processes, but sanctions are fairly common in other circumstances. For example, Canada imposed sanctions on Russian oligarchs in response to Russian disinformation campaigns they sponsored about the war in Ukraine.

Beyond bilateral responsive actions, other GAC tools are:

- **Proactive responses**. Examples include active cyber operations and export restrictions.
- **Proactive bilateral and multilateral responses**. Partnering or sharing information with other governments bilaterally or at multilateral tables like the G7 or Five Eyes or partnering with civil society. For example, Canada worked with the Netherlands to develop the *Global Declaration on Information Integrity Online*, which now has 30 signatories.
- **Public communications**. Setting out Canadian positions in official statements, ministerial social media and advocacy work. These include public attributions of activities by foreign actors, using social media to highlight misinformation or disinformation campaigns, fact checking narratives and offering counter-narratives.

Diplomatic measures can be used to communicate with other countries or the public, in addition to the state at issue. For example, a public PNG declaration tells other states that consequences are real.

However, Deputy Minister Morrison remarked that the essence of diplomacy is maintaining discussions with foreign states, even adversarial ones, to advance Canada's interests. That is why, while public measures such as declaring a diplomat PNG or imposing sanctions on a diplomat or country may help deter or counter foreign interference, it can also come at significant cost to Canada.

Using GAC's diplomatic tools to deter and counter People's Republic of China (PRC) foreign interference

Canada's relationship with the People's Republic of China ("**PRC**") illustrates how GAC uses diplomatic tools to deter and counter foreign interference while maintaining a relationship with a foreign state. GAC witnesses explained that, given the PRC's global and economic significance, Canada's relationship with it is important to Canadian security and prosperity. Mr. Morrison remarked that Canada can either sit on the sidelines and watch or engage and attempt to shape the PRC's behaviour to the benefit of Canada. Diplomatic engagement seeks to do the latter.

Bilateral responsive actions: demarches and other representations

I heard that there was diplomatic activity in response to PRC foreign interference before the return of Michael Spavor and Michael Kovrig ("**Two Michaels**"), although it was not always publicly visible.

According to GAC, Canada pushed back and found ways to raise the cost to the PRC for foreign interference attempts. Government regularly raised concerns about foreign interference with the PRC and denied visas to PRC diplomats. However, until the Two Michaels returned, Canada's priority was on getting them home. It therefore had to be prudent in its interactions with the PRC. Immediately after the return of the Two Michaels in September 2021, foreign interference moved to the forefront of GAC's agenda and Canada used regularly scheduled diplomatic meetings to raise the issue.

GAC has systematically warned the PRC that foreign interference is a core issue for Canada, and that if the PRC did not address it there would be consequences. Between December 2021 and March 2023, Canada made 31 representations at all levels of seniority, including by the Prime Minister to President Xi Jinping, about PRC foreign interference, surveillance and other issues involving the security of Canada.

For example, a call took place on 17 January 2022 between the then Deputy Minister of Foreign Affairs and her PRC counterpart. This was the first formal senior-level engagement between the two following the return of the Two Michaels. The Deputy Minister put PRC officials "on notice" by calling out PRC foreign interference activity. GAC witnesses said that it was significant, and likely surprising to the PRC, that Canada made foreign interference the core topic of this meeting.

Since the fall of 2021, Canada has issued four diplomatic notes to the PRC, including two about PRC Overseas Police Stations (see Volume 4, Chapter 17). Having issued warnings through multiple meetings and notes, Canada's response progressed to concrete actions such as denying visas to PRC officials and denying a long-standing PRC request to create a new position in its embassy in Canada.

In addition, in the summer and fall of 2023, GAC officials demarched the PRC Ambassador regarding the WeChat disinformation campaign targeting

Michael Chong and a spamouflage campaign that targeted various members of Parliament (see Volume 4, Chapter 15). GAC subsequently issued public statements to denounce these two campaigns.

Some might be of the view that most diplomatic measures are not sufficient deterrents to foreign interference activities, but we must bear in mind that taking forceful measures generally leads to the recipient country taking similar measures against Canada.

Declaring Zhao Wei *persona non grata*

On 8 May 2023, Canada took a very public step in response to PRC foreign interference and declared PRC diplomat Zhao Wei *persona non grata*. On 1 May 2023, the *Globe and Mail* had published an article about Mr. Zhao's interest in Member of Parliament Michael Chong and his family.

I heard from a number of witnesses about what led to the PNG declaration.

GAC senior officials and political staff said that Mr. Zhao was declared PNG as part of a series of escalating diplomatic steps taken, most of which were not done publicly, to condemn and deter PRC foreign interference activities. I described many of these efforts above.

GAC said that a PNG declaration was already under consideration when the *Globe and Mail* article was published. Mr. Morrison recalled an interdepartmental meeting in April 2023 where all options were on the table, including expulsion of a diplomat.

When the news article on the activities of Mr. Zhao came out, GAC's Intelligence Bureau sought to update its understanding of the activities of PRC diplomats to ascertain whether they were engaging in foreign interference.

On 2 May 2023, GAC's Intelligence Bureau produced an intelligence assessment on Mr. Zhao's activities. In a memorandum informed by this assessment sent to the Minister of Foreign Affairs that same day, GAC identified a range of responses for the Minister's consideration:

- a demarche
- a demarche with a request for Mr. Zhao's immediate departure
- a demarche followed by a PNG declaration.

On 3 May 2023, in the course of this broader review of the activities of PRC diplomats, GAC received additional CSIS reports relating to Mr. Zhao. This was when GAC senior officials learned about a CSIS intelligence product from 2021. CSIS had already disseminated this intelligence product to GAC in 2021, but with limited distribution. According to GAC's Director General of Intelligence, this product was not a "smoking gun," but it provided additional information on PRC foreign interference activities. It did not say anything about a connection between Mr. Zhao and Mr. Chong.

Once senior officials within GAC saw the additional reports, including the 2021 CSIS product, GAC's Intelligence Bureau prepared a revised intelligence

assessment about Mr. Zhao. The revised assessment's conclusions were different from the conclusions of the May 2 assessment.

Records indicate that GAC officials met with CSIS, the Privy Council Office, the Prime Minister's Office and the Prime Minister on 6 May 2024 to discuss if there would be a PNG declaration. I heard that, while the Prime Minister's approval is not required to make a declaration, he is usually consulted given the seriousness and relative rarity of these situations.

The Prime Minister testified that once Mr. Zhao's behaviour in Canada became publicly known, Canada had to respond. It was no longer tenable for Mr. Zhao to occupy a diplomatic post here. GAC also concluded that with the publication of the news story, it had become less risky and costly for Canada to make a PNG declaration.

The declaration was intended to send a message to the PRC and other countries about consequences of foreign interference activities in Canada and to assist in restoring public trust.

On 4 May 2023, Mr. Morrison summoned the PRC Ambassador for an official in-person demarche on Canada's concerns about PRC foreign interference. He advised PRC officials that Mr. Zhao's position in Canada was no longer tenable. GAC asked the PRC to voluntarily withdraw Mr. Zhao, because this would avoid a responsive expulsion of a Canadian diplomat from the PRC. PRC officials refused. Ultimately, the PRC responded by expelling a Canadian diplomat of comparable standing to Mr. Zhao.

On 8 May 2023, Mr. Morrison signed a memorandum to the Minister of Foreign Affairs, which included the updated assessment on Mr. Zhao and officially recommended declaring Mr. Zhao *persona non grata*. The official declaration was made later that day.

Given the timing of this declaration, some, including Mr. Chong, reasonably considered that it was a response to the 1 May 2023 *Globe and Mail* article. GAC witnesses testified that, while the *Globe and Mail* story made Mr. Zhao's position in Canada untenable, there was a discrepancy between what the newspaper reported and what the intelligence suggested.

Mr. Morrison testified that the consensus view of the national security and intelligence community in Canada is that Zhao Wei did not engage in foreign interference with respect to Mr. Chong. Mr. Morrison said that doing research and collecting information in and of itself is not foreign interference. I discuss the topic of PRC research on MPs in Volume 4, Chapter 14.

GAC's Rapid Response Mechanism (RRM) Canada and misinformation and disinformation

As I explained in Chapter 1, in 2018, G7 members agreed to establish the G7 Rapid Response Mechanism ("**RRM**") to prevent, thwart and respond to malign and evolving threats to G7 democracies by sharing information and analyses and by identifying opportunities for coordinated responses.

GAC's RRM Canada is the permanent secretariat of the G7 RRM. RRM Canada monitors open source (publicly accessible) online information and analyzes it to identify potential manipulation by foreign actors. RRM Canada's primary focus is international online information. However, during federal general and by-elections, RRM Canada also monitors the domestic online environment for possible misinformation or disinformation. As such, RRM Canada has been a member of the Security and Intelligence Threats to Elections Task Force ("**SITE TF**") since its inception (the SITE TF and RRM Canada's role is discussed further in Volume 3, **Chapter 12**).

RRM Canada has an ongoing dialogue with many social media platforms so it can receive and share relevant information. This dialogue is not always effective. For instance, on 8 September 2023, RRM Canada followed up with Tencent, WeChat's parent company, about the disinformation campaign against Michael Chong. However, RRM Canada does not know if Tencent acted on the information, and it has had no further engagement with Tencent.

RRM Canada does not do baseline monitoring of the domestic online environment outside of election periods. However, if it learns something from international partners or comes across something as part of its international monitoring work, it shares it with the SITE TF.

Cyber Attribution Framework (CAF)

Canada uses the Cyber Attribution Framework ("**CAF**"), established in 2019, to decide whether to publicly attribute a malicious cyber attack directed at Canadian or allied networks to a state. GAC leads the CAF.

The CAF process starts with a technical assessment by CSE of the likelihood that a cyber incident was caused by a state actor. Then, Public Safety or the Department of National Defence assesses the impact of public attribution on domestic agency activities. Next, there is a legal assessment led by GAC to determine if the activity violated international law or United Nations norms of acceptable behaviour in cyber space.

GAC then conducts a foreign policy risk assessment, since public attribution is effectively "calling out" a state for its behaviour. Finally, GAC makes a recommendation to the Minister of Foreign Affairs about public attribution or other actions. The decision rests with the Minister of Foreign Affairs.

Thus far, there have been no public attributions about cyber foreign interference in democratic institutions.

However, I heard evidence about two cyber incidents, not necessarily linked to foreign interference in democratic institutions, where it was ultimately decided not to make a public attribution. In one case, there was insufficient data to attribute the event to a foreign state actor. In the other case, the decision was made for tactical reasons.

The Royal Canadian Mounted Police (RCMP)

The RCMP detects, deters and counters foreign interference through enforcement of a number of Acts, including the: (1) *Foreign Interference and Security of Information Act* ("***FISOIA***"; formerly the *Security of Information Act*); (2) *Criminal Code*; and (3) *Canada Elections Act*. The *FISOIA* and the *Criminal Code* were amended by the *Countering Foreign Interference Act* in July 2024 and now include more offences directed at foreign interference.[6]

The RCMP Federal Policing Branch works on the most serious and complex criminal threats to the safety and security of Canadians and Canadian interests, including threats to democratic institutions, economic integrity, physical and cyber infrastructure and foreign interference.[7] Five program areas have governance and oversight roles related to foreign interference: Federal Policing National Security ("**FPNS**"), Federal Policing Protective Services, Federal Policing National Intelligence, Federal Policing Criminal Operations and Federal Policing Strategic Management.

In 2018, the RCMP temporarily established within FPNS a Foreign Actor Interference Team, comprised of seven members, focused on foreign interference. The team became permanent in 2020 and has had dedicated funding since 2023. It educates and guides investigative units about foreign interference.

Specific foreign interference training is not currently part of the RCMP Depot Division curriculum. RCMP witnesses told me that the training provided at Depot is geared towards preparing recruits for front-line policing. The national security investigator's course does include some foreign interference training, and the RCMP is currently working on developing an advanced national security criminal investigator's course and more specialized foreign interference training. Historically, the RCMP's Federal Policing budget resources were consistently displaced to fund other organizational priorities (such as Contract and Indigenous policing). However, there is a growing recognition that a level of specialization in foreign interference and dedicated foreign interference-related resources are required.

Response toolkit

Criminal investigations

The primary responsibility for foreign interference investigations lies with FPNS. Investigations are led by Integrated National Security Enforcement Teams ("**INSETs**") and National Security Enforcement Sections ("**NSESs**") in RCMP divisions across Canada. NSESs are made up only of RCMP officers,

---

6 The *Countering Foreign Interference Act*, introduced as Bill C-70, is discussed in detail in Volume 3, **Chapter 12**.

7 The RCMP calls foreign interference "foreign actor interference."

whereas INSETs bring together trained personnel from the federal, provincial and municipal levels of law enforcement and the national security and intelligence community.

INSETs work in collaboration with local police. Both INSETs and NSESs are directed by RCMP Headquarters.

Extraterritoriality poses an investigative challenge for the RCMP. However, it has officers in analyst and liaison positions abroad, as well as international partnerships (for example, with INTERPOL) that facilitate inter-agency cooperation in international investigations.

Criminal investigations involving certain public institutions or individuals, such as politicians, must be pre-approved by the Assistant Commissioner of FPNS through a sensitive sector request. This is because these kinds of investigations may negatively impact a fundamental institution of Canadian society. In addition to politics, other sensitive sectors include religious institutions, media, academia and trade unions.

At my request, the RCMP reviewed its investigative holdings since 2018 for work on foreign interference. It identified over 100 investigations into foreign interference activities in various areas: economic integrity, critical infrastructure, proliferation, transnational repression, theft of intellectual property and protected information, disinformation and democratic institutions. Out of these, the RCMP identified only six occurrences of possible foreign interference targeting Canada's democratic processes. Five of these investigations were closed because the RCMP concluded that the allegations were unfounded. One is ongoing.

I note here that the RCMP's ability to investigate is limited to activities that may constitute an offence or, in other words, illegal activities. As such, new criminal offences introduced by the *Countering Foreign Interference Act* may assist the RCMP in investigating foreign interference threat activities.

Disruption

As discussed in Volume 2, Chapter 5, there are significant challenges associated with prosecuting foreign interference-related offences when they are based on intelligence. This is one of the reasons the RCMP acknowledges that prosecutions are no longer necessarily the "gold standard" of threat mitigation.

Deputy Commissioner Mark Flynn said that when prosecution is not possible or not an efficient use of resources, the RCMP should look for other opportunities to reduce the threat to public safety and pursue those with equal vigour. Disruption measures such as regulatory sanctions, financial intervention, immigration inadmissibility and community policing may be used in the foreign interference context. The RCMP's goal is to disrupt and dismantle threat actors, as well as to hold them accountable.

The RCMP's response to PRC Overseas Police Stations was an example of disruption. The RCMP sent uniformed officers to neighbourhoods with suspected stations. The goal was to:

- shine a light on the problem to help investigative efforts
- show affected communities that the RCMP was taking the issue seriously
- build trust with community members.

Previously, the RCMP would have taken a more discreet approach with a less visible investigation. The Overseas Police Stations and the government's response, including various views on the RCMP's response, are discussed further in Volume 4, Chapter 17.

Engagement with the public and stakeholders

Another means by which the RCMP counters foreign interference is by engaging with the public and stakeholders within the community to build resilience. The RCMP's outreach activities are discussed further in Volume 4, Chapter 16.

Public Safety

Public Safety develops and provides advice to the Minister of Public Safety on national security matters. The Minister is responsible for five portfolio agencies: the RCMP, CSIS, the Canada Border Services Agency, the Correctional Service of Canada and the Parole Board of Canada. Of these, CSIS and the RCMP are most directly engaged in countering foreign interference. As I explained in Volume 2, Chapter 6, the agencies report directly to the Minister of Public Safety but do not report to the Deputy Minister.

Policy development and coordination

Public Safety's primary function is to facilitate operations of the agencies under the Minister's responsibility through the development of policy. It develops policy to remedy gaps in the government's ability to counter threats and advises the government on national security, community safety and criminal justice, as well as emergency management issues.

Public Safety is not directly accountable for operational responses to intelligence and does not direct immediate threat responses. Rather, it compiles information and convenes discussions that allow the government to interpret information and contribute to decisions about the government's response.

Public Safety is a consumer of intelligence. For Public Safety, intelligence is contextual and increases its understanding of operational challenges, which

supports its policy work. When senior Public Safety officials attend briefings by CSIS and the RCMP, one of their main roles is to provide current context for the agency delivering the briefing.

The Public Safety Deputy Minister, assistant deputy ministers and directors general sit on and until recently chaired or co-chaired several inter-departmental committees addressing threats to the security of Canada. I discuss the current inter-departmental committee governance structure later in this chapter.

In March 2023, the government appointed a National Counter Foreign Interference Coordinator ("**NCFIC**") within Public Safety. I discuss the role of the NCFIC further below in relation to national security coordination and governance.

The Privy Council Office (PCO)

PCO coordinates the public service's support of the Prime Minister and Cabinet and reports directly to the Prime Minister. PCO has convening and challenge functions and plays a key role in coordinating the national security and intelligence community with respect to both policy and operations.

PCO's convening function means that it brings together the government's security and intelligence community to ensure inter-departmental coordination and awareness of threats and responses. This applies to policy development and operations. This convening of the community is critical, because it is rare that an issue or proposed policy sits narrowly within the mandate of a single minister or department.

PCO also has a challenge function. This means that it asks questions, offers advice and gives guidance to other departments or agencies based on a broad, whole-of-government perspective. Because PCO does not have the accountabilities of departments or agencies reporting directly to ministers, it can offer a bird's-eye view.

PCO does not develop or initiate policy itself. Rather, it works with lead departments on policy initiatives so that all departments whose work is relevant to an issue are consulted before the initiative goes to Cabinet. Part of its role is to flag competing tensions and priorities for ministers to allow them the opportunity to debate, discuss and weigh various considerations when making decisions.

PCO is chair or co-chair of multiple inter-departmental governance committees, including committees that coordinate operational responses to national security threats. I discuss these committees and the national security governance structure in more detail below.

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

The branch of PCO most directly involved in matters of national security is the office of the National Security and Intelligence Advisor to the Prime Minister ("**NSIA**").

The NSIA provides the Prime Minister and Cabinet with strategic assessments, strategic policy advice and operational advice about national security, intelligence, foreign policy and defence. The NSIA is a coordinator within the national security and intelligence community and can bring departments and deputy ministers together to look at particular issues, respond to current events and manage crises. As further explained in Volume 4, Chapter 14 the NSIA is also responsible for the flow of intelligence within PCO and to the Prime Minister.

The NSIA reports directly to the Clerk of the Privy Council, who is the Deputy Minister to the Prime Minister, Secretary to Cabinet and head of the federal public service. The NSIA is supported by a Deputy NSIA, a position established in 2023 due to the ever-increasing workload and travel schedule of the NSIA.

The NSIA oversees a number of secretariats, four of which are relevant to foreign interference.

The **Security and Intelligence Secretariat** ("**PCO-S&I**") gives policy advice and support to the NSIA on national security and intelligence matters, including coordinating operational responses to national security issues.

Through its Strategic Policy and Planning Unit, PCO-S&I coordinates and advises on national security policy development. PCO-S&I performs PCO's challenge function, ensuring that departmental proposals meet the needs of Cabinet and are consistent with the government's overall policy direction. The challenge function operates at all levels, from analysts to the most senior ranks.

Through its operations unit, PCO-S&I coordinates and advises on security and intelligence operations, events and issues. This is done in part by chairing, co-chairing or acting as secretariat to key inter-departmental committees whose mandates include coordinating operational responses to national security threats.

PCO-S&I is also responsible for coordinating Cabinet's development of intelligence priorities.

The **Intelligence Assessment Secretariat** ("**PCO-IAS**") produces strategic intelligence analyses and assessments on foreign trends and developments that impact Canadian interests. PCO-IAS's work is policy relevant and policy neutral, meaning that intelligence assessments reflect the government's intelligence requirements, but are not influenced by desired policy or operational outcomes. Analysis draws from any source, including classified intelligence, diplomatic reporting and open sources. In recent years, PCO-IAS has begun to integrate both foreign and domestic intelligence into its assessments.

The **National Security Council Secretariat** supports the NSIA in their capacity as Secretary of the National Security Council, which I discuss below.

The **Foreign and Defence Policy Advisor Secretariat** monitors, coordinates and provides advice to senior PCO officials and the Prime Minister on foreign policy and defence issues.

Open source intelligence (OSINT)

As I discuss in Volume 2, Chapter 5, open source intelligence ("**OSINT**") is publicly available information that can be used for intelligence purposes through collection and analysis. Various government departments have OSINT capability and use OSINT to advise their ministers and deputy ministers. However, there is no assessment secretariat for domestic OSINT like Canada has for foreign intelligence.

I heard the government is trying to identify policy or legislative change necessary to address gaps in the cohesion of OSINT activities occurring across the government. One possibility being considered is housing a central OSINT assessment secretariat within Public Safety, since it is a key player in responding to foreign interference. The department already compiles information and convenes discussions that allow the government to interpret information and contribute to decisions about the government's response.

OSINT is seen as increasingly valuable. It is becoming a more and more prominent part of the government's considerations when making national security decisions. According to former NSIA Jody Thomas, OSINT is critical to understanding societal cohesion, impacts on democratic processes and public confidence in institutions, particularly with respect to social media.

Martin Green, former Assistant Secretary of PCO-IAS, noted that the broader use of OSINT is a big discussion point amongst the Five Eyes. He said OSINT could be of particular value to Canada because the largest producers of covert information tend to be other countries, not Canada. OSINT offers an opportunity to "Canadianize" our intelligence, to be less dependent on our allies and to make intelligence easier to use and share with other levels of government.

There are several challenges to mining open source data, including definitional and legal issues, particularly with respect to privacy. Mr. Green noted that Canadians might object to government harvesting their open source online data.

However, if something bad were to happen (for example, if the Freedom Convoy protests in 2022 had resulted in serious violence), Canadians might ask why the government was not monitoring social media for warning signs.

In Mr. Green's view, if we approach OSINT in the right way, it could give senior decision-makers tools to speak to the public and increase public confidence in government.

11.4 National Security Coordination and Governance

Coordinating the national security community and its response to foreign interference is a challenge. This section describes the structures the government has put in place to try to meet that challenge.

The role of inter-departmental committees

Inter-departmental committees, staffed by senior public servants, are a critical vehicle for information sharing, policy discussion and response coordination across government. Since issues are typically relevant to more than one agency or department, inter-departmental committees are essential mechanisms of horizontal coordination for national security policy, operations and intelligence assessment. They are a key part of how the various departments and agencies involved in national security communicate with each other, keep each other informed of issues and decide what to do about them.

Committees vary in terms of their membership, areas of focus, frequency of meetings and level of seniority. Committees at the deputy minister level are often mirrored at the assistant deputy minister and director general levels so that important information is relayed vertically through the ranks to the most senior levels of the public service. Similar committees or groups also exist less formally at the working level.

The number, mandate and composition of committees change and evolve over time. PCO has recently led a process to streamline the inter-departmental committee structure, which had become cumbersome and somewhat duplicative, as committees were not formally disbanded as they became dormant over time. The intent of the restructuring was to improve information flow and increase overall efficiency and effectiveness. I would add that, in my view, it is essential to avoid needlessly multiplying committees. While they are both useful and necessary, they may also, as we know, lead to extensive discussions to find a consensus, with little action to show for it.

This effort began in the fall of 2023 and was ongoing when the Commission's public hearings ended.

Below, I first describe the committees under the former structure most relevant to foreign interference and then I describe the revised structure. The committees focused specifically on elections security are not included here but are mentioned in Volume 2, Chapter 6. Committees marked with an asterisk (*) continue to exist under the new governance structure. I describe in the first section their former functioning, and in the second section their current functioning.

Deputy Minister Committee on Operational Coordination (DMOC)*

The Deputy Minister Committee on Operational Coordination ("**DMOC**") was an informal meeting of deputy ministers chaired by the NSIA, which met every week to discuss a variety of operational matters. Deputy ministers shared intelligence on incidents to ensure a coordinated approach on issues the NSIA deemed important. DMOC had a large membership, extending beyond the traditional members of the national security and intelligence community: for example, it included Transport Canada, the Coast Guard and Immigration, Refugees and Citizenship Canada.

The supporting assistant deputy minister committee to DMOC was the Assistant Deputy Minister Committee on National Security Operations ("**ADM NS Ops**"). It was responsible for ensuring situational awareness of key operational issues across the national security and intelligence community. It also facilitated strategic coordination across government in response to national security events or emergency situations.

Deputy Minister Committee on Intelligence Response (DMCIR)

The Deputy Minister Committee on Intelligence Response ("**DMCIR**") also chaired by the NSIA, evolved out of DMOC as a forum for a smaller number of deputy ministers (CSE, CSIS, GAC, Public Safety, the RCMP and PCO's Foreign and Defence Policy, Emergency Preparedness and Democratic Institutions and Machinery of Government secretariats) to discuss particularly sensitive information and/or intelligence reporting.

DMCIR's mandate was to identify and discuss relevant, actionable intelligence, including on potential foreign interference, and decide how to respond with coordinated operational, enforcement or policy action. It reviewed operational and tactical intelligence reporting on specific, urgent and short-term issues requiring a response. For example, DMCIR was the main forum through which the government coordinated its response to incidents such as the WeChat disinformation campaign that targeted Michael Chong in the summer of 2023 and the spamouflage campaign that targeted members of Parliament in the fall of 2023.

DMCIR was supported by a subcommittee of ADM NS Ops, called "ADM NS Ops Tactical," which recommended intelligence for discussion at DMCIR, provided advice to deputy ministers on options to address intelligence and served as a coordinating body to follow up on DMCIR actions.

Many witnesses spoke to the importance of DMCIR. Former CSIS Director David Vigneault said it became one of the key ways that intelligence relevant to the work of deputy ministers was identified and discussed in an organized manner.

Deputy Minister Intelligence Committee (DMIC)

The role of the Deputy Minister Intelligence Committee ("**DMIC**"), also chaired by the NSIA, was to review longer term, strategic and forward-looking intelligence assessments. It was supported by the Assistant Deputy Minister Intelligence Assessment Committee, which discussed strategic intelligence assessment products produced by PCO's Intelligence Assessment Secretariat (PCO-IAS) and other sources.

Deputy Minister National Security Committee (DMNS)*

The Deputy Minister National Security Committee ("**DMNS**"), co-chaired by the NSIA and the Deputy Minister of Public Safety, looked at security, defence and foreign policy issues and priorities, and the linkages between them. It was a key committee for developing policy on national security and coordinated the government's response to current and emerging issues. Core membership included the Canadian Armed Forces, the Canada Border Services Agency, CSIS, CSE, the Department of Justice, Innovation Science and Economic Development, the Treasury Board Secretariat, the Department of National Defence, PCO, Public Safety and the RCMP.

DMNS was supported by Assistant Deputy Minister National Security Policy ("**ADM NS Pol**") and Assistant Deputy Minister Intelligence ("**ADM INT**") Committees. Public Safety and PCO co-chaired ADM NS Pol, which was a strategic-level forum for senior members of the national security and intelligence community to meet on the development and implementation of policy related to national security. ADM INT was responsible for implementation, management and oversight of the government's intelligence priorities and requirements. This included discussions on government intelligence needs, operational gaps and coordination.

Deputy Minister Committee on Cyber Security (DMCS)

The Deputy Minister Committee on Cyber Security ("**DMCS**"), co-chaired by Public Safety and CSE, developed and led Canada's cyber security policies and operations. DMCS was supported by the Assistant Deputy Minister Committee on Cyber Security.

Other deputy minister committees

There also used to be country-specific committees, such as the Deputy Minister China Committee ("**DMCC**"). Chaired by GAC, DMCC would meet to discuss Canada's strategic approach to China, including issues about foreign policy, and sometimes, foreign interference. DMCC was supported by the Assistant Deputy Minister China Committee.

The revised governance structure

As I mentioned above, the government revised this inter-departmental committee structure during the Commission's mandate. The Commission requested and received an update on the status of this restructuring before finalizing this report.

My understanding is that the governance structure now has five deputy minister committees instead of approximately a dozen. The new committees are:

- Deputy Minister Committee on Operational Coordination ("**DMOC**")
- Deputy Minister Committee on Intelligence Action ("**DMIA**")
- Deputy Minister Committee on National Security, Cyber, and Intelligence Policy ("**DMNS**")
- Deputy Minister Protection Committee ("**DMPC**")
- Deputy Minister Committee on Economic Prosperity and Security ("**DMES**").

PCO chairs all the committees, with three chaired by the NSIA (DMOC, DMIA and DMNS). The government's view is that this revised structure will improve centralization and efficiency of the committees. Each committee's membership differs slightly, but the core national security agencies and departments are generally represented. All committees invite other deputy ministers on an *ad hoc* basis.

DMOC continues to oversee national security incident and issue management and coordinates security and intelligence activities and operations. It is also a forum for operational updates and discussion. Whereas DMIA is designed to proactively use intelligence, DMOC is reactively focused on the most pressing and time sensitive operational files. Meetings are generally at the Top Secret level.[8]

DMIA replaces DMCIR as a forum for discussing particularly sensitive information and intelligence reporting. DMIA then directs responses and advises government. The committee is intended to enable the use of contextualized intelligence and prevent strategic surprise, as well as enhance coordination and efficacy of the intelligence community. DMIA is intended be proactive and geared towards identifying issues, finding solutions and taking action. Both intelligence producers and key intelligence consumers participate.[9] Meetings are generally held at the Top Secret level.

---

[8] The members of DMOC are: the PCO Foreign and Defence Policy Advisor, Public Safety, PCO Deputy Secretary to Cabinet for the Public Inquiry on Foreign Interference, CSE, CSIS, Transport Canada, the RCMP, Department of National Defence and the Canadian Armed Forces, GAC, Immigration, Refugees and Citizenship Canada and Canada Border Services Agency.

[9] The members of DMIA are: Public Safety, GAC, Department of National Defence and the Canadian Armed Forces, CSE, CSIS, the RCMP and PCO Deputy Secretary Governance.

DMNS oversees and coordinates national security and intelligence policy development and implementation. It also provides strategic policy advice and direction on medium and long-term national security and intelligence issues. Where appropriate, it reviews national security and intelligence policy recommendations or products destined for Cabinet. DMNS is responsible for the overall policy and strategic direction of the security and intelligence community. Meetings are generally at the Secret level.[10]

DMPC oversees the protection and security of ministers, other officials and visiting foreign dignitaries. While the overall security of events is the responsibility of the lead department or agency, DMPC is responsible for the protection of individuals under its mandate. For instance, DMPC is responsible for making recommendations to the Minister of Public Safety on who should be designated to receive protection based on threat analyses and gives advice to the RCMP about the level of protection that should be offered. Meetings are generally at the Secret level.[11]

At the time of writing, **DMES**'s terms of reference were still being developed. My understanding is that its mandate is to support the coordination of approaches that protect Canada's economy and critical sectors. It is not a decision-making committee. The government expects DMES will be co-chaired by GAC and the NSIA.[12]

The evolving role of the National Security and Intelligence Advisor (NSIA)

The NSIA convenes the national security and intelligence community and works with other departments. The NSIA has the ability and the authority to call departments and deputy ministers together to look at particular issues, respond to current events and manage crises. Other departments can bring together deputy ministers or assistant deputy ministers at various times, but the convening authority of PCO is broad and more pronounced.

Over the last year, further steps were taken to strengthen the NSIA's role in coordinating the national security and intelligence community.

---

10 The members of DMNS are: Public Safety, GAC, Department of National Defence and the Canadian Armed Forces, the Department of Justice, CSE, CSIS, the RCMP and Canada Border Services Agency.

11 The core members of DMPC are: Public Safety, Treasury Board of Canada Secretariat, Canadian Heritage and PCO. The auxiliary members of DMPC are: the RCMP, CSIS, CSE, the Sergeant-at-Arms, the Public Prosecution Service of Canada and Integrated Terrorism Assessment Centre.

12 The members of DMES are: Department of Finance, Innovation, Science and Economic Development Canada, GAC, Public Safety, Natural Resources Canada, CSIS, CSE, Transport Canada, Canada Border Services Agency, HOM-WSHDC and the RCMP. Other deputy ministers, including Canadian Heritage, Treasury Board of Canada Secretariat and Crown Indigenous Relations, are invited to DMES meetings.

First, the Prime Minister elevated the NSIA position to the rank of a Deputy Clerk position. The current Clerk, John Hannaford, explained that this signals the importance of the position and strengthens the influence of the NSIA within the deputy minister community.

Second, the NSIA is now secretary of the National Security Council, a Cabinet Committee created in September 2023, which I discuss in more detail below. This reinforces the role of the NSIA as the point of integration for government on national security issues, and gives the NSIA a lever to convene and control the Council's work.

Third, the Prime Minister sent a mandate letter to the NSIA for the first time, which was published by PCO on 25 November 2024. The letter reflects the NSIA's current responsibilities, including for the flow of intelligence and analysis to the Prime Minister, their coordination role on national security decisions, including enhancing awareness amongst ministers, their role in coordinating operational responses to major incidents and their role in supporting the National Security Council and implementing its decisions. I view the publication of a mandate letter to the NSIA as a useful initiative. It should become standard practice.

The mandate letter also sets out several specific priorities for the NSIA intended to be informed by the reports of the Independent Special Rapporteur on Foreign Interference, the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians, as well as the work of this Commission:

- National Security Strategy: the NSIA is to produce a renewed National Security Strategy in 2025 with an integrated framework for Canada's national security, defence and diplomatic position. The strategy will be developed through the National Security Council.
- International engagement: the NSIA is to engage with international partners on national security, foreign and defence policy and to explore the potential for new bilateral and multilateral partnerships to advance Canada's interests and security.
- Intelligence priorities: the NSIA is to refresh Canada's intelligence priorities on an annual basis, ensuring that they align with the strategic direction set by the National Security Council and are communicated publicly.
- Intelligence assessment: the NSIA is to modernize the intelligence assessment process and to systematize the flow of information across government.
- Communications and engagement: the NSIA is to improve engagement with stakeholders, including parliamentarians, diaspora communities and other orders of government on national security to raise awareness, identify and counter threats and inform priority setting.

- Emergency preparedness: the NSIA is to support federal efforts to coordinate Canada's federal emergency preparedness and response capacity.

The NSIA has also been asked to consider whether anything further is required to accomplish this mandate.

The evidence and review of the processes put in place to counter foreign interference satisfy me that the function of the NSIA is very important, even critical. Having had the opportunity to hear from many of those who have occupied that position in the past, as well as the present, I was able to observe that this position is always entrusted to senior and very experienced public servants. I also note, however, that many individuals have filled this position. In my opinion, the high turnover rate probably played a part in some of the communication issues within government that have been identified by reviewers.

The role of the National Counter Foreign Interference Coordinator (NCFIC)

As I will explain in Volume 3, **Chapter 12**, the creation and placement of a counter foreign interference coordinator had been a topic of discussion and debate within government since at least 2020. The NCFIC position was eventually created in March 2023.

PCO witnesses told me that it was decided to house the position at Public Safety, not PCO, because Public Safety is the policy lead for national security and foreign interference. The decision to place the NCFIC at Public Safety recognizes that accountabilities lie with ministers and deputy ministers, not with PCO. Witnesses explained that direct involvement of PCO in matters could compromise its challenge function. PCO is supposed to be the objective coordinator, convenor and challenger, not the one directly doing things.

The creation of the NCFIC role led to much discussion about what the role should be, where it fit in the governance structure and the relationship between it and governance tables and committees. For instance, should the NCFIC work on their own to a certain extent, and then bring their work to a committee? Should committees work independently of the NCFIC? Should committees be involved in the NCFIC's work at all?

The current NCFIC, Sébastien Aubertin-Giguère, told me that because there were already many committees and much going on in this arena, it was better to leverage the existing structure and mechanisms rather than create a whole separate stream of governance for foreign interference. The NCFIC is a regular participant at ADM NS Ops, ADM NS Ops Tactical (which frequently deals with foreign interference), ADM NS Pol and other assistant deputy minister meetings whenever the topic is relevant to foreign interference.

In mid-October 2023, around the time that work on revising the inter-departmental committees was beginning, the NCFIC's role and place within government became a focus of discussion at a Deputy Ministers Committee on Intelligence Response (DMCIR) meeting.

Senior officials realized that they did not all have the same expectations for the NCFIC. The discussion went back to first principles, questioning whether the NCFIC should coordinate from a policy or operational perspective, and whether it should be housed at Public Safety or PCO. At the end of the meeting, DMCIR members agreed there was a need to revisit the purpose of the role and review its framework.

Ultimately, the NCFIC role has remained policy coordination, rather than operational. PCO witnesses explained that operational coordination is already done by PCO, which is better suited to do this in light of its convening function. Many witnesses commented that the role of the NCFIC is still very new and remains a work in progress. I agree with them, and add that if the role is properly defined, the NCFIC may be able to solve many of the coordination and communication issues that emerged in the evidence.

Cabinet committees

Cabinet has committees focused on specific policy areas. Each Cabinet committee is supported by a PCO secretariat. The new National Security Council is particularly relevant to foreign interference.

Policy or legislative initiatives are generally deliberated at Cabinet committees before they go to full Cabinet. Initiatives are presented to Cabinet committees in documents called "Memoranda to Cabinet." Memoranda to Cabinet go through a process of inter-departmental consultation and discussion by ministers before being considered by a Cabinet committee. Committees then make recommendations to Cabinet for decision. Cabinet decisions are sent back to departments for implementation.

Cabinet committees that may address foreign interference issues include the Cabinet Committee on Global Affairs and Public Security ("**CCGAPS**"), the Incident Response Group ("**IRG**") and the recently created National Security Council.

CCGAPS considers issues about Canada's engagement with, and participation in the international community, including trade promotion and diversification. It is responsible for issues related to domestic and global security and sets intelligence priorities. CCGAPS advances policy work in the area of national security.

The IRG is an *ad hoc* Cabinet committee that can be activated in response to a specific situation. It provides a tactical and operational forum for ministers and deputy ministers to coordinate responses to specific incidents. It is chaired by the Prime Minister, and its membership depends on the situation it is addressing.

As noted above, the National Security Council was established in 2023. Chaired by the Prime Minister, and with the NSIA as Secretary, the National Security Council creates a standardized process for bringing intelligence to Cabinet and is focused on long-term strategic planning. It does not make operational decisions but guides and orients government's strategic actions. Permanent members include the Minister of Public Safety, Minister of National Defence and Minister of Foreign Affairs. The committee also invites other ministers on an *ad hoc* basis, depending on the agenda.

The Prime Minister said the impetus for establishing the National Security Council was in part that IRGs had had to be stood up on a regular basis in recent years in response to various events. In the course of this, questions had sometimes arisen about future planning and the need for strategic thinking. The National Security Council provides a dedicated Cabinet-level forum intended to allow a strategic, whole-of-government approach to national security issues.

As with the IRGs, a key feature of the National Security Council is that senior public servants (usually deputy ministers and heads of agencies) are present and participate in discussions with ministers. This allows for in-depth deliberations and a coherent strategic focus.

Witnesses testified that the National Security Council is a significant innovation that has already proven useful. The current Clerk, Mr. Hannaford, described it as "extraordinarily important."

It is apparent from the evidence above that the government has for some time been striving to strengthen and simplify the governance structure relevant to countering foreign interference. It is too early to assess the changes made, let alone those under discussion, but the rethinking was necessary. I was able to see the complexity of the structure that had been in place until recently and how it could complicate decision-making.

11.5 Conclusion

Canada has a wide range of departments, agencies and governance structures that respond to foreign interference. As my discussion about Canada's inter-departmental committees makes clear, this is an area where things are dynamic and ever-changing. In the next chapter, I further discuss these changes by looking at policy and legislative initiatives that have occurred in recent years in response to the threat of foreign interference.

CHAPTER 12

Policy and Legislative Initiatives

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.*

12.1 Introduction

In this chapter, I discuss two key parts of the government's work to detect, deter and respond to foreign interference: the Plan to Protect Canada's Democracy and the Countering Hostile Activities by State Actors Strategy. I also briefly touch on newer developments.

In 2016 and 2017, Russia used cyber tools and disinformation campaigns to try to interfere in a range of democratic events: the United States ("**US**") and French presidential elections, German parliamentary elections and the United Kingdom's vote on its membership in the European Union (Brexit).

These events indicated potential vulnerabilities in electoral processes. They also raised questions about how governments should respond in such situations. The US election produced what became known as the "Obama dilemma," in reference to the dilemma that the President faced when he was aware of Russian interference but felt he could not publicly intervene because he feared being seen as interfering with the election for partisan gain.

The government paid close attention to these events and, in 2019, announced a series of initiatives collectively called the Plan to Protect Canada's Democracy ("**Plan**"). It was intended to help protect Canada's electoral processes from threats seen in other countries. The Plan is still in place and there are ongoing discussions about how it should evolve.

In parallel to the development of the Plan in 2018, the government began work on the Countering Hostile Activities by State Actors Strategy ("**HASA Strategy**"). Hostile Activities by State Actors ("**HASA**") refers to actions by hostile states, or their proxies, that are deceptive, coercive, corruptive, covert, threatening or illegal, yet fall below the threshold of armed conflict, and which undermine Canada's national interests. While the Plan focused on protecting elections and democratic institutions, the HASA Strategy was about much broader policy and legislative initiatives to respond to the full range of foreign interference threats that Canada can face. The intention was to have a whole-of-government and whole-of-society response to HASA. In 2022, a Memorandum on HASA was submitted to Cabinet. This included a proposal to consult on the legislative amendments that would become Bill C-70, the *Countering Foreign Interference Act*, as well as policy and resourcing proposals.

12.2 The Plan to Protect Canada's Democracy

The origin of the Plan

On 1 February 2017, the Prime Minister issued a mandate letter to Karina Gould, then Minister of Democratic Institutions, directing her to lead, with the Ministers of National Defence and Public Safety, the government's efforts to defend Canadian electoral processes from cyber threats.

In the months that followed, Minister Gould collaborated with several ministers, met with the heads of government agencies and consulted with political parties to help develop Canada's response.

While Russia was viewed as the greatest foreign interference threat when this work began, in the years that followed the People's Republic of China ("**PRC**") emerged as a key threat actor. The work moved beyond addressing general cyber threats from Russia to responding to a wider range of foreign interference threats to Canada's democracy.

The result of these efforts was the Plan, which was publicly announced on 30 January 2019.

Content of the Plan

The Plan has four pillars:

- combating foreign interference
- promoting institutional resilience
- building citizen resilience
- establishing rules of the road for digital platforms (since renamed "Building a Healthy Information Ecosystem").

Much of the evidence I heard about the Plan centred on two key institutions that were created to respond to foreign interference threats during elections: the Security and Intelligence Threats to Elections Task Force ("**SITE TF**") and the Critical Election Incident Public Protocol ("**CEIPP**"). The Plan also included a bundle of other initiatives designed to build societal resilience against misinformation and disinformation.

The Security and Intelligence Threats to Elections Task Force

The SITE TF was established in August 2018, while the Plan was still in development, to coordinate efforts to prevent covert, clandestine or criminal activities from interfering with the Canadian electoral process. It is made up of representatives from the Communications Security Establishment ("**CSE**"),

the Canadian Security Intelligence Service ("**CSIS**"), the Royal Canadian Mounted Police ("**RCMP**") and Global Affairs Canada ("**GAC**"). I discuss the tools and capabilities of each SITE TF member in Volume 3, **Chapter 11**.

The SITE TF is an information sharing and coordinating forum, not a senior decision-making body. Its members coordinate the review of election-related intelligence, provide situational awareness and share information so that responses can be taken where needed. Individual members maintain their independent authorities to act.

The Critical Election Incident Public Protocol and the Panel of Five

The CEIPP is a Cabinet Directive made public on 9 July 2019. It requires five senior public servants, called the "Panel of Five" (or "**Panel**"), to communicate with Canadians if Canada's ability to have a free and fair election is threatened. Its members are the:

- Clerk of the Privy Council ("**Clerk**")
- National Security and Intelligence Advisor to the Prime Minister ("**NSIA**")
- Deputy Minister of Justice and Deputy Attorney General
- Deputy Minister of Public Safety
- Deputy Minister of Foreign Affairs.

During elections, the Panel receives information from the SITE TF and other sources. If it concludes that an incident, or an accumulation of incidents, threatens Canada's ability to have a free and fair election, then the government issues a public statement to notify Canadians of the incident. The standard of an incident or series of incidents threatening Canada's ability to have a free and fair election that the Panel uses to determine whether it should make a public announcement was referred to as "the threshold" during the Commission's proceedings. The assessment of whether the threshold is met is considered at both riding and national levels. Panel decisions are made by consensus.

The Panel was established to remove political interests from the evaluation and announcement of threats to the electoral process. By relying on non-partisan senior public servants, the government sought to avoid conflict of interest issues that could arise if elected officials campaigning for political office were responsible for raising public concerns about foreign interference.

Minister Gould explained why the government designated these five senior public service positions in particular. She said they have a deep understanding of the nature of intelligence and its limits. They also bring different perspectives, which means the Panel can assess factual situations with adequate nuance.

If the threshold is met, the Panel informs the Prime Minister, other major party leaders or other designated party officials and Elections Canada that a public announcement will be made. Immediately afterwards, the Clerk, on behalf of the Panel, either issues a public statement or asks the relevant agency head(s) to do so.

The threshold for a public announcement is high. There must be more than a mere possibility of a threat to an election. François Daigle, former Deputy Minister of Justice and Deputy Attorney General, and a Panel member in 2021, told me the Panel looked for information that allowed them to determine if an incident was probable and would have a probable impact on the election.

In assessing whether an incident is probable, the Panel considers the credibility and reliability of the intelligence it receives. In assessing the impact of the incident, the Panel considers factors such as the incident's reach, scale, source, relevance, lifespan, ability to self-correct and whether there are other options to mitigate risks to a free and fair election.

The reason for a high threshold is a concern that Panel intervention might do more harm than good because the moment a public announcement about foreign interference is made, confidence in the election can be undermined. It can also negatively affect public confidence in Canada's democracy as a whole. There is the further potential that the Panel itself would be viewed as partisan and interfering in the election. In addition, it is possible that foreign countries could try to cause an announcement to be made to undermine confidence in elections or amplify disinformation.

Although the Plan was an excellent initiative, my understanding is that the population knows little about, or is unaware of, the Panel of Five, its composition and its mandate. It seems essential to me that the Canadian population be familiar with the Panel's role if we want the public to accept a potential intervention by the Panel. I hope that the Commission's work will contribute to making the Panel better known, but I know that this is not nearly enough. The government needs to dedicate itself, as of now, to ensuring that the Panel and its role are known to the majority of the population.

The Canada Declaration on Electoral Integrity Online

Disinformation online can create confusion and exploit existing societal tensions. As part of the Plan, the government worked with social media platforms to increase the transparency, authenticity and integrity of these platforms to help safeguard elections. One component of this approach was the Canada Declaration for Electoral Integrity Online ("**Declaration**").

The Declaration is a voluntary agreement that establishes a set of commitments between platforms and the government to safeguard federal elections from malicious interference and build a healthier online ecosystem. The Declaration does not have the force of law and not all social media platforms are signatories.

The Digital Citizen Initiative

One of the broader goals of the Plan was to build citizen resiliency. The Department of Canadian Heritage ("**Canadian Heritage**") is the lead for this work. Canadian Heritage's Digital Citizen Initiative ("**DCI**") is a strategy that aims to support democracy and social cohesion by building resilience against online disinformation. It also builds partnerships to support a healthy information ecosystem. The Canadian Heritage Digital and Creative Marketplace Framework develops policy around online harms and disinformation.

Based on the evidence I have seen, I am convinced the role of Canadian Heritage will soon become extremely important regarding foreign interference. All signs indicate that foreign states that try to interfere in our elections or other democratic institutions will increasingly do so through disinformation on social media. Enabling the public to understand and detect disinformation is already important but, given the rapid pace at which technology evolves, in my view, these efforts must intensify.

The Plan in operation: 2019

The Canada Declaration of Electoral Integrity Online 2019

In advance of the 2019 general election, four major US social media companies – Microsoft, Twitter, Facebook and Google – signed the Declaration. With this, the government intended to signal that it expected social media platforms to do their part to ensure the integrity of the 2019 election by enforcing their own standards and policies.

The SITE TF and the Panel of Five

The SITE TF's work began well before the 2019 election. In November 2018, the SITE TF created the "Tech Table" (a group of subject-matter experts from CSE, GAC and CSIS) to coordinate efforts to combat foreign interference online. The SITE TF also began to develop a range of analytic products to help define threats to the election and clarify internal and external engagement processes. These included baseline threat assessments of hostile state capabilities and intentions, scenarios and analyses of potential responses and documents prepared at the Secret and unclassified levels intended for broader audiences.

The Panel of Five began meeting just prior to the election period. It received regular baseline briefings from the SITE TF. It reviewed the terms of its mandate and met with election officials to better understand their roles. The Panel attempted to get a better understanding of the CEIPP threshold by working through scenarios designed to explore issues such as when it would be appropriate to act, how an announcement would proceed and who would make it. Once the election period began, the Panel met weekly and was always on call.

Panel members also received information through their departments and were on CSIS's distribution list for relevant intelligence products. During its weekly meetings, the Panel was briefed by the SITE TF. The Panel also received daily Situation Reports ("**SITREPs**") from the SITE TF between meetings. The SITREPs were based on information provided by SITE TF members. The Panel could ask the SITE TF or others for more information if needed.

All the SITE TF members took a broad view of what information they should share with one another. GAC's Rapid Response Mechanism ("**RRM**") Canada provided real-time reporting of its monitoring of the domestic online environment for misinformation and disinformation. CSE forwarded reports considered sufficiently important about the capabilities of states of interest. CSIS provided products potentially relevant to foreign interference or democratic institutions, as well as information about the motivations and capabilities of threat actors. The RCMP, given its mandate, had less information to share, but passed on anything it thought might be significant.

While the SITE TF's primary audience was the Panel of Five, it also shared information with a range of external partners, including through the Electoral Security Coordinating Committees, which are groups of officials with responsibilities related to election integrity. The SITE TF also provided Secret level briefings to security-cleared political party representatives. The briefings included open source materials as well as some classified information about foreign interference tactics in use.

As I discuss in Volume 2, Chapter 7, in 2019, the Panel concluded that the threshold for an announcement had not been met. The Panel found some foreign interference had occurred, but nothing that had threatened Canada's ability to have a free and fair election.

The 2019 SITE TF After Action Report

Following the election, the SITE TF produced a classified After Action Report ("**AAR**"). SITE TF AARs are not intended to be evaluation or assessment products. According to one CSIS representative, an AAR is best thought of as a tactical report on what the SITE TF did or did not observe. The 2019 AAR identified successes, challenges and areas for improvement.

The 2019 AAR reported that the SITE TF saw foreign interference activities targeting certain ridings and candidates. It said those activities were not part of a broad-based electoral interference campaign and did not impact the overall outcome of the election. GAC's representative on the SITE TF in 2019 explained that the conclusion on impact was the Panel of Five's conclusion; the SITE TF merely reported it. It is not the SITE TF's role to assess the impact of what it observed.

The Judd report and amendments to the CEIPP

The CEIPP requires an independent review after an election to assess the implementation and effectiveness of the CEIPP. The review for 2019 was done by former CSIS Director James Judd ("**Judd Report**"). Mr. Judd found the CEIPP was successfully implemented and recommended its use for the next general election.

He made a number of recommendations for improvements to the CEIPP and other government responses to foreign interference. As a result, Cabinet issued an amended Cabinet Directive in May 2021. Changes included:

- The CEIPP was made applicable to all future elections.
- The Panel of Five's mandate was expanded to consider domestic as well as foreign threats.
- The CEIPP was extended to the full caretaker period, which may be longer than the election period in some circumstances.
- The Panel was expressly given authority to communicate information to other entities.

Political parties were expressly allowed to give information to the Panel.

The government did not accept the Judd Report's recommendation to extend the CEIPP to cover the pre-election period, which is the period before an election campaign begins. This was because during the pre-election period, ministers have the powers and responsibilities to respond to foreign interference. The CEIPP is, in part, a reflection of the caretaker convention which holds that, starting from the election period until a new government is formed, the Government (particularly ministers) should only conduct business that is routine, non-controversial or urgent, and in the public interest.

The Plan in operation: 2021

The Canada Declaration on Election Integrity Online 2021

The Declaration was updated in 2021 in anticipation of the general election, and more platforms signed on. In addition to the original four members (Facebook/Meta, Google, Microsoft and Twitter), TikTok, LinkedIn and YouTube also signed.

The SITE TF and the Panel of Five

In 2021, the SITE TF operated in a similar manner to 2019. SITE TF meeting and reporting frequency remained the same, and it produced largely the same types of documents. However, as a lesson learned from the 2019 election, it acknowledged the importance of sharing information at the lowest classification level possible.

The SITE TF also began to produce "threat summaries" in late 2020 to allow all government partners to understand the overall threat landscape. Initial summaries in late 2020 and January 2021 were followed by monthly reports from May to August 2021. The monthly reports began when the Panel of Five became active, so they had a more cohesive view of what the SITE TF was seeing.

One key difference in 2021 impacting the SITE TF's operations was the COVID-19 pandemic. The SITE TF had to operate in a mixed classification environment because members could not always meet in a classified space. This meant that at times, they could only discuss topics at a very high level. The pandemic also meant the SITE TF chair had fewer resources to help with the administrative and secretariat functions of the SITE TF.

However, the SITE TF had more capabilities than in 2019. CSE had more resources, and RRM Canada had greater experience and linguistic capacity. Because the SITE TF's mandate broadened to include domestic threats, including threats to election security, the RCMP played a greater role than it had previously.

The Panel of Five met before, during and after the election period. Starting in January 2021, it focused on understanding relevant threats, discussed lessons learned from 2019 and worked through hypothetical scenarios.

Once the election was announced, the SITE TF sent the Panel daily SITREPs. However, because of the pandemic, Panel members could only read them when they went into their offices. The SITE TF also provided weekly briefings, after which the Panel deliberated in private.

The SITE TF continued to provide briefings to political party representatives.

As in 2019, the 2021 Panel of Five concluded the threshold for an announcement was not met.

The 2021 SITE TF After Action Report

The SITE TF produced a classified After Action Report (AAR) following the 2021 general election. It said that the PRC had sought to interfere in the election by supporting individuals viewed as pro-PRC or neutral, and India might have engaged in interference intended to influence electoral outcomes. Other states like Russia, Iran and Pakistan were not observed as having attempted to interfere.

The 2021 AAR made a number of recommendations, including that government:

- Review its communications plan to be more strategic about communications about election security.
- Continue funding RRM Canada and continue contracting with external partners to supplement RRM Canada's monitoring.
- Ensure funding for independent monitoring by academic and civil society groups.
- Review how the security and intelligence community might better engage with political parties outside of the election cycle.

Evolution of the Plan after 2021

The Rosenberg Report

The review of the 2021 CEIPP was conducted by former Deputy Minister Morris Rosenberg. The report ("**Rosenberg Report**") was released in 2023. As with the Judd Report, the Rosenberg Report concluded that several elements worked well and should be maintained, but also recommended certain improvements.

Several of Mr. Rosenberg's recommendations related to better communication with the Canadian public about the risk of foreign interference and measures the government takes to protect the integrity of elections. Other recommendations were about ensuring better functioning of the Panel of Five. This included better preparation, continuity of membership and having earlier briefings with input from more sources.

Mr. Rosenberg also recommended further study on several issues, including the role of different members of the SITE TF and whether the Panel of Five should be able to make announcements in circumstances where foreign interference exists, but it falls below the threshold set out in the CEIPP.

Increased briefings for Panel members

In 2023, in response to the Rosenberg Report, the government committed to briefing new Panel members within three months of appointment and to holding regular Panel meetings starting in the spring of 2023. Since then, new Panel members have received individual briefings, and, since January 2024, the SITE TF has briefed the Panel about every six weeks. Members of the SITE TF and the Panel of Five told me how much they valued these regular briefings.

Using the SITE TF for by-elections and the role of the Deputy Minister Committee on Intelligence Response

Although the SITE TF effectively operated year-round, its focus until 2023 was on general elections. It did not have responsibility for by-elections.

On 16 May 2023, the government announced that, in light of the significant amount of public discussion about foreign interference at the time, and the importance of ensuring public confidence in elections, the SITE TF would provide enhanced monitoring for the four by-elections to be held in June 2023. This was a significant change in approach and came as a surprise to the SITE TF. The SITE TF has been stood up for every federal by-election since.

There are differences between how the SITE TF operates during by-elections compared to general elections.

The most significant is its reporting relationship. Because the CEIPP does not apply during by-elections (since the caretaker convention is not in effect and ministers retain their responsibilities and accountabilities), the Panel of Five has no authority. Instead, the SITE TF reported to the Deputy Minister Committee on Intelligence Response ("**DMCIR**", see Volume 3, **Chapter 11**), and deputy ministers would go to their minister if they felt action needed to be taken. DMCIR's membership was similar to the Panel of Five, but not identical. The Deputy Minister of Justice and Deputy Attorney General did not sit on DMCIR, and there were senior officials on DMCIR who were not members of the Panel.

DMCIR also had a different role than the Panel of Five. While the Panel is a decision-making body, DMCIR was a committee of public servants accountable to their respective ministers. If information respecting an election incident was reported to DMCIR that required public communication, the information would go from DMCIR to the responsible minister.

Prior to each by-election, the SITE TF now produces a baseline threat assessment that considers whether or not there is intelligence that a foreign state intends to interfere with the by-election. It also considers the demographics of the riding and the specific candidates running.

The SITE TF's reporting during by-elections is less frequent than during a general election. If it has no new information to report, it only issues weekly SITREPs. Ministers' offices used to be on the distribution list for SITREPs. However, in June 2023, DMCIR decided to remove them. The CSIS representative on the SITE TF explained that if DMCIR became aware of something it felt needed to go to a minister, DMCIR would notify that minister. He further explained that regular reporting continued to flow, so if information needed to go to a discussion, it could be disseminated through the normal reporting chains.

Following the 2023 media reporting, the Privy Council Office ("**PCO**") requested that the SITE TF track readership of its SITREPs. This proved challenging. Therefore, in 2024, the SITE TF moved to use CSE's centralized database system, which allows distribution to be tracked (see Volume 4, Chapter 14). All SITE TF related products are now distributed this way.

I heard evidence from SITE TF members that having the SITE TF in place for by-elections brings both opportunities and costs. The most significant cost was to RRM Canada. During the 2023 and 2024 by-elections, half of the RRM Canada analysts spent two thirds of their time on SITE TF work. This meant RRM Canada had to stop, reduce or postpone work in other areas. For example, for the June 2023 by-elections, RRM Canada paused its monitoring on the PRC Overseas Police Stations (see Volume 4, Chapter 17). There is also an operational burden on the RCMP's Ideologically Motivated Criminal Intelligence team. About half of their time was directed to the by-elections.

There was a lesser impact on CSE and CSIS since collection and dissemination of intelligence on foreign interference is part of their regular mandates. However, these agencies had some additional administrative burdens, particularly for the SITE TF's chair.

Adopting an enhanced monitoring role for by-elections also resulted in opportunity costs for the SITE TF itself, as it had to pause work on tabletop exercises and reviewing recommendations for improvement.

Still, SITE TF members told me that monitoring by-elections helped them avoid the "cold start" problem that happens if the SITE TF is only used every few years. More frequent periods of enhanced monitoring helped reinforce effective operations, encouraged discussions and assisted in planning operations for the next general election. It also built group cohesion and coordination.

Unclassified SITE TF After Action Reports

Starting with the 2023 by-elections, the SITE TF began producing unclassified AARs. The SITE TF has issued public AARs for all the by-elections occurring since June 2023. In each case, it reported that it had not observed any indication of foreign interference.

Members of the SITE TF said that producing unclassified reports is challenging. If they identify intelligence about threat activities, it can be difficult to determine what can be said in a public AAR. Even reporting that no incidents of foreign interference were observed could reveal intelligence gaps to hostile state actors. However, SITE TF witnesses agreed that releasing information to the public was a way to build Canadian resilience to electoral foreign interference. I agree with this view entirely.

The Digital Citizen Initiative and the Digital Citizen Contribution Program

The Digital Citizen Initiative (DCI) is a component of the Plan that is not directly tied to the electoral cycle, but rather continues year-round. It falls under the "building citizen resilience" pillar of the Plan. The goal is to support democracy and social inclusion in Canada by building citizen resilience against online disinformation and supporting a healthy information ecosystem.

When the government announced the Plan in 2019, it also announced $7 million for phase one of the DCI. Because of the urgency to have measures in place for the 2019 election, funding was provided through pre-existing programs administered by Canadian Heritage. This resulted in over 20 contribution agreements with civil society, academia and the private sector.

Canadian Heritage subsequently established the Digital Citizen Contribution Program ("**DCCP**") to administer funding for applied research and citizen focused activities.

Each year, the DCCP issues a call for proposals with priorities developed by Canadian Heritage officials in consultation with other departments and external partners. The DCCP's 2023-2024 call for proposals included seven priorities, one of which was for projects that would develop and publish tools to build resilience to foreign state misinformation and disinformation targeting Canadians, including diaspora members.

Since 2022, the DCCP also funds the Canadian Digital Media Research Network ("**CDMRN**"),[13] a network of academic and civil society groups that monitor and analyze the information ecosystem in Canada. The CDMRN produces baseline assessments of the information ecosystem and uses an incident response protocol to respond to major information incidents, including those related to elections. I discuss the CDMRN in Volume 3, **Chapter 13**.

Representatives of the CDMRN attended a 25 March 2024 Panel of Five retreat to discuss the Canadian information ecosystem and the CDMRN's incident alert protocol. A discussion followed about how the CDMRN might support and complement the Panel's work. This was the first time since the creation of the CEIPP that people external to the government were invited to brief the Panel.

The CDMRN is expected to play a significant role in monitoring the online ecosystem during the next federal general election.

The Protecting Democracy Unit

In 2022, the government established the Protecting Democracy Unit ("**PDU**") within PCO's Democratic Institutions Secretariat ("**PCO-DI**"). The PDU's mandate is to coordinate, develop and implement government-wide measures to protect Canada's democratic institutions.

Examples of the PDU's work include counter misinformation and disinformation toolkits for parliamentarians, public servants and community leaders and training for the public on disinformation.

Looking to the future

The Plan has been the subject of several reviews, reports and assessments since it was first put in place.

First came the reviews by Mr. Judd and Mr. Rosenberg discussed above. Then in 2023, the government commissioned a report – the LeBlanc-Charette Report – to explain what it was doing to counter foreign interference and to discuss recommendations about the Plan that were still under consideration.[14]

---

[13] The DCCP provided the CDMRN with $5.5 million in funding over 3 years.

[14] The LeBlanc-Charette Report was commissioned in response to the 2022–2023 media leaks and increased concerns within Parliament and among the public about foreign interference.

In 2024, three more reports relevant to the Plan were released: the 2024 reports by the National Security and Intelligence Committee of Parliamentarians ("**NSICOP**"), the National Security and Intelligence Review Agency and this Commission's Initial Report. I heard evidence that all these reports are being considered in the government's work to develop a third version of the Plan. Policy options are being regularly discussed at both the civil service and ministerial levels.

Below, I discuss some of the questions raised about the Plan that may impact the development of its next version.

Membership of the Panel of Five

One topic that received considerable attention during the Commission's hearings was the composition of the Panel of Five.

Some participants suggested that deputy ministers lack sufficient independence from Cabinet to fulfill their obligations under the CEIPP, or that they may lack enough understanding of electoral politics to correctly assess the impact of particular events. Judges, respected eminent persons and the Chief Electoral Officer have been suggested as Panel members, either in addition to, or as a replacement for, existing members.

The question of Panel membership received significant attention within the government when the CEIPP was first established. PCO-DI has considered different possible compositions but believes that the current members form a unique and effective group. They have access to intelligence and know how it can be used, which informs their understanding of the threat landscape. The members of the Panel also retain their own authorities and can essentially act as an operational coordinating body whose purpose is to respond to potential foreign interference incidents.

The Chief Electoral Officer is not a member of the Panel. Stéphane Perrault, who currently occupies that role, told me that this maintains the independence of Elections Canada and reflects its own accountabilities, which differ from those of the government.

Panel public communication

Panel members identified greater public awareness of the Panel as important for building confidence in public institutions. Knowing that there is a governance structure in place to address foreign interference during elections could reassure the public. In addition, greater knowledge of the Panel would better equip the public to understand the meaning of a Panel announcement if one were ever required during an election. The Panel is now examining various ways to explain its role to the public and adopt a more proactive communication approach with respect to their work before, during and after an election.

However, the Panel also told me there are risks with public communication. For example, an attempt by the Panel to address concerns about disinformation could be seen as a sign of bias. PCO witnesses believe it is critical that officials do not engage in debates around the truthfulness or authenticity of information that is flowing during an electoral process if the public service is to maintain its non-partisan role.

To achieve the benefit of public communication while avoiding the risks, the Panel is considering a range of options, including holding a technical briefing with the media, organizing a more formal press event, enabling media representatives to observe the Panel doing a tabletop exercise or a combination of these approaches.

Another CEIPP threshold

I heard that the government is reviewing whether the CEIPP should be changed to allow for the possibility of Government of Canada announcements, even if the current threshold is not reached. While the government does not want to interfere with legitimate democratic discourse, there may be times when Canadians have an interest in knowing if there is foreign interference in a general election even if it does not meet the high threshold provided for by the CEIPP. Presumably, this would require the government to come up with criteria that must be met to justify public announcements meeting a lower threshold. Questions that still need to be considered include who should make a sub-threshold announcement (for example, the SITE TF), and how it would be delivered (for example, a technical briefing to journalists).

PCO witnesses emphasized that there is an important distinction between a Panel announcement under the CEIPP and general communications by the government. They said the intention is that during election periods, the Panel will continue to maintain the same high threshold for a public announcement.

Making the SITE TF permanent

The original idea was for the SITE TF to operate only during general elections. But this did not account for the fact that foreign interference threats also exist outside of election periods. The reality is that the SITE TF operates continually, although this is not reflected in its Terms of Reference.

For instance, the SITE TF receives intelligence reporting on foreign interference in non-federal elections or in political party processes like nomination and leadership contests even though this is not in its Terms of Reference. This allows the SITE TF to better assess and understand possible threats to federal elections. It is useful to have a baseline of the threat environment outside election periods.

Some SITE TF witnesses said that a permanent SITE TF could do more robust national threat assessments, would be better positioned to share information

with stakeholders and the general public or could benefit from greater engagement with international partners. However, they acknowledged, and other witnesses agreed, that making the SITE TF permanent, with enhanced capabilities, would require additional resources to carry out a mandate that, in some respects, overlaps with the mandate of security agencies. Daniel Rogers, then the Deputy NSIA and now CSIS Director, told me that the government was mindful of using its resources to counter foreign interference as efficiently as possible.

John Hannaford, the current Clerk of the Privy Council (Clerk) and chair of the Panel of Five, said it has been useful for senior public servants to have advice from the SITE TF during by-elections. In his view, whether the SITE TF needs to be permanent will depend on the demands that are being placed by the elections schedule.

David Vigneault, former CSIS Director, said it was important to have a broader approach to foreign interference, rather than having different groups looking at it only in certain circumstances like an election. However, he was not sure that the SITE TF was the appropriate process for tackling broader foreign interference issues including misinformation and disinformation or threats to diaspora communities.

Also, because the SITE TF was not originally meant to be a permanent body, witnesses said there are some challenges with having a permanent SITE TF. These include the current structure of a rotating chair and membership turnover, which make developing institutional memory difficult. Turnover may also make building and maintaining trust with external partners like political parties harder.

The government is considering making the SITE TF permanent by establishing a consistent chair and permanent administrative secretariat. I was told that it is likely that no final decision will be made before the release of this report.

Where to locate a permanent SITE TF

If the SITE TF were to have a permanent secretariat, one question would be where to house it within the government. The government is still considering this. One option is at the Privy Council Office (PCO). Another is at Public Safety Canada with the National Counter Foreign Interference Coordinator.

Several government officials noted that having a permanent SITE TF within PCO has pros and cons. For example, having the SITE TF within PCO could give it a certain degree of leverage. However, there are questions of duplication of function and efficiency. Moreover, Mr. Rogers noted that PCO is not an operational department, and the SITE TF is an operational entity. In addition, proximity to the political level may not be ideal. Then again, proximity to the heart of the government could be beneficial for SITE TF's governance and coordination.

Nathalie Drouin, current National Security and Intelligence Advisor to the Prime Minister (NSIA), and Mr. Rogers were largely agnostic about where the SITE TF should be housed. Mr. Rogers said the more important question is whether it can integrate effectively into other decision-making bodies.

At the time of this report, discussions were ongoing about whether the SITE TF should become permanent, and if so, how to structure it and what it would do. In light of the different points of view I heard, I note that particular attention should be devoted to whether the SITE TF should monitor every by-election or only monitor those identified as likely to be of interest to foreign interference actors. Monitoring a by-election requires significant resources. Based on what I have learned throughout the Commission's work, I do not think that there are risks of foreign interference in all ridings.

Monitoring Canada's domestic online environment for disinformation

At present, no federal entity has a specific mandate to monitor Canada's domestic online environment for disinformation outside of elections.

Many witnesses, including officials from Public Safety, the NSIA, the Clerk and the Deputy Minister of Foreign Affairs said there is a need for government capacity to monitor the domestic online environment and to be able to act on what it learns. Witnesses also noted that the way in which the government uses this information needs to be carefully considered in light of the relevant legal obligations and risks.

The question of monitoring the domestic information environment overlaps to some extent with the question of the government's relationship with civil society organizations such as the Canadian Digital Media Research Network (CDMRN). The Clerk, Mr. Hannaford, said the government was reflecting on how the Panel and the CDMRN would interact during an election period. Ms. Drouin said there is a convergence of interests and the CDMRN can add value by shedding light on an issue while remaining independent of the government.

Who would monitor Canada's domestic online environment for disinformation

If the government were to monitor the domestic online environment for disinformation during elections or year-round, the question is which government entity would do it.

The Rapid Response Mechanism ("**RRM**") Canada is part of the SITE TF because of its online monitoring capability and expertise. During the 2019 and 2021 elections, RRM Canada monitored the domestic online environment for election-related misinformation and disinformation. It supported the SITE TF with open source research and analytics, as well as with information from G7

partners about evolving foreign interference tactics. As explained above, it did the same for by-elections as of June 2023.

While RRM Canada's expertise is viewed as highly useful for the SITE TF, this was not the function it was originally intended to perform. As I discuss in Volume 3, **Chapter 11**, RRM Canada was created as part of a Canadian-led initiative within the G7 to address threats to democracy. Its focus is predominantly international, which is why it is part of GAC.

Several witnesses queried why GAC, which after all is the "foreign" ministry, should lead monitoring of the domestic online information environment. And as I noted earlier in this chapter, RRM Canada's work during election periods comes at the cost of reducing its ability to focus on its usual mandate. Concerns have been raised with senior levels of government that its role on the SITE TF is not consistent with its mandate.

GAC witnesses noted that even if responsibility for monitoring the domestic online information environment for disinformation were moved from RRM Canada, RRM Canada could remain part of the SITE TF. This would allow the SITE TF to know what RRM Canada and its G7 partners are seeing internationally, without directing its resources away from monitoring the international online information environment.

I understand there have been ongoing conversations about building capacity for domestic monitoring within another department like Public Safety or PCO, but this remains an open question.

The Deputy Minister of Public Safety, Shawn Tupper (now retired), suggested that one possibility might be to expand the scope of Public Safety's Government Operations Centre, a branch within the Department that provides whole-of-government coordination in relation to emergency management. The Government Operations Centre assists in responding to national security events, including by bringing in other departments and expertise. It is informed by close connections with provincial, territorial and municipal emergency response sectors.

Better public communication from the government

One of the main lessons from the SITE TF's 2021 After Action Report (AAR) was that communication is a critical tool in responding to foreign interference. The SITE TF noted that communications were a challenge in the lead up to, and during, the 2021 election. For example, because the government did not proactively communicate its efforts to safeguard the election, this resulted in criticism of its perceived lack of action.

The SITE TF recommended that the government review its communications plan. PCO's Deputy Secretary to the Cabinet (Governance), acknowledged the value of increased communications with Canadians in order to "normalize communications" in the elections space and increase trust in federal electoral processes.

Engagement with political parties

Effective engagement with political parties on foreign interference is a challenging issue, which I discuss in more detail in Volume 4, Chapter 15. In this section, I address the specific relationship between the SITE TF and political parties.

With the assistance of PCO's Democratic Institutions Secretariat, the SITE TF has offered unclassified briefings to political party representatives for nearly all by-elections since June 2023. These briefings have not been well attended. Only the New Democratic Party of Canada ("**NDP**") and Bloc Québécois attended the briefings for the June 2023 by-elections. The briefings ahead of the March and June 2024 by-elections were only attended by the NDP.

The Executive Director of the Conservative Party of Canada testified that he was unaware his party was invited to these briefings. Representatives of the Green Party of Canada also said they were unaware of the briefings. Government witnesses testified that, generally speaking, all of the major political parties taking part in a by-election have been invited to a briefing. The National Director of the Liberal Party of Canada said he knew about the briefings but assumed that they would not have anything new because they were unclassified. If there was information his party needed to know, he thought that it would be classified or that the government would make greater efforts to get his attention.

Following the political party briefing in June 2023, PCO concluded there was a lack of concrete examples of foreign interference and the briefing "did not hit the mark." In PCO's view, it did not meet the parties' expectations. The SITE TF then discussed the need to find and incorporate concrete examples of foreign interference into the briefings.

I was told efforts have been made to revise the briefings, including with concrete, open source examples of possible foreign interference in Canada, some even drawn from the Commission's Initial Report. However, with the low level of participation of political parties, it is not yet clear whether this revised content will be helpful.

The SITE TF has also provided classified briefings to security-cleared political party representatives during general elections. Secret level briefings allow a greater degree of information to be shared, though, as I explain in Volume 4, Chapter 15, political parties may be limited in what they can do with what they learn.

Online platforms

Earlier in this chapter I mentioned the Canada Declaration on Election Integrity Online (Declaration). After the 2019 election, then Minister for Democratic Institutions Dominic LeBlanc concluded the Declaration had been effective. It was therefore renewed for the 2021 election. Currently, PCO's Democratic Institutions Secretariat (PCO-DI) is advising the Minister of

Democratic Institutions on whether Canada should renew the Declaration for the next general election, and what changes could be made in terms of updates to the Declaration or new signatories.

In terms of expanding the range of signatories, Assistant Secretary to the Cabinet Allen Sutherland indicated that PCO-DI has approached Tencent, WeChat's parent company, and had a general discussion about their platform and whether they might be interested in becoming a signatory. At present, WeChat is not a signatory to the Declaration.

Because of the rapidly changing environment for social media platforms, PCO-DI is exploring the possibility of Canada engaging with social media companies as part of a group of democracies rather than singly. The Commission heard that social media companies, particularly large ones, are sometimes unwilling to cooperate with relatively small countries who attempt to regulate them.

The Declaration is a voluntary agreement. Another option for dealing with social media platforms would be regulation. The government has considered this option, but also noted such an approach raises issues of censorship and regulation of free speech.

Nevertheless, the government has started regulating some online content and social media. In 2023, the government amended the *Broadcasting Act* to regulate foreign streaming services. The Canadian Radio-television and Telecommunications Commission ("**CRTC**") is using contributions from these services to create a news fund to support independent media.

Also, under the *Online News Act*, if a social media platform meets certain criteria, it must notify the government and negotiate with news companies whose content is posted on the platform. For those who do not want to negotiate with media outlets, the CRTC can issue an exemption in return for a monetary contribution.[15]

The proposed *Online Harms Act* (Bill C-63) would have imposed responsibilities on social media platforms to reduce the risk of harm of seven specific categories of content, which could include some forms of misinformation and disinformation. The government's rationale for proposing Bill C-63 was that content moderation has gone down among platforms, so leaving content moderation to the platforms can cause harm. The proposed legislation would have required platforms to be accountable for mitigating harms covered by the law. Bill C-63 would also have authorized the government to order social media platforms to give researchers access to their data sets and information. With the prorogation of Parliament on 6 January 2025, Bill C-63 died on the order paper.

[15] For example, Google is providing $100 million that the CRTC will use to strengthen Canadian journalist organizations.

12.3 The Countering Hostile Activities by State Actors Strategy

The Plan was not the only set of policy initiatives that Canada has pursued to respond to foreign interference threats. Starting in 2018, the government began parallel efforts to develop a Countering Hostile Activities by State Actors Strategy (HASA Strategy).

Origin of the HASA Strategy

In July 2018, Public Safety was tasked with leading the work on an inter-departmental counter HASA Strategy.[16] The overarching objective was to establish the basis for a whole-of-government and whole-of-society approach to HASA by leveraging the national security and intelligence community and other partners, including private entities and other government jurisdictions. As part of this work, Public Safety noted that a public-facing version of the HASA Strategy could form part of a broader communication approach to raise awareness about this threat among Canadians.

A brief draft HASA Strategy was produced several months later. It outlined five priority sectors based on an assessment of national interest and overall vulnerability to HASA, namely: democratic processes and government institutions; economic prosperity; international affairs and defence; social cohesion; and critical infrastructure.

In its 2019 Annual Report, the National Security and Intelligence Committee of Parliamentarians (NSICOP) recommended the government produce a comprehensive strategy on foreign interference. It characterized the government's reactions to foreign interference as "*ad hoc* and case-specific" and noted members of the national security and intelligence community differed on how to define the problem and on how they understood its gravity and prevalence.

NSICOP found there was a lack of inter-departmental coordination and collaboration on foreign interference, and that Canada's ability to address foreign interference was limited by the absence of a holistic approach to considering relevant risks, appropriate tools and possible implications of responses to state behaviours. NSICOP also noted the absence of a public foreign interference strategy similar to those for terrorism and cyber security.

---

[16] HASA encompasses any effort by a foreign state, or its proxies, to undermine Canada's national interest, and those of Canada's closest allies, with a view to advancing its own self-interest. These attempts may go beyond routine statecraft, challenge the rules-based order or deliberately seeks to remain ambiguous. HASA encompasses actions that are short of armed conflict yet deceptive, coercive, corrupt, covert or illegal in nature.

After the 2019 General Election, Bill Blair, then Minister of Public Safety, asked his department to keep working towards a HASA Strategy.

Rob Stewart, Deputy Minister of Public Safety from December 2019 to October 2022, said advancing a plan like this involves an elaborate, non-linear, process of consultation and approvals internal to the government, which is always somewhat challenging.

Dominic Rochon, the Senior Assistant Deputy Minister of Public Safety's National and Cyber Security Branch from October 2019 to October 2022, added that part of the challenge was that the HASA Strategy encompassed not just foreign interference, but a whole range of activities and areas where hostile states act, such as economic security. The process therefore involved a large number of departments and agencies, each with their own needs and legislative tools requiring refinement.

Thus, I heard how the HASA Strategy was a vast undertaking that became the subject of many discussions, including at the Deputy Minister Committee on National Security (see Volume 3, **Chapter 11**), and many refinements. One particularly difficult question had to do with governance and coordination, including the creation of a counter HASA coordinator. There was general agreement that a coordinator was necessary, but not about where the coordinator should reside – at Public Safety, PCO or elsewhere.

The evidence shows that another challenge in advancing the HASA Strategy was the number of other priorities facing Public Safety at the time. Many issues associated with the COVID-19 pandemic fell to it, and the Department was also dealing with fallout from the mass casualty event in Nova Scotia.

The HASA Memorandum to Cabinet

Marco Mendicino became Minister of Public Safety after the 2021 general election. He said his top priority in relation to foreign interference was to push the HASA Strategy forward through a Memorandum to Cabinet ("**Memorandum**").

In May 2022, Minister Mendicino submitted the HASA Memorandum to Cabinet. It discussed whether the government should take initial steps to modernize Canada's approach to counter HASA by enhancing policy approaches, strengthening coordination, improving legislative tools and developing new capabilities to counter threats.

The HASA Memorandum recommended the endorsement of the priority sectors set out in the HASA Strategy, which I have described above.

Various measures were recommended, including enhancing legislative tools, creating new capabilities and the implementation of a strategic communications approach:

- Endorse the principles, priority sectors and pillars in the HASA Strategy to guide current and future federal actions against HASA.
- Public Safety to implement a whole-of-government strategic communications approach, which would include engagement with domestic stakeholders, including members of diaspora communities vulnerable to HASA.
- Explore enhancements for legislative tools to ensure Canada's ability to detect and counter HASA threats by consulting on potential amendments to a number of statutes.
- The RCMP to develop new capabilities and new activities.
- Public Safety to expand its coordination of government counter-HASA activities to help implement the HASA Strategy.

I note that the HASA Strategy and the HASA Memorandum have a much broader scope than the Commission's mandate. However the aspects of the Memorandum concerning democratic processes and institutions fall within it.

Cabinet ratified the HASA Memorandum in June 2022. This was almost four years after the work to develop a counter HASA Strategy began.

Mr. Stewart said that Cabinet endorsing the HASA Memorandum was essentially a licence to continue the work by consulting with Canadians on the proposed toolkit and legislative amendments.

Developments after ratification of the HASA Memorandum

Mr. Mendicino said once Cabinet ratified the HASA Memorandum in June 2022, Public Safety focused on implementation. He said that he was eager to see it materialize, but this took some time because Public Safety needed a whole-of-government response to help facilitate public engagement and deal with concerns that the HASA Memorandum might be overreaching, run afoul of the *Charter* or discriminate against diaspora communities. Moreover, implementation occurred against the backdrop of the COVID-19 pandemic, the Russian invasion of Ukraine, the "Freedom Convoy", and later, the Public Order Emergency Commission.

In addition, as I explained in Volume 3, **Chapter 11**, debate continued within the government about whether to house the National Counter Foreign Interference Coordinator ("**NCFIC**") at Public Safety or PCO.

In March 2023, the NCFIC position was finally created within Public Safety. Funding followed in the 2023 budget, but before this was available, Public Safety had to reallocate pre-existing resources in order to support the NCFIC's work. This work included coordination, managing relations with allies, and

driving the policy work and consultations that would eventually lead to the *Countering Foreign Interference Act* (Bill C-70), which I discuss below.

In the spring of 2023, Public Safety launched a first round of public consultations on potential legislative amendments. This was limited to testing reactions to a foreign agent registry.

Concerns had been expressed that a registry would stigmatize Chinese Canadians, particularly given the anti-Asian racism resulting from the pandemic. These concerns drove the decision to keep the registry country agnostic, meaning that the registry would not distinguish between different countries when imposing reporting obligations under the legislation. The feedback from consultations was generally supportive of a registry.

A second round of consultation was launched in the fall of 2023 under Minister Dominic LeBlanc's tenure as Minister of Public Safety. These consultations were about the other legislative changes that were ultimately included in Bill C-70.

Both rounds of consultations involved seeking written comments and holding roundtables with stakeholders including academics, advocacy groups, Indigenous governments and members of different communities. Officials received extensive feedback. There was general agreement that foreign interference was a serious issue, and that Canada's tools needed to adapt.

After the consultations, the proposed legislative changes were brought back to Cabinet one more time before the legislation was introduced.

Patrick Travers, Senior Global Affairs Advisor to the Prime Minister, said that the time it took to implement these legislative amendments must be viewed in light of the lessons learned from previous legislative initiatives dealing with national security matters. The previous Government's attempt to reform national security architecture had encountered significant opposition, and after the governing party changed, this architecture was remodeled through the *National Security Act, 2017*. Any legislation touching the core powers of the national security agencies, their oversight and the rights of Canadians was particularly sensitive and needed to be considered very carefully.

The Prime Minister testified that this was the reason there were multiple rounds of consultations with different diaspora communities and stakeholder groups, and why the legislation went back to Cabinet multiple times. He said that it was important to find the right balance. The Prime Minister and his senior staff are of the view that the widespread support for Bill C-70, not only in Parliament but also within civil society, showed that the work in the lead-up to introducing the bill had been successful in building the necessary consensus for it.

The *Countering Foreign Interference Act* (Bill C-70)

Following the two rounds of consultations, Bill C-70 was introduced in the House of Commons on 6 May 2024, and received Royal Assent on 20 June 2024. It became the *Countering Foreign Interference Act*.

This act amended the *Canadian Security Intelligence Service Act* ("***CSIS Act***") with immediate effect, while changes made to the *Criminal Code*, *Canada Evidence Act* and the *Security of Information Act* (now, the *Foreign Interference and Security of Information Act* or "***FISOIA***") came into force on 19 August 2024. It also established a Foreign Influence Transparency Registry, which Public Safety officials estimate will take a year to set up. The major components of the Act are discussed below.

Amendments to the *CSIS Act*

The *CSIS Act* was amended in several significant ways.

Expanded foreign intelligence mandate

CSIS can assist the Minister of Foreign Affairs or the Minister of Defence in the collection of information or intelligence relating to the capabilities, intentions or activities of foreign states or non-Canadians within Canada. This collection must occur "within Canada." The geographical limitation caused operational difficulties for CSIS based on a series of Federal Court decisions that interpreted the limitation to mean CSIS could not collect information located outside Canada, for instance information hosted on servers outside the country. The *CSIS Act* was therefore amended to distinguish between the location of the collection activity, within Canada, and the location of the information being collected, which could be outside Canada. With the amendment, CSIS can now collect, within Canada, foreign intelligence located outside of Canada or directed at a person or thing that was in Canada but is temporarily outside of Canada.

Information sharing

CSIS had limited authority to disclose some types of information to entities outside of the federal government. With the amendments, CSIS can now disclose information to any person or entity outside the federal government to build resiliency against threats to Canada's security. This allows it to disclose information that it considers important in helping to counter threats such as foreign interference. Before CSIS can share such information, it must first have given it to a federal department or agency that performs duties and functions relevant to the information. The information cannot include personal information about Canadian citizens, permanent residents or persons in Canada (other than the recipient of the information) or the name of Canadian entities such as the name of a Canadian corporation (unless the corporation is the recipient).

New search and seizure powers

The *CSIS Act* had a one-size fits-all warrant provision, which was modelled after the laws about wiretaps. CSIS now has a number of new tools it may use with permission from the Federal Court. These include an order requiring a person or entity to preserve things in their possession or control, an order requiring a person or entity to produce to CSIS things in their possession or control and a single-use warrant authorizing CSIS, on a one-time basis, to take certain steps to obtain information, records, documents or other things.

Witnesses also said there was a need to modernize the *CSIS Act* because of significant societal and technological changes since it was enacted in 1984. The amended data set provisions, many of the new warrant authorities and the expanded scope of foreign intelligence investigations all relate to the modern digital environment.

Also important was the reality that threat actors are engaged in a much wider range of activities and target a much wider range of Canadian institutions. The expanded authorities for CSIS to disclose information were particularly significant because the federal government is not the only target for hostile foreign actors. Provinces and territories, Indigenous governments and municipalities, research institutions and the private sector are all targets as well.

The *CSIS Act* as enacted in 1984 did not anticipate this, and restricted CSIS's authority to disclose information outside the federal government. Provisions allowing CSIS to take measures to reduce threats to the security of Canada introduced in 2015 – which I discuss in Volume 3, **Chapter 11** – have been relied upon by CSIS in order to share sensitive information. The 2024 amendments give CSIS a more direct and widely applicable authority to do so.

Amendments to the *Foreign Interference and Security of Information Act* (FISOIA)

The *Countering Foreign Interference Act* amended the *Security of Information Act*, now renamed the *FISOIA*, by amending existing offences or creating new ones:

- **Foreign-influenced intimidation.** Criminalized foreign-influenced intimidation. Threats or violence were already offences.
- **Commission of an indictable offence for a foreign entity.** A new offence of committing an indictable offence (for example, theft or fraud) at the direction of, for the benefit of, or in association with a foreign entity.
- **Deceptive or surreptitious conduct for a foreign entity.** A new general foreign interference offence where a person knowingly engages in surreptitious or deceptive conduct or omits, surreptitiously or with the intent to deceive, to do anything at the direction of, for the benefit of, or in association with a foreign entity. This offence applies if

the person's conduct is for a purpose prejudicial to the safety or interests of the Canadian government, or if the person is reckless as to whether their conduct is likely to harm Canadian interests.

- **Political interference for a foreign entity.** A new offence of engaging in surreptitious or deceptive conduct at the direction of, or in association with, a foreign entity, with the intent to influence a Canadian political or governmental process or to influence the exercise of a democratic right in Canada.

The new political interference offence is particularly relevant to foreign interference in democratic institutions, including electoral processes. It applies to government and political processes at all levels of the government, both during and between elections. It applies to political party processes, including not only nomination and leadership contests, but also processes like the development of party platforms.

The offences are all punishable by a maximum penalty of life in prison. Maximum penalties for preparatory acts to *FISOIA* offences were increased from two to five years.

Amendments to the *Criminal Code*

Bill C-70 changed the *Criminal Code* sabotage offence by refocusing it on acts with the intent to endanger the security of Canada. It also created a new sabotage offence designed to protect Canada's critical infrastructure as well as the health and safety of the public. The making, selling or possession of devices intended to be used to carry out sabotage are now prohibited.

The *Foreign Influence Transparency and Accountability Act* (*FITAA*)

The *Foreign Influence Transparency and Accountability Act* ("***FITAA***") creates a Foreign Influence Transparency Registry, which is a new regulatory regime designed to promote transparency in activities done for foreign principals. Inspired in part by regimes in other countries, *FITAA* establishes a novel and somewhat complex scheme in Canada. As I noted above, the legislation is not currently in force, and important aspects of it will be set out in regulations that have not yet been drafted. I therefore will only provide a high-level summary of the core aspects of the legislation.

FITAA requires persons or entities who enter into arrangements with a foreign principal to undertake or carry out certain activities in relation to political or governmental processes in Canada to register. This includes situations where a person agrees to communicate with a public office holder, distribute money or disseminate information, including on social media at the direction or in association with a foreign principal. Foreign principals include foreign states or entities that they control.

In aid of this scheme, *FITAA* creates the position of Foreign Influence Transparency Commissioner, whose role includes maintaining a public registry with information about foreign arrangements. The Commissioner will be appointed for up to seven years by the Governor in Council (Cabinet and the Governor General) following consultations with recognized groups in the Senate and opposition parties. They have powers of investigation to enforce the registration requirement. Violations of the requirements of *FITAA* can result in prosecution or the imposition of administrative monetary penalties.

New rules for the disclosure and consideration of sensitive information in Federal Court proceedings

The *Countering Foreign Interference Act* creates new rules in the *Canada Evidence Act* about how sensitive information is handled in a range of legal proceedings in Federal Court. The "secure administrative review proceedings" regime allows for Federal Court judges to consider sensitive information in a judicial review proceeding without the person challenging the government action being permitted to see it. Instead, a security-cleared lawyer may be appointed to represent the interests of the individual, and to access the sensitive information in question. These rules replace many individual regimes that existed under different statutes and will apply to judicial review of decisions made by the Foreign Influence and Transparency Commissioner.

Further developments

As discussed above, some significant elements of the HASA Memorandum were advanced with the introduction of Bill C-70. Bill C-70 included all the amendments to the *CSIS Act*, *FISOIA* and the *Criminal Code* that were part of the public consultation process, as well as the creation of a general secure administrative review proceedings process under the *Canada Evidence Act*. Two of the six elements relating to the intelligence-to-evidence problem (see Volume, 2, Chapter 5) that were part of the consultations were included, namely limiting appeals of certain disclosure decisions until after trial and permitting certain sealing orders to be made for national security reasons.

The government recognizes that to fully modernize Canada's foreign interference toolkit, further legislative changes are necessary and is considering what additional tools are needed.

A public HASA Strategy

As mentioned above, the government intended the HASA Strategy to have a public-facing element. As Tricia Geddes, the current Deputy Minister of Public Safety[17] explained, the goal was to convey to Canadians a broad appreciation of the threat and the ways in which the government was addressing it. A public strategy was not finalized prior to the HASA Memorandum.

In November 2022, the first foreign interference media leaks occurred. In response, then-Minister of Public Safety Mendicino asked the Prime Minister's Office to help him move the HASA Memorandum forward and resolve ongoing debates about communication of a public strategy.

On 14 June 2023, then Deputy Minister of Public Safety Shawn Tupper sent a memorandum to Minister Mendicino entitled "Canada's Counter-Foreign Interference Strategy." The memorandum explained that the HASA Strategy would be renamed, moving away from "HASA" in favour of "foreign interference." This was to make clear to the public that the HASA Strategy was aimed at foreign interference, as that was more consistent with the language the media was then using. In essence, the change of name was a "rebranding" of the HASA Strategy.

Minister Mendicino did not approve the Counter-Foreign Interference Strategy before Minister LeBlanc replaced him in July 2023. Public Safety then sought Minister LeBlanc's approval to release a public-facing version of the Strategy. A memorandum to Minister LeBlanc seeking this approval described work on a classified version of the Counter-Foreign Interference Strategy as ongoing.

Minister LeBlanc said that the rapidly changing political discourse around foreign interference in Canada led to the Counter-Foreign Interference Strategy being put on hold. He, as well as other witnesses, also said that the media leaks had made it challenging to find the most effective ways to communicate to the public about foreign interference. With the appointment of the Independent Special Rapporteur on Foreign Interference and, later, my own appointment to lead a public inquiry, the government decided to wait for my recommendations before finalizing a strategy. Ms. Geddes observed that most elements of the Counter-Foreign Interference Strategy were ultimately communicated to the public through the consultations leading up to Bill C-70.

As outlined above, the HASA Memorandum is one of two key policy responses to foreign interference, the other being the Plan to Protect Canada's Democracy (Plan). The HASA Memorandum proposed two strategies: a whole-of-government HASA Strategy and a strategic communication and engagement strategy. The government also intended the HASA Strategy to have a public-facing element. It is six years since the government began developing these strategies and over two years since the HASA Memorandum was ratified. To date, there is no document,

[17] During the Commission's proceedings Tricia Geddes was Associate Deputy Minister of Public Safety. She became Deputy Minister on 31 October 2024.

whether public facing or internal, that comprehensively sets out the government's counter-foreign interference strategy.

Witnesses still considered that an internal and public-facing strategy would be valuable and told me that work is ongoing on these. Ms. Geddes identified the current work of the National Counter Foreign Interference Coordinator (NCFIC) as a key aspect of this effort.

Given that the Commission's mandate is limited to foreign interference in democratic processes and institutions, my investigation did not focus on other sectors envisaged by the HASA Memorandum, such as critical infrastructure or economic prosperity and research security. Thus, I am not necessarily aware of initiatives that the government may have implemented that are directed at those sectors.

That said, it strikes me that the fate of the HASA Strategy is a good illustration of an issue I have observed on more than one occasion during the Commission's work: the government often spends a great deal of time and energy consulting, coordinating and discussing proposed measures with stakeholders (of which there are often many) but this process does not lead to concrete action and ultimately the implementation of the measures envisaged. Instead, measures are sometimes implemented suddenly, in response to an event that highlights their absence, or are simply not implemented at all.

It is difficult to pinpoint the reasons for this phenomenon.

I recognize that the federal government apparatus is large and complex, and we cannot expect it to be very nimble. This being said, it would probably be advantageous and more efficient to break down broad initiatives into more targeted and manageable pieces that do not involve as many stakeholders and, consequently, as many processes and consultations. As the saying goes, "don't bite off more than you can chew." These initiatives should obviously be consistent with each other, but ensuring this consistency is the responsibility of a central authority.

It seems to me that this phenomenon can also be partially explained by the existence of ill-defined lines of accountability, particularly when the initiative or measure envisaged requires the participation of several departments, agencies or other stakeholders. Indeed, the roles and responsibilities of departments, agencies and the National Security and Intelligence Advisor to the Prime Minister (NSIA) in relation to foreign interference were at times unclear to me. PCO, Public Safety and the NSIA sometimes have overlapping and confusing responsibilities. This confusion, in my view, can probably explain the hesitancy I observed when it comes to making decisions. I believe this requires reflection.

12.4 A new National Security Strategy

On 25 November 2024, the Prime Minister issued a mandate letter to the NSIA that, among other things, tasks her with working through the National Security Council to deliver a renewed National Security Strategy in 2025. This strategy is to set out the integrated framework for Canada's national security, defence and diplomatic position. While there is no explicit mention of a public version of the National Security Strategy, the mandate letter stresses the need for transparency and public accountability. I note that the last time Canada's National Security Strategy was updated was 20 years ago in 2004 – three years after 9/11.

A new National Security Strategy will evidently be part of Canada's future framework for responding to foreign interference threats. I expect any new National Security Strategy will expressly address how existing counter foreign interference initiatives such as the Plan and any counter foreign interference strategy will work with this new vision for Canada's national security.

CHAPTER 13

Other Institutions Responding to Foreign Interference

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.*

13.1 Introduction

In Volume 3, **Chapter 11**, I discussed the federal departments and agencies that play a role in protecting Canada against foreign interference. That discussion, however, only captured a portion of the entities that are key to Canada's response.

Consistent with what I heard about the need for a whole-of-society approach to foreign interference, many others contribute to this effort. Some are independent public bodies. Others are democratic institutions themselves. Still others are from the private sector or form part of civil society. Some actively attempt to respond to foreign interference, and others, while not focusing on foreign interference, do work that has important consequences to Canada's ability to detect, deter and counter it.

I discuss many of the key entities from outside of the government in this chapter.

13.2 Elections Canada

Elections Canada is responsible for administering Canada's federal electoral system under the *Canada Elections Act* ("***CEA***"). It is headed by the Chief Electoral Officer ("**CEO**"). As an agent of Parliament, the CEO enjoys independence from the government.

Elections Canada's mandate is twofold: it conducts federal elections, and it administers the rules set out in the *CEA* such as political party registration and political finance rules. It does not enforce the *CEA* (i.e. investigate violations and lay charges), which is the responsibility of the Commissioner of Canada Elections.

Forms of foreign interference that may be within Elections Canada's jurisdiction include threats to physical (e.g. polling stations) and electronic (e.g. the Elections Canada website) electoral infrastructure, disinformation campaigns regarding the electoral process and the illicit funding of candidates, parties or other entities. It also plays a role in providing information about and fostering confidence in the electoral system as a whole, including by engaging with communities who may face barriers to electoral participation.

Administering elections

Elections Canada organizes all federal elections and by-elections. This involves maintaining the National Register of Electors, appointing returning officers, training election workers and giving Canadians voting information.

Once an election is called, Elections Canada must recruit 230,000 to 250,000 people in a matter of days to administer the election. Because of the scale of this workforce and the narrow window of time in which they are hired and work, most of them do not undergo security screening. The CEO told me that this would be impossible. Instead, Elections Canada relies on protections elsewhere in the system to maintain its integrity, including the different ways to vote, ballot secrecy and the presence of third-party observers who ensure Elections Canada staff perform their duties properly.

Elections Canada does not administer political party nomination or leadership contests. It only administers some of the limited political finance rules that apply to these processes.

Political financing

Canadian election law aims to establish a level playing field and prevent the undue influence of money. It does this by setting out political financing rules, which govern how money and other contributions are collected, spent and reported. This includes limits on contributions and expenditures for certain regulated activities like election or partisan advertising or partisan activities. The system regulates parties, electoral district associations,[18] candidates, nomination and leadership contestants and third parties – collectively known as "regulated political entities."

Different rules apply in the election and the pre-election periods. These rules are complicated, but a key feature of them that is relevant to foreign interference is that they exclude the use of foreign money in Canadian elections.

Only Canadian citizens and permanent residents can make contributions (e.g. donate money, goods or services) to regulated political entities. The exception is for contributions to "third parties", which are subject to different rules. I discuss third parties below. Regulated political entities are not required to obtain proof that a donor is eligible, though Elections Canada recommends that they do so. The full names and addresses of any individual contributing over $200 must be given to Elections Canada by regulated political entities and are published on the Elections Canada website.

[18] Also informally called "riding associations" or "constituency associations."

The rules about contributions to third parties are different. The term "third party" refers to entities that do not fall into any of the other categories of regulated entities. Examples of third parties include individuals, unions, corporations and community organizations.

Third parties are not limited to receiving contributions from citizens and permanent residents, but they cannot use funds from foreign sources for regulated activities like election advertising or partisan activities. Foreign third parties are not permitted to spend money on regulated activities at all.

Third parties must register with Elections Canada if they spend at least $500 on regulated activities in the pre-election or election period. Like other regulated entities, they are subject to spending limits.

Third parties must have a separate bank account for all contributions and expenditures for regulated activities. However, I heard from the CEO that it can be challenging to identify foreign funding of third parties for a variety of reasons. This, in my view, may be a foreign interference risk. For example, a third party could receive both foreign and domestic funds outside of an election period, commingle them, and once an election is called, use the money for regulated activities and report it as coming from their own funds. The CEO has already made recommendations to Parliament to amend the *CEA* to address some of these issues. He also made similar recommendations to the Commission.

Regulated entities are required to file a range of different returns with Elections Canada, which reviews them for completeness. It also audits some of them, using a risk-based approach to decide which ones should have extra scrutiny.

Public education

A core element of Elections Canada's mandate is to provide Canadians with information on the electoral process, such as how to vote and mechanisms that ensure electoral integrity. Recognizing that foreign interference can deter members of diaspora communities from voting, Elections Canada has multilingual guides to communicate information about election integrity measures and educational programming targeting diaspora communities.

Elections Canada provides key information on voting on its website in 51 languages. During election campaigns, it hires Community Relations Officers to engage with populations facing obstacles to voting, including diaspora communities. Outside of election periods, Elections Canada works with civil society groups and school educators to deliver educational programming on the electoral process.

Media monitoring

Elections Canada monitors traditional media and the online environment for inaccurate information about the electoral process, such as information about an incorrect election date or inaccurate information about voter identification rules. It does not monitor political discussion, nor does it monitor platforms that are not open to the public. Because its focus is on the accuracy of information, it does not investigate the source or intent behind information.

Elections Canada issues daily monitoring reports during the election period and weekly reports outside of it. These reports are shared with government partners.

Elections Canada may respond to inaccurate information about the electoral process, particularly if it is spreading quickly or has the potential to cause harm. Its main response is to communicate accurate information to the public. Less frequently, Elections Canada may also tell social media platforms about inaccurate information and leave them to deal with it under their terms of service.

Relationships with other government entities

Elections Canada works closely with the Canadian Centre for Cyber Security to ensure the security of its IT infrastructure.

Elections Canada has open lines of communication with the Canadian Security Intelligence Service ("**CSIS**"). Intelligence, including from the Security and Intelligence Threats to Elections Task Force ("**SITE TF**"; see Volume 3, **Chapter 12**), mostly comes to Elections Canada through Election Security Coordination Committees, which are bodies co-chaired by Elections Canada and the Privy Council Office ("**PCO**") that bring together a range of departments and agencies who play a role in maintaining electoral integrity. Intelligence is sometimes shared with Elections Canada in direct briefings by CSIS. Elections Canada has recently enhanced its ability to access Secret level information directly and continues to work to implement secure videoconferencing systems.

Elections Canada is independent from the Critical Election Incident Public Protocol (see Volume 3, **Chapter 12**), but the CEO and the Panel of Five ("**Panel**") can communicate with each other if there are major election incidents. In the event of a serious incident about the administration of an election, the CEO would make a public announcement. Depending on the circumstances, the Panel could make a separate or parallel announcement.

Impact of legislative amendments

The role played by Elections Canada – as well as that of the Office of the Commissioner of Canada Elections, which I discuss below – in responding to foreign interference has been somewhat expanded through recent legislation.

In 2018, Parliament enacted the *Elections Modernization Act* (Bill C-76). This legislation did not focus on foreign interference, but it did make some amendments to the *CEA* that are relevant to that issue. Most notably, the legislation made changes to Canada's political financing rules that limited the extent to which foreign money can be spent on regulated activities such as partisan advertising. As with Canada's other political finance measures, Elections Canada is responsible for implementing these rules.

In March 2024, the Government introduced the *Electoral Participation Act* (Bill C-65). While this legislation was before Parliament for most of the Commission's work, in January 2025 it died on the order paper when Parliament was prorogued. Because the Bill is still relevant for some of the recommendations I have made (see Volume 5, Chapter 19), I will still briefly address it.

Like Bill C-76, Bill C-65 was not specifically targeted at foreign interference. It would have enacted many amendments to the *CEA*, largely in response to the CEO's recommendations flowing from the 2019 and 2021 general elections. Several of those amendments were designed to enhance electoral integrity and could have played a role in countering foreign interference.

With respect to those amendments to the rules within the jurisdiction of Elections Canada, Bill C-65 would have further modified political finance rules, most significantly with respect to third parties. Bill C-65 would have enacted stricter rules on how third parties are permitted to collect and expend money on regulated activities, making them more closely resemble the rules that apply to other regulated entities. These changes were designed to increase transparency and better counter certain types of illicit funding, which have been identified as being used as a foreign interference tactic.

13.3 The Office of the Commissioner of Canada Elections

The Commissioner of Canada Elections ("**CCE**") is the independent officer responsible for enforcing the *CEA*. The CCE is appointed by the CEO after consulting the Director of Public Prosecutions.

The CCE leads a team of approximately 80 employees, including 20 investigators who comprise the Office of the Commissioner of Canada

Elections ("**OCCE**"). The OCCE is primarily a complaints-driven organization. It receives complaints directly from the public, or they can be referred by other agencies. The majority of complaints relate to political finance rules.

Foreign interference under the *Canada Elections Act*

The *CEA* does not include a general prohibition against foreign interference, or even define that term. Therefore, some foreign interference activities are not prohibited by the *CEA*. Other forms of foreign interference may be captured by various provisions of the Act.

The *CEA* has prohibitions that apply specifically to foreign nationals, including prohibitions on making political contributions, expenditures and foreign broadcasts. Bill C-76, which I discuss above, introduced an offence of undue influence by foreigners. This offence is committed when a foreigner – including a foreign government – knowingly incurs an expense or commits an offence in order to influence an elector to vote or not voteat all, or for a particular party or candidate. Other forms of influence, such as statements or other expressions of opinion, are permitted.

The *CEA* also contains prohibitions that apply to both Canadians and foreigners – such as intimidation of an elector – and that can capture some forms of foreign interference.

When a complaint is flagged as potentially involving a foreign actor or foreign funds, the OCCE assigns it to an investigator and treats it as "non-routine," which ensures that it will receive additional supervision.

Bill C-65 would have amended the *CEA* in several ways that are relevant to the OCCE's jurisdiction. It would have established new prohibitions and modified existing ones in relation to false or misleading information about the electoral process. More generally, Bill C-65 would have expanded the scope of certain provisions about the administration and enforcement of the *CEA*, including by granting the OCCE certain powers regarding conspiracies, attempts to commit offences, accessories after the fact or counselling in relation to a violation of the Act.

The OCCE receives many complaints alleging foreign interference that do not constitute an offence under the *CEA* and these are generally closed without further action. During the 2019 election, the OCCE saw a significant rise in complaints related to foreign interference, largely because issues were amplified on social media, and as a result, received multiple complaints about the same matter.

The OCCE identified 201 files with allegations of foreign interference for the 2019 election, which made up about 2% of the complaints it received. For the 2021 election, there were 22 complaints, or roughly 0.5% of all complaints received. However, these cases can take up significant investigative resources.

To date, the OCCE has not taken any formal measures or laid charges in relation to foreign interference, but some complaints have uncovered other contraventions of the *CEA*. It should be recalled that the authority given to the OCCE is limited; it can only investigate contraventions of the *CEA*.

Investigative tools and methods

OCCE investigators rely on open source methods, interviewing witnesses and other law enforcement tools. The OCCE does not have an intelligence department, nor does it use electronic surveillance techniques, informants or human sources. The OCCE can request and examine public documents, including from Elections Canada. It can seek production orders and search warrants. It can apply for a court order to compel testimony under oath or produce documents. The OCCE can seek assistance from outside of Canada under one of Canada's mutual legal assistance treaties.

The OCCE is not a designated recipient of information from the Financial Transactions and Reports Analysis Centre of Canada ("**FINTRAC**"), Canada's financial intelligence authority. Because of this, it does not receive direct disclosures of things like suspicious transaction reports. Instead, it must go through the Royal Canadian Mounted Police ("**RCMP**") to request information from FINTRAC. The OCCE recently asked to be added as a designated recipient of FINTRAC information. The OCCE believes that this will generate leads and address issues of tracing, commingling and obfuscation of funds. I did not hear evidence from FINTRAC and therefore do not know its view on this. However, the request, at first glance, seems reasonable and justified.

Compliance and enforcement

The OCCE enforces the *CEA* through administrative and criminal processes and has a range of tools at its disposal. These include informal measures such as issuing caution letters, and formal measures such as undertakings, compliance agreements, administrative monetary penalties ("**AMPs**") and laying criminal charges. Prosecutions of electoral offences under the *CEA* must meet the stringent standard of proof beyond a reasonable doubt.

AMPs are meant to promote compliance with the *CEA*. Currently, the maximum AMP for a violation by an individual is $1,500, and $5,000 for a corporation or entity. The Commissioner of Canada Elections (CCE) has suggested raising AMPs, particularly for foreign interference.

Under the *CEA*'s criminal regime, the maximum sentences for persons convicted of an offence are five years in prison, a fine of $50,000 for an individual and $100,000 for an entity or both. The CCE has proposed increasing these penalties as well.

I agree with the suggestion to raise both administrative monetary penalties and the maximum fines for criminal convictions under the *CEA* and will return to this in my recommendations.

Election preparation and work during an election period

The OCCE prepares extensively for elections, including evaluating lessons learned from previous elections and building capacity to handle complaints. During election periods, it prioritizes the reception, triage and review of complaints to achieve compliance before election day. The OCCE also works with political parties, designating points of contact for urgent matters during election periods.

In preparation for the 2019 general election, the OCCE established relationships with the research community and subject-matter experts both inside and outside of the government to share knowledge on topics such as foreign interference. It also engages with representatives of provincial and foreign elections management bodies on enforcement issues of common interest.

Since the 2019 election, the OCCE has been concerned about manipulated imagery or videos that could violate the *CEA*. It collaborates with RCMP experts to understand and mitigate these risks. The RCMP provides on-call assistance, especially during critical election times. The OCCE analytical team is responsible for tracking all artificial intelligence and deepfakes related to the elections they come across. The OCCE also monitored the dozens of elections around the world in 2024 to learn and prepare for Canada's next federal election.

Relationships with other government entities

The OCCE has relationships with several partners in the national security and intelligence and law enforcement communities. It has memoranda of understanding with CSIS and the RCMP to facilitate information sharing and assistance. The OCCE participates in the Elections Security Coordinating Committees. It also participates in the Interdepartmental General Election Taskforce that brings together government entities and law enforcement entities to increase efficient intelligence communication during an election.

The OCCE is not part of the Security and Intelligence Threats to Elections Task Force (SITE TF). It has attended some SITE TF meetings, including a series of meetings specific to foreign interference held between November 2023 to June 2024 with an expanded set of participants. If the SITE TF were to expand and offer observer status, the OCCE would be interested in discussing this.

The OCCE is also trying to better equip itself to use classified intelligence in its work. It has worked closely with the RCMP since March 2023 to understand the One Vision Framework developed to facilitate information sharing between CSIS and the RCMP. The OCCE plans to use intelligence in its operations by educating staff about tactics used by other countries. It also plans to use it in investigations and to inform strategic planning. The OCCE continues to work with CSIS to ensure it is part of CSIS's intelligence distribution. If it does not do this, the OCCE noticed that it can sometimes fall off CSIS's radar.

For instance, before reading a February 2024 SITE TF report summarizing electoral interference by the People's Republic of China ("**PRC**"), the OCCE's Executive Director of Enforcement was not aware of a CSIS assessment found within the document. She explained that while this information may not have changed any decisions or investigative steps taken by the OCCE, this classified information is helpful to understanding the threat environment and contextualizing investigations.

To be able to use intelligence, the OCCE is developing its ability to receive, handle and retain classified information. Currently, staff have to travel to other agencies' facilities to review information and intelligence in paper form, which is inefficient, especially during election periods.

The OCCE has made significant progress in its effort to obtain secured communications infrastructure. It has been assessing for a year the feasibility of a project seeking to give it access to Secret level communications at the OCCE's offices. It has also determined that it needs access to the Canadian Top Secret Network ("**CTSN**"). I heard there are still several steps left before the OCCE can access CTSN, including specific qualifications, experience and training. The OCCE's request seems eminently justified to me, and efforts should be made to satisfy it as quickly as possible.

Digital platforms

The OCCE engages with digital platforms to ensure a rapid response to online activities that violate the *CEA*. During an election period, the OCCE's primary concern is ensuring compliance. It coordinates with Elections Canada and other partners about social media activity of concern. With certain platforms, the OCCE can ask for the removal of publications that violate the *CEA*.

The OCCE has no ongoing relationship with WeChat but has had contact with it on matters unrelated to foreign interference.

13.4 The Canadian Radio-television and Telecommunications Commission (CRTC)

Much of the government's policy framework for media is the responsibility of the CRTC, an independent public entity in charge of regulating and supervising broadcasting and telecommunications in Canada. It issues broadcast licences and regulates television and radio, and now streaming services. Its guiding principles are that Canadians should be exposed to many different points of view and news and decide what information they accept, and that the CRTC should interpret its mandate and conduct its activities in a way that does not interfere with freedom of expression.

The CRTC also regulates some of Canada's media ecosystem, which means it could potentially help respond to foreign interference, especially misinformation and disinformation.

Licensing and regulation of television and radio

All broadcasters and distributors of media content over cable and satellite networks are under the CRTC's jurisdiction. Television and radio providers must be licensed unless they receive an exemption. All licensees must be Canadian-owned, as well as Canadian-controlled. This latter requirement means that a licensee must in fact exercise control over its business, which includes control over editorial content and programming decisions.

The term broadcast distribution undertakings ("**BDUs**") refers to cable, Internet Protocol television and satellite operators like Bell or Rogers. BDUs can distribute non-Canadian television programming as part of their subscription packages, but only if the station is on a list maintained by the CRTC. To be placed on the "authorized for distribution" list, a station must be sponsored by a Canadian, such as a BDU. When a station is put on the list, it is subject to certain obligations, but it is not itself licensed.

Responding to foreign interference

The CRTC's Executive Director of Broadcasting told me that the CRTC's greatest challenge in responding to foreign interference is its inability to react quickly. It is a tribunal whose regulatory processes are based on public procedures and records and adherence to rules respecting procedural fairness. If it receives a complaint that a foreign state has instructed a station to broadcast something false on an election day, it is very unlikely that the CRTC could respond in real time.

One example I heard about – a complaint from the Spanish human rights organization Safeguard Defenders – shows how slow the CRTC process can be. The organization complained to the CRTC in December 2019 that two PRC state media channels authorized for distribution in Canada had broadcast confessions that were obtained under torture. The complaint sought to have the stations removed from the authorized for distribution list. This request is still under consideration by the CRTC more than five years later.

Such unfortunate delays are not exclusive to the CRTC, but I cannot help but note that they are likely to discourage the filing of complaints.

The CRTC also has limited authority over user-generated content on the Internet and none over users of social media.

Licensees are subject to the CRTC's *Television Broadcasting Regulations* and equivalent radio regulations. These regulations prohibit licensees from broadcasting content that, among other things, is likely to expose an individual, group or class of individuals to hatred or contempt based on various grounds, including sex, race or ethnic origin. They also prohibit licensees from broadcasting false or misleading news.

The SITE TF has identified manipulation and influence of traditional and online media to control narratives and distribute disinformation as a potential foreign interference threat. The prohibition of false and misleading news in the regulations might prohibit the broadcast of propaganda, as well as misinformation and disinformation. However, the *Broadcasting Act*'s objectives are primarily about supporting cultural expression in English, French and Indigenous languages and upholding and preserving freedom of the press to the greatest extent possible. Thus, the CRTC is very reluctant to become the arbiter of truth or act as a censor. This was a view also held by others in the government.

If a message is broadcast claiming election polls are closed when they are not, then the CRTC might find that false or misleading news. But I heard from the CRTC that it does not have standards of evidence against which to assess contested factual issues or the capacity to carry out intensive factual investigations.

Also, even if the CRTC were to find that a licensee or a channel authorized for distribution was broadcasting false or misleading news, it cannot prevent use of the Internet to spread this material. This is illustrated by the events that surrounded the decision to ban the distribution of Russia Today ("**RT**") on television in Canada.

RT is a Russian state media outlet, that was on the authorized for distribution list and so could be broadcast in Canada. In 2022, when Russia invaded Ukraine, RT broadcast content seeking to justify the attacks on Ukraine by promoting a narrative that spread hate against Ukrainians. In response, the Governor in Council (i.e. the Governor General acting on the advice of

Cabinet) asked the CRTC to assess whether RT's content was in support of, or contrary to, the *Broadcasting Act*.

The CRTC held a hearing and concluded that it was not in the public interest to continue to authorize the distribution of RT. While RT was not a licensee, if it had been one, its broadcast would have been in violation of the *Television Broadcasting Regulations* because it exposed Ukrainian people to hate or contempt. It was therefore removed from the list. This is the first time a non-Canadian station has been removed from the authorized for distribution list for non-administrative reasons.

While RT's content is no longer available on television, its content remains accessible online in Canada since the CRTC's decision does not apply to the Internet.

Relationships with other government entities

The CRTC has information sharing memoranda of understanding with entites like Elections Canada and the Office of the Commissioner of Canada Elections (OCCE). The CRTC has referred some complaints to Elections Canada and vice versa. In September 2024, the CRTC received information from the OCCE about potential PRC ownership or control over Canadian licensees. At the time of drafting this report, the CRTC was still determining the next appropriate steps.

13.5 The House of Commons

The House of Commons ("**House**") is the elected assembly of the Parliament of Canada. The House consists of 338 members of Parliament ("**MPs**") elected by Canadians. The Speaker presides over the House and chairs the Board of Internal Economy, which is the House's governing body for administrative and financial matters. The Board oversees the House administration.

As a democratic institution, both the House and its members may be the targets of foreign interference. Foreign interference issues involving MPs are handled as matters relating to the general security of the House. The Office of the Sergeant-at-Arms and Corporate Security ("**Sergeant-at-Arms**") is responsible for the institutional security of the House, as well as the personal security of individual MPs outside the Parliamentary Precinct. This includes their constituency offices and their private residences.[19]

[19] Within the Parliamentary Precinct, the security of parliamentarians is the responsibility of the Parliamentary Protective Service, which is a separate entity from the House administration.

The Digital Services and Real Property directorate ("**Digital Services**"), headed by the Chief Information Officer ("**CIO**"), is responsible for information and cyber security.

Personal security

The Sergeant-at-Arms oversees about 114 employees, who develop corporate security policies and programs. The Sergeant-at-Arms acts as liaison with intelligence and law enforcement agencies to address security matters, including foreign interference. Law enforcement partners include the RCMP, police forces of jurisdiction and the Parliamentary Protective Service.

The Office of the Sergeant-at-Arms has regular communication with both the RCMP and CSIS and has a memorandum of understanding with the Privy Council Office (PCO), CSIS and the RCMP that allows for the exchange of information.

The Sergeant-at-Arms monitors open source intelligence for threats and harassment toward MPs. If it detects a physical threat, this is brought to the attention of the risk management team, who works with the RCMP and the police force of jurisdiction. The Sergeant-at-Arms and the RCMP each generate reports every weekday morning about threats to MPs. The RCMP's reports have input from the PCO Security and Intelligence Secretariat.

The Sergeant-at-Arms conducts security screening for the House. This is required for prospective House employees, an MP's staff, students, volunteers and service providers who require access to the Parliamentary Precinct or the House's computer network. It does not apply to MPs themselves, who do not require a clearance to sit in the House.

Physical site access is granted based on an analysis of information received from CSIS and the RCMP. This is a distinct process from security clearances, which are needed to access classified materials and are done by the government.

To perform site access security screenings, the Sergeant-at-Arms does criminal background checks and "loyalty to Canada" investigations with the assistance of the RCMP and CSIS. When issues arise, the Sergeant-at-Arms may conduct a "resolution of doubt" interview. The number of these interviews has increased significantly over time – there were 10 in 2019, and 128 in 2023. Only a handful of accreditations have been refused in the past decade because of foreign interference concerns. However, two such refusals happened between March and September 2024.

The fact that two security screenings have led to refusals linked to foreign interference between March and September 2024 – even if such refusals were rare in the past – can mean more than one thing: foreign interference is more present, security screenings are more thorough or this is only happenstance.

Information and cyber security

The Chief Information Officer (CIO) heads a team of about 760 employees who oversee and provide IT security infrastructure, applications and support to the House, MPs, House employees and MPs' staff. The House cyber security system includes security policy, compliance, threat detection and staff awareness and training.

House IT systems are independent from the government. Digital Services supports the network infrastructure common to all parliamentary partners, namely the Senate, the Parliamentary Protective Service and the Library of Parliament.

The House IT security program is based on both proactive and reactive measures. The House adopts a multilayered approach based on industry standards for reducing risk and ensuring MPs can conduct their business efficiently, whether in caucus, at their constituency office or in the Chamber. There are controls in place for devices and users, as well as perimeter controls, including at points of contact with the Internet as well as with government networks.

The House provides MPs with computers for their Parliament Hill and riding offices. MPs are not supposed to use these devices for partisan activities like fundraising or seeking re-election. This means that MPs may end up using their personal devices for both parliamentary and partisan activities. Different MPs have different approaches to the number of devices that they use, and how they use them.

MP John McKay testified that the line between parliamentary and partisan affairs can sometimes be blurry and that, in his view, there will inevitably be times when House equipment is used for activities viewed as partisan. MP Garnett Genuis explained that he often receives communications from constituents about legislative matters or other parliamentary work on his personal devices.

The House administration has no authority over the use of personal devices by MPs and does not have the ability to monitor their use in the same way that it monitors the House's own IT infrastructure. Further, the House does not provide IT services for home Internet despite the fact that some MPs may use their home networks for parliamentary work. However, if an MP suspects that a personal device has been hacked, Digital Services can be asked to examine and analyze the device.

Digital Services also provides MPs with the ParlVoyage program, a parliamentary travel service with access to a secure IT environment for parliamentary functions when travelling to high-risk destinations. Digital Services provides cyber security briefings and awareness sessions as part of this program.

Digital Services has a memorandum of understanding and longstanding relationship with the Communication Security Establishment's ("**CSE's**") Canadian Centre for Cyber Security ("**CCCS**"). It has regular meetings with CCCS, both scheduled and in response to specific incidents. CCCS's role is to assist with the protection of the House infrastructure perimeter and incident management.

Digital Services and CCCS also share information about cyber security awareness, best practices and new trends. CSE shares intelligence with Digital Services on a "need to know" basis CCCS if consistent with its mandate to protect the House from cyber threats. Digital Services cannot share MPs' information without their consent.

Digital Services regularly receives information from CCCS about cyber threats. These come as formal technical bulletins from CCCS, with a request for action or a recommendation. Digital Services will not necessarily know if a given threat activity is being done by a foreign government.

CCCS may ask Digital Services for information to help CCCS understand a cyber threat. CCCS can investigate the perimeter of the House's IT network but not inside it and so has to ask Digital Services for information.

If Digital Services detects or becomes aware of a cyber attack, it does not necessarily disclose it to parliamentarians. It does not notify anyone about unsuccessful cyber attacks because of the staggering number of these that occur on a daily basis. Attacks that focus on a specific parliamentarian may be reported to that MP. The Speaker of the House is notified when an attack affects parliamentary activities or poses a reputational risk to the House.

It would be impossible, and probably counter-productive, to inform parliamentarians of all cyber attacks. However, in my view, parliamentarians specifically targeted by a cyber attack should be informed. They can then take the measures that they consider appropriate.

Training about foreign interference for MPs and staff

As I discuss in more detail in Volume 4, Chapter 15, the House coordinates with national security and intelligence as well as law enforcement agencies to give unclassified briefings about foreign interference to MPs and staff. These briefings are also provided to the caucuses of all recognized parties, the Green Party of Canada ("**Green Party**") and independent MPs. Briefings were also given this year to House staff. The briefings relate to the current foreign interference threat landscape and precautions that can be taken.

Digital Services provides cyber security training to MPs and staff. It also has a general cyber security awareness program for MPs about the evolving cyber threat landscape. For example, Digital Services added a "phishing reporting" button in its email software for users to easily report suspected phishing attempts. It is also in the process of developing awareness material on foreign interference generally, as well as cyber awareness content about foreign interference.

13.6 The Senate

The Senate is the Upper House of the Parliament of Canada. There are 105 senators appointed by the Governor General on the recommendation of the Prime Minister. As part of their legislative role, senators scrutinize legislation and can propose amendments to bills. Senators can also propose their own bills. They play an important role in looking at issues of national importance, especially through the work of committees.

Like the House, the Senate regulates itself. It is supported by a non-partisan administration headed by the Clerk of the Senate. The Senate administration is organized into the Legislative Services Sector, the Corporate Sector and the Legal Sector.

As with the House, the Senate handles foreign interference concerns as matters of general security. The institutional security of the Senate is the responsibility of the Corporate Security Directorate ("**CSD**"), while IT-related aspects of security are handled by the Information Services Directorate ("**ISD**").

Institutional security and personal security of senators

CSD has approximately 42 employees. It is the main strategic advisor for all matters of institutional security, including plans and measures relating to physical security. Physical security operations are the responsibility of the Parliamentary Protective Service. CSD responsibility includes accreditation, residence security for senators and security for senators when travelling.

When senators are appointed, CSD gives optional onboarding training to them and their staff, which includes content on foreign interference. The CSD also provides briefings to Senate groups and caucus meetings. When senators travel internationally on Senate business, the CSD provides them and their staff with advice and briefings.

CSD works with law enforcement and intelligence agencies, both proactively and in response to specific incidents. CSD and CSIS usually meet at least four times a year and sometimes more. These meetings sometimes also include the RCMP. CSD shares open source information daily with, and receives information from, the House, the RCMP, CSIS, local police and Global Affairs Canada.

Information and cyber security

The Information Services Directorate (ISD) is responsible for IT equipment for all senators and Senate employees. ISD also provides services like phishing detection. It has a team that deals with cyber security and IT security. IT-related foreign interference issues are brought to this team.

ISD provides essentially the same equipment and support to senators as Digital Services does for MPs but does so independently from the House. ISD does not usually provide support to senators for personal email and social media. However, it may offer to help prevent the spread of malware or attacks on the reputation of a senator.

ISD gives mandatory training to senators and staff. There are two mandatory training courses for senators. The first explains how to handle information over its entire life cycle. The second, provided within the first two weeks of a senator's arrival, raises awareness of cyber security. In addition, the head of ISD, or someone from their team, meets with each new senator to talk about cyber security risks. ISD also runs phishing simulations for senators.

ISD has guidelines for senators when they travel and asks senators to contact it before they go. ISD does risk assessments based on where senators are travelling to and who they are meeting with.

ISD has implemented several best practices recommended by the Canadian Centre for Cyber Security (CCCS). Unlike the House, it does not have a memorandum of understanding with CCCS. However, ISD does collaborate with CCCS, the House, Corporate Security Directorate (CSD) and the RCMP on cyber threats. It would be advisable to formalize this collaboration in a memorandum of understanding.

13.7 Political Parties

Political parties are on the frontlines of our democratic institutions. They are also a potential target of foreign interference. All political party representatives who testified at the public hearings expressed some concern about parties potentially being a target for foreign interference.

That said, the leaders of these political parties seem generally averse to measures to counter foreign interference that would also have the impact of limiting their autonomy. The representatives who testified before me were all firmly opposed to regulation of leadership and nomination races. They all stated that the internal measures that have been put in place to ensure the integrity of these races are sufficient. In my view, they are not.

Political parties are self-governing entities. Parties are essentially free to make their own rules to regulate their membership, choose their candidates and select their leaders.

Membership criteria and fees

Broadly speaking, a political party's membership determines who can vote during a leadership or nomination contest, who may hold offices within the party and who can participate in party conventions during which party policies are usually determined. A party's rules are an important reflection of its values and commitments, such as youth engagement or democratic participation.

The Conservative Party of Canada ("**Conservative Party**"), New Democratic Party of Canada ("**NDP**") and Green Party require members to be citizens or permanent residents. At the time of the public hearings, the Liberal Party of Canada ("**Liberal Party**") extended eligibility to all those who ordinarily live in Canada and to Canadians living abroad who are eligible to vote in federal elections. On 9 January 2025, it announced that it had decided to change its rules for gaining and maintaining membership in the Liberal Party. Under these rules, an individual must be a Canadian citizen, have status under the *Indian Act*, or be a permanent resident of Canada. The Bloc Québécois has no citizenship or residency requirement.

Most parties require members to be at least 14 years old, although the NDP's age requirement varies between 12 and 14 depending on the province or territory.

Most parties charge a membership fee. Some parties allow cash payments (the Green Party, the NDP and the Bloc Québécois) while others like the Conservative Party do not. The Liberal Party does not charge a membership fee.

Parties use various measures to ensure compliance with their membership rules. Examples of measures used include requiring applicants to attest that they meet eligibility requirements by checking a box, monitoring the IP addresses of those who buy memberships online and prohibiting bulk membership purchases.

Candidate nomination contests and selection

Each party sets and enforces its own rules for nomination contests, including qualifications for contestants, if and when a nomination meeting (where the voting happens) is called and how the meeting will be run. These rules typically involve a distribution of responsibility and power between the central party and electoral district associations.

Electoral district associations are party organizations active in a specific riding. They are typically involved in recruiting potential candidates to represent the riding for the party. They also organize and facilitate nomination meetings.

Parties generally have a vetting process before someone is able to run in a nomination contest. Although parties do not vet for foreign interference concerns specifically, the vetting process could uncover such information. Usually, parties review the potential contestant's social media and Internet presence, their work history and professional links, as well as their affiliation with organizations or other groups. Some parties do a criminal background check, and one party requires prospective contestants to consent to disclosure of information from a range of government agencies and departments. Another party relies on an external company to do its vetting. Thus, there is no standard vetting process common to all parties.

Voting in a nomination contest is generally limited to party members living in the riding. Each party uses a different verification process to confirm voting eligibility. Most require members to show identification displaying their name, address and photograph. At least one party will waive identification requirements when exceptional circumstances warrant. There are generally mechanisms in place if a nomination contestant wishes to appeal the conduct or the results of the nomination meeting.

Under the *Canada Elections Act* (*CEA*), a party's leader must sign the paperwork for each of the party's endorsed candidates. If the leader chooses not to sign a candidate's papers, that individual cannot run under the party's name, even if they won the nomination contest. Parties are not, in fact, required to hold nomination contests.

The leader's power to reject candidates selected by a nomination contest has been suggested as a way to defend against foreign interference. As I explain in Volume 4, Chapter 13, if a leader becomes aware of foreign interference concerns about a candidate early enough, they can prevent them from running for the party.

As I explained in Volume 3, **Chapter 10**, the SITE TF suggests that nomination contests could be used by foreign states to target candidates and ridings to influence who may become an MP. I agree. That said, the evidence before me does not indicate that foreign interference in federal nomination processes has been widespread to date. I heard evidence relating to potential foreign interference with only one federal nomination contest: Don Valley North (see Volume 2, Chapter 7). I note that this is the only instance of potential foreign interference with a nomination process mentioned in the government's list of major instances of suspected foreign interference in Canada's electoral processes (see Volume 3, **Chapter 10**).

Leadership contests

I heard that political party leadership contests may also be a source of vulnerability to foreign interference.

Today, leadership races are one-member-one-vote contests that allow every member of a party to cast a ballot to elect the leader. The one-member-one-vote method incentivizes contestants to sign up as many members as possible.

Political parties run their own leadership contests and are free to determine their rules. For example, parties can determine the cut-off dates for individuals to register as a contestant and to sign up members. They can set spending limits for contestants or require them to provide a minimum deposit or fee to the party. Parties determine the duration of the leadership race, the rules for voting and how results will be communicated.

Parties tend to determine the specifics of each leadership race on a case-by-case basis, which means that the rules change over time depending on general trends in democracy and culture and on the specific circumstances that exist at the time.

The Commission heard evidence about allegations of Government of India interference in a Conservative Party leadership race. CSIS witnesses noted that they had no reason to believe the impacted candidate would have been aware of the alleged support. They also noted that, while concerning, not all India's activities in this matter were covert.

The intelligence about this matter was disseminated to senior Privy Council Office (PCO) officials and the National Security and Intelligence Advisor to the Prime Minister in two products, one of which was also disseminated to senior Public Safety Canada officials. It was also included in an intelligence assessment widely distributed throughout the intelligence community and part of a SITE TF update to the Deputy Minister Electoral Security Coordinating Committee (see Volume 2, Chapter 6). CSIS officials had no recollection of having briefed this intelligence to the political level, including to the candidates themselves.

In January 2024, CSIS and the Integrated Terrorism Assessment Centre ("**ITAC**") delivered a defensive briefing to the Conservative Party leader's Chief of Staff.[20] This briefing was the result of an ITAC product that was primarily focused on the threat of violent extremism. It also included high-level information about threats of foreign interference that might target the Conservative Party leader. CSIS did not share information about the allegations of interference in the leadership race with the Chief of Staff at this time, as the briefing was unclassified.

[20] CSIS has offered several defensive briefings to members of Parliament. I discuss this further in Volume 4, Chapter 15.

In June 2024, CSIS delivered a classified briefing to the Conservative Party leader's Chief of Staff. CSIS's Deputy Director of Operations explained that this briefing was an example of broader efforts to provide classified information to increase resilience to foreign interference. The purpose of the briefing was to provide general information, supported by different specific examples of foreign interference threat activities and tactics. At this time the Conservative Party's leader's Chief of Staff was advised of the allegations of interference in the leadership race.

13.8 The Media

Because misinformation and disinformation can have a significant impact on all Canadians, a healthy media ecosystem is important to build citizen resilience against foreign interference.

Resilience in this context has been described as ensuring the population is properly equipped to know when to validate information with credible sources of information before accepting certain information as true. Canadians must be equipped to understand that all information is not necessarily true, and that not all information should be given the same weight.

It is therefore important to Canadian democracy that our population has credible and reliable sources of trusted information to counterbalance misinformation and disinformation. Journalism and news media are essential to protecting Canada's democratic institutions, including elections. Witnesses from the Department of Canadian Heritage spoke about the importance of supporting Canadian media to ensure news is trustworthy and of good quality. In light of the evidence heard, I agree entirely, but I would add that it is also important that media be independent from government and political parties.

13.9 Civil Society Organizations

Many witnesses said the role of civil society is crucial for a whole of society approach to detect, deter and counter foreign interference. The Commission did not have the capacity to investigate all civil society groups who may play a part in responding to foreign interference in democratic institutions. However, this section describes work to help Canadians defend against misinformation and disinformation, which government and non-government witnesses said was a significant method of foreign interference. It is also the most pervasive and difficult to counter.

The Media Ecosystem Observatory (MEO)

I heard evidence from three witnesses from the Media Ecosystem Observatory (**"MEO")**. The MEO was created in the lead up to the 2019 federal election, as a collaboration between the Max Bell School of Public Policy at McGill University and the Munk School of Global Affairs & Public Policy at the University of Toronto. It aimed to address gaps in researchers' understanding of what was happening in the Canadian information ecosystem, including during election periods. The MEO studies the flow of information in the media ecosystem and behavioural responses to that information. It monitored and produced reports examining the digital information ecosystem during the 2019 and 2021 federal elections (see Volume 2, Chapters 7 and 8).

The MEO's approach recognizes that misinformation and disinformation circulate in the same way as truthful information, and it is often challenging to delineate the truth or falsity of a statement. What is more, the origin of a piece of information is often impossible to know. Instead of focusing on individual pieces of information or attempting to identify possible information manipulation based on the source, the MEO instead tries to understand the information ecosystem as a whole. To do this, the MEO mainly collects three types of information.

First, it collects digital trace data from online platforms, which includes metadata such as likes, shares, comment counts, embedded links, uploaded photos, hashtags and mentions. With these data, it traces the spread of information among users on and between platforms. The MEO monitors around 4,000 Canadian accounts that appear to have the most significant impact on the spread of political information, as well as key accounts from foreign countries (primarily from the PRC, Russia and India) that produce misinformation and disinformation relevant to Canada.

Second, the MEO surveys Canadians. It uses surveys to assess the impact on Canadians of events in the information ecosystem. These surveys try to determine if the information that circulates changes individuals' views or behaviours.

Third, the MEO does media monitoring where researchers read online information to get qualitative data about the ecosystem. This information helps to contextualize the empirical data obtained by the MEO and to describe information trends.

The Canadian Digital Media Research Network (CDMRN)

In April 2022, the MEO received a grant from the Digital Citizenship Contribution Program – which I discuss in Volume 3, **Chapter 12** – to develop the Canadian Digital Media Research Network **("CDMRN")**. The CDMRN is a partnership between the MEO and nine other organizations. It tries to understand the Canadian information ecosystem, describe the ordinary baseline of the information environment and respond to "information incidents"—that is, disruptions to the information ecosystem that significantly impact the normal flow or integrity of information.

One of the MEO's conclusions from monitoring the 2021 election was that the ability to quickly understand and contextualize external interventions in the media ecosystem would be useful, as compared to having to wait for analysis after the fact. This led its organizers to think about developing greater capacity for understanding the media ecosystem, particularly during election periods.

The CDMRN's incident response protocol is intended to provide this capacity. Information incidents may be detected through the MEO's monitoring or through tips from research partners or journalists. The MEO will assess whether the incident is sufficiently serious, and if so, designate an incident response team and use the resources of the CDMRN to analyze the incident and provide frequent, timely and public reporting as the incident unfolds. The CDMRN will ultimately produce an incident summary.

During elections, the CDMRN plays a somewhat similar role to GAC's Rapid Response Mechanism Canada (see Volume 3, **Chapter 11**). The CDMRN, however, is operationally independent from the government. While the MEO receives significant government funding and regularly briefs civil servants about its public findings, the MEO does not take direction from the government and its reports are public. The information it gives to the government is the same as what is provided to the public.

Challenges facing the MEO and the CDMRN

The CDMRN is intending to monitor the online ecosystem during the next federal election. However, I heard two things potentially threaten the capacity of MEO and the CDMRN to do this work. The first is funding. The work of MEO and the CDMRN is resource intensive and relies on government funding. While the government expects the CDMRN to play an important role during the next election, it is only funded through to the end of March 2025. Funding uncertainty beyond 2025 impairs the MEO's ability to plan its operations and recruit and retain staff.

The second area of concern arises from changes in the ability of the MEO and other civil society organizations to access critical data through social media platforms' application programming interfaces ("**APIs**"). Recently, platforms that were giving non-governmental researchers free or low-cost access to their API have significantly increased prices for data access or limited data that are available or both. Restrictions on API access significantly limit the MEO's ability to do its work and have created what witnesses described as a crisis in the research community globally. This issue is beyond the Commission's mandate, but I believe the government should look into it.

13.10 Conclusion

Attempting to catalogue all the entities that play a role in responding to foreign interference would be an impossible task within a report of this size. Defending Canada's sovereignty and democracy necessarily requires efforts from the whole of society.

The conclusion to draw from this chapter is simply that there are many types of institutions and actors with a range of roles that are relevant to how Canada responds to foreign interference. Effective response requires effort from all of them.

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.

Term	Acronym or Abbreviation	Definition
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
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.

Term	Acronym or Abbreviation	Definition
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.
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".

Term	Acronym or Abbreviation	Definition
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.
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.

Term	Acronym or Abbreviation	Definition
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.
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.

Term	Acronym or Abbreviation	Definition
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.
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.

Term	Acronym or Abbreviation	Definition
Misinformation (Mésinformation)		False or inaccurate information (not intended to mislead). See also “Disinformation.”
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.

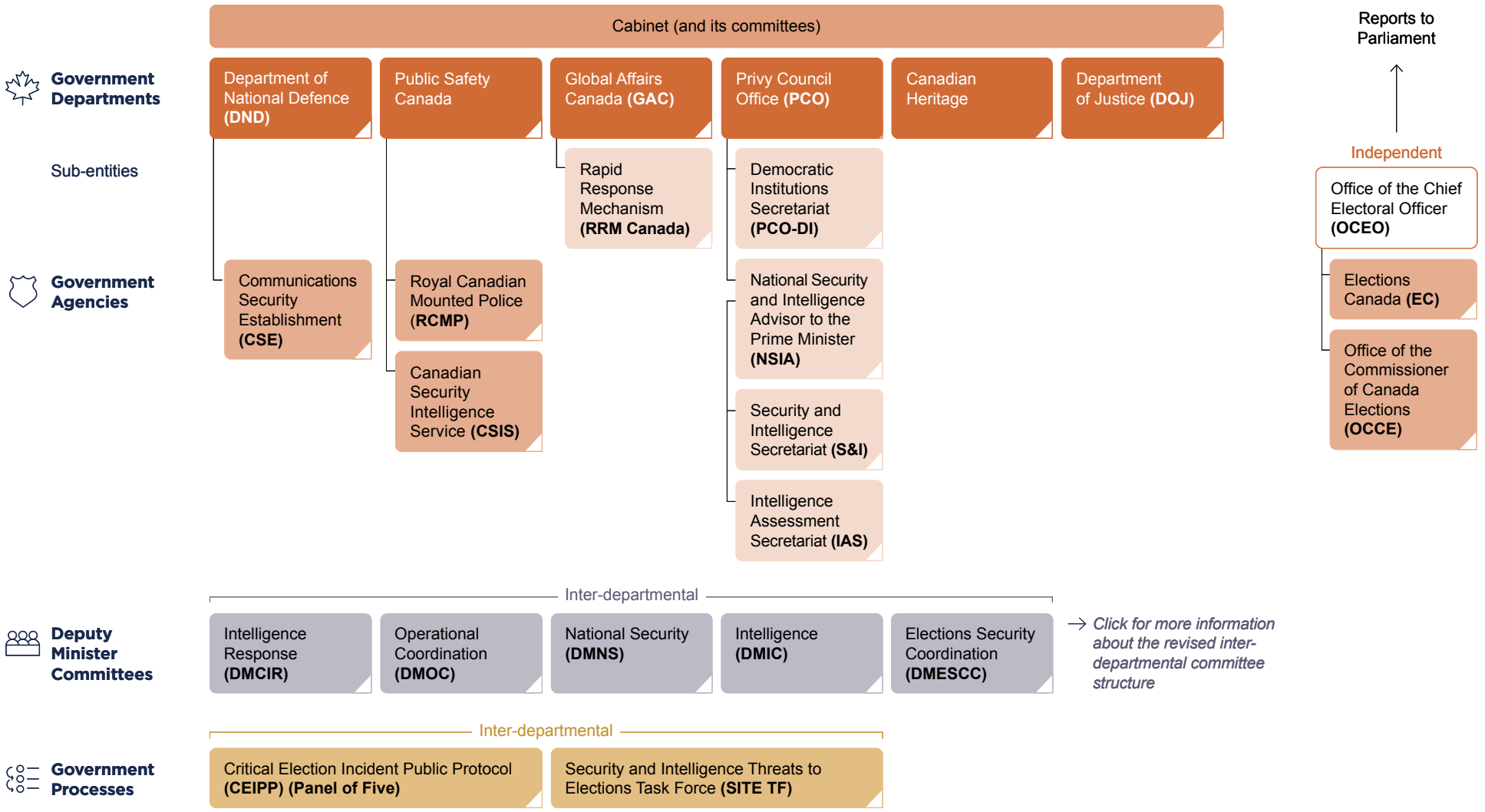
Term	Acronym or Abbreviation	Definition
— Parliamentary privilege (Privilège parlementaire)		Rights and immunities deemed necessary for the House of Commons and the Senate and their members to fulfill their functions. For example: freedom of speech in the House and in committees of the House, and exemption 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