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

The Honourable Marie-Josée Hogue,
Commissioner

VOLUME 1

Report Summary

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 1: Report Summary.

Cette publication est également disponible en français :
Volume 1 : Synthèse du rapport.

CP32-169/2-2025E-1-PDF
ISBN 978-0-660-75079-8

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

A Word from the Commissioner

On 7 September 2023, the government established the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions ("**Commission**") and appointed me Commissioner. Last May, I tabled an Initial Report with preliminary findings on certain aspects of the mandate entrusted to me. I am now delivering the Final Report, which summarizes all the evidence presented before me and the conclusions I have drawn from it. This report covers all aspects of my mandate and includes my recommendations.

Since 18 September 2023, I have devoted myself exclusively to the work of the Commission, with the support of a team of seasoned professionals. My team has conducted a rigorous and thorough investigation. I heard from more than 150 witnesses over 39 days of public hearings and several weeks of *in camera* hearings. I had access to the documents I deemed relevant, without redactions for national security reasons. I had unprecedented access to certain Cabinet confidences. I also met Canadians from a range of diaspora communities who have been particularly affected by certain aspects of foreign interference, and reviewed submissions from hundreds of citizens. I further benefited from the enlightenment of academics and field experts.

All these elements have enabled me to carry out my mandate of examining and assessing foreign interference and its impact on the integrity of the 2019 and 2021 general elections, the flow of information within the government apparatus relating to these matters and the measures taken in response to this information, as well as my broader mandate to examine and assess the capacity of various government actors and processes to detect, deter and counter foreign interference in our democratic institutions, including electoral processes. They have also informed my recommendations on how to enhance the protection of democratic processes against foreign interference.

The Commission was faced with the challenge of striking a balance between the public nature of its proceedings and the confidential nature of certain information relevant to its mandate, the disclosure of which could be detrimental to national security. For this reason, my report includes a classified supplement. Nothing in this supplement contradicts the findings and conclusions of my report. Rather, it provides specific details that I was unable to include in this report.

I would add that the Commission not only had access to a significant quantity of confidential documents, it also negotiated the public release of as much information as possible from these documents, while taking the precautions necessary to protect national security. I believe that the Commission has thus succeeded in maximizing the transparency of its work.

The first observation I would like to make from the evidence is that it is true that some foreign states are trying to interfere in our democratic institutions, including electoral processes. This is nothing new and comes as no surprise – states have been trying to interfere with each other's business since time immemorial. What is new, however, is the means deployed by these states, the apparent scale of the issue and the public discourse on the topic.

I have also noted that our democratic institutions have thus far remained robust:

- Although there are a very small number of isolated cases where foreign interference *may* have had some impact on the outcome of a nomination contest or the result of an election in a given riding, there is no evidence to suggest that our institutions have been seriously affected by such interference or that parliamentarians owe their successful election to foreign entities. While any attempted interference is troubling, I am reassured by the minimal impact such efforts have had to date.
- Nor have I seen any evidence of "traitors" in Parliament plotting with foreign states to act against Canada. Although a few cases involving things like attempts to curry favour with parliamentarians have come to light, the phenomenon remains marginal and largely ineffective. I am not aware of any federal legislation, regulations or policies that have been enacted or repealed on account of foreign interference. While the states' attempts are troubling and there is some concerning conduct by parliamentarians, there is no cause for widespread alarm.
- Fortunately, I did not come across a situation where a parliamentarian decided not to speak out, or expressed an opinion that was not really their own, out of fear of reprisals from foreign actors. However I attribute this to the courage of our elected officials, because the risk is real - particularly given the potential for retaliatory disinformation campaigns by foreign states.

I also note from the evidence that Canada has responded to attempts at foreign interference with measures and mechanisms to better detect, deter and counter them. I took note of the competence, dedication and experience of the members of Canada's senior public service and national security and intelligence community who testified before me. These men and women, who work in the shadows and beyond partisan lines, play a crucial role in safeguarding our democratic institutions, and they do it well.

That said, the government's response has been far from perfect:

- I have observed that the government has sometimes taken too long to act, and that coordination between the various players involved has not always been optimal.
- Processes by which information had to be passed on to certain decision-makers, including elected officials, have not proved as effective as they should have been.
- In addition, the government has proven to be a poor communicator and insufficiently transparent when it comes to foreign interference.

The measures implemented over the past two years, along with several statements made on the matter, suggest that the government is now prioritizing the fight against foreign interference. This must continue.

I particularly would like to highlight the intention expressed by a number of government actors to improve communication with the public and increase transparency on the issue of foreign interference. In the current climate, I believe this is essential. On the one hand, trust in Canada's democratic institutions has been shaken, and it is imperative to restore it. This can only be achieved through greater transparency. On the other hand, while the government has the primary responsibility for ensuring national security and protecting our democratic institutions, what I have read and heard convinces me that society as a whole must help defend these institutions. To achieve this, the government must step up its efforts in educating and informing the public about foreign interference.

So far, its efforts in this regard have been piecemeal and underwhelming. If the public is to play its part in countering the threat of foreign interference, it must better understand what it is.

Greater transparency would ensure that Canadians are not entirely dependent on media reports and leaked information (which can easily be misleading or be misunderstood) to learn about attempts or acts of foreign interference. Leaks are illegal, ill-advised, and must undoubtedly be denounced. The risk of leaks increases if government agencies keep such incidents almost entirely secret, and the dependency on investigative reporting will persist. Of course sometimes the government is justified in keeping its operations secret, and in matters of national security sometimes it is vital to do so. But the national security and intelligence community must work hard to find ways to keep Canadians informed. Properly informed, I have no doubt that Canadians will be able to understand what foreign interference is and help defend Canadian democracy against this threat.

Canadians also need to be better informed about what intelligence is and the significant limitations it entails. In my view, the level of alarm among elected officials and the general public that followed the report tabled in June 2024 by the National Security and Intelligence Committee of Parliamentarians (better known as "NSICOP") illustrates the impact this lack of knowledge and understanding can have. The information in the NSICOP Report should not have come as a total surprise.

Canada has been fortunate not to face the level and extent of national security threats that many of our allies have up until now. But there is no guarantee that this will always be the case, and indeed, at this point in time it seems unlikely to continue. As threats increase, Canadians need to be better informed.

The Commission's experience has shown that a great deal of information can be made public without compromising national security, as several witnesses from the national security and intelligence community who appeared before me readily acknowledged.

This work is certainly both challenging and difficult, but it is essential if we are to preserve the health of our democracy.

A healthy democracy is characterized by a vibrant and diverse range of voices and groups, engaged in a constant process of deliberation, discussion, negotiation and compromise. Because of this characteristic, democracy requires a civic setting in which people can freely express their ideas. To create such a setting, democracy relies on values and principles such as the equality of individuals and respect for others, as well as consideration for the diversity of opinions and beliefs. It requires social and political institutions that encourage the participation of all.

By fostering distrust, creating division and preventing compromise, disinformation threatens this fundamental feature of democracy.

The evidence reveals that foreign interference comes in a variety of forms, and that the means deployed are evolving. Some actors still use traditional methods, but many are now attempting to interfere in our democracy by engaging in disinformation on social networks. While allegations of interference involving elected officials have dominated public and media discourse, the reality is that misinformation and disinformation pose an even greater threat to democracy.

Some spread disinformation about candidates and elected officials who express views that diverge from their own interests. Their goal is to try and prevent these candidates from getting elected, and to affect policy choices and positions.

Disinformation can sometimes be directed at a political party as a whole, as appears to have been the case in 2021 when the Conservative Party of Canada, under the leadership of Erin O'Toole, was the target of a disinformation campaign (though the evidence could not establish a definitive link to the People's Republic of China).

Disinformation is also used as a retaliatory tactic, to punish decisions that run contrary to a state's interests. This may have been the case with a disinformation campaign that followed the Prime Minister's announcement regarding suspected Indian involvement in the killing of Hardeep Singh Nijjar (though again no definitive link to a foreign state could be proven).

Others engage in disinformation with the sole aim of stirring up division within democracies. Their aim is not to favor or harm a candidate, but rather to spread the idea that democracy does not work. The goal is to sow mistrust in our society. Russia is the prime example of this.

Disinformation is difficult to detect and, above all, to counter since the technological means available evolve at breakneck speed. It is noxious, and it is powerful, it poses a major risk to Canadian democracy. If we do not find ways of addressing it, misinformation and disinformation have the ability to distort our discourse, change our views, and shape our society. In my view it is no exaggeration to say that at this juncture, information manipulation (whether foreign or not) poses the single biggest risk to our democracy. It is an existential threat.

The Commission's work has also shown that transnational repression is a genuine scourge. I did not examine this phenomenon in depth since this form of foreign interference goes well beyond the democratic processes and institutions my mandate tasked me with examining. But what I have learned about it is sufficient for me to sound the alarm that the government must take this seriously and consider ways to address it. My understanding is that this is underway.

Canada faces a significant challenge: finding ways to counter the threat of foreign interference in our democracy while safeguarding the fundamental values it embodies, namely freedom of thought, freedom of opinion, freedom of expression and the right to privacy. Moreover, the fight against foreign interference cannot come at the cost of stigmatizing vulnerable communities. Such stigmatisation would be entirely unjustified and would play directly into the hands of foreign actors seeking to sow discord.

Countering foreign interference is a challenge that all of us who live in Canada must confront, together.

Marie-Josée Hogue, Commissioner

Acknowledgements

The work required to carry out the mandate entrusted to me was important, sensitive and urgent. This meant that I needed a talented, dedicated, responsible and willing team. I was fortunate enough to find one.

Co-Executive Directors Annie Desgagné and Casper Donovan ran the Commission's administrative operations masterfully, showing rigour, flexibility, intelligence and sound judgment. Hélène Laurendeau generously agreed to act as interim director when circumstances forced both co-directors to be absent at the same time. I would like to thank all three of them.

Though small in size, their administrative team did a tremendous job. Each team member showed exceptional dedication and has my sincere gratitude. I would especially like to thank my assistant, Florence Benoit, who agreed to come with me from the Quebec Court of Appeal to the Commission.

Of course, none of this would have been possible without the hard work of the team of lawyers masterfully led by Lead Counsel Shantona Chaudhury. From the youngest to the most experienced, they all impressed me with their energy, hard work and desire to serve the public interest.

I should also mention the work carried out by the lawyers representing the Participants, including the Attorney General of Canada. Their work was exemplary, as their collaboration with Commission Counsel. They fulfilled their duty to represent their clients, showing forcefulness when necessary, but doing so constructively.

I was also fortunate enough to receive valuable input from highly experienced advisors with hands-on experience in a number of fields related to the Commission's work. They offered their expertise when I needed it and gave me invaluable advice.

The Research Council, headed by Professor Geneviève Cartier, was also a great help. The Council organized round tables during which I was able to hear the views of over 40 experts. Having spent considerable time reflecting on many of the problems we discussed, the members of the Research Council helped me assess the pros and cons for the various solutions that were proposed.

I suspected that highly technical language would be used in many of the documents and testimony. Since I wanted all of the Commission's documents to be as easy as possible for the average reader to understand, I arranged for the Commission to have a lawyer specializing in plain language. I entrusted this task to Guillaume Rondeau, who oversaw the drafting of a number of documents, including the Initial and Final Reports. He met this challenge with great success.

A communications advisor, Michael Tansey, was in charge of keeping the media and the public informed about our work. He answered questions tirelessly, always remaining open and transparent.

I would like to thank each of them all for sharing their talent, hard work and boundless generosity.

The Commission needed access to a physical space, technological equipment and administrative support services in order to carry out its investigation, hold public and *in camera* hearings, and draft its reports. This was a considerable challenge given the constraints involved in using classified documents. The task was accomplished in large part thanks to the assistance of the Privy Council Office, which provided critical logistical support while respecting the Commission's independence. Public Services and Procurement Canada employees were very helpful in organizing the public hearings, which were held in the Library and Archives Canada building, while the *in camera* hearings were held in a secure location that the Courts Administration Service kindly made available to the Commission. Many more people provided administrative support during the hearings.

A special thanks to the interpreters who also worked tirelessly during the public hearings and facilitated multilingual consultation with various diaspora community members across Canada.

A small but hard-working team also provided translation services for classified documents. I also appreciate the dedicated teams who provided high-quality translation, editing and formatting services in a timely manner for the Commission's unclassified documents.

I would also like to thank the media, who made sure to report on the main aspects of our work, helping Canadians better understand the issue of foreign interference. I am also grateful for their patience and cooperation throughout the public hearings.

Lastly, I must mention the invaluable help we received from the public. The public's participation gave me a better understanding of how foreign interference affects people's lives. Many agreed to meet with me to share their experiences. Others spoke on panels, and several hundred took the time to provide the Commission with individual submissions.

I would like to extend my warmest thanks to these public participants. They have made a major contribution to the work we have been doing.

Table of Contents

Report Summary

Introduction

As Canadians we cherish our democracy, and rightly so. There are few things that so powerfully reflect our common values of human dignity, worth and freedom as our democratic institutions. This is not to say that our system is perfect. For many, it may seem far from it. But it is undeniable that one of the greatest accomplishments of our society is that we have developed a political and social order in which we are able to govern ourselves and live peacefully with each other. Furthermore, each and every citizen may participate in making choices about the path that we as a country choose to go down, together.

It is therefore not surprising that recent discussions about foreign interference in Canada's democratic institutions have caused so much concern. It is because we care about our democracy that so many have expressed fear, anger, disappointment and regret in response to claims that foreign states have acted to manipulate and undermine our democracy. These reactions are not just understandable, they are the necessary consequence of being a people that care about upholding our democratic values. As painful as these reactions have been, they are also a sign of our commitment to democracy, and by extension, a sign of our democracy's strength.

Our democracy is strong, but it is not invulnerable. The strength of our social and political institutions relies in large part on trust and confidence. Trust that our elected representatives and civil servants will work tirelessly for the good of the country. Confidence that our democratic institutions have the resources and resilience necessary to resist attempts by foreign states to undermine them. But trust and confidence can be fleeting. When fear of foreign interference begins to erode our trust and confidence, our democracy weakens.

Maintaining trust and confidence in our democratic institutions in the face of allegations of foreign interference can be challenging for many reasons. For one thing, some foreign states act intentionally to undermine our social cohesion. They spread disinformation, particularly by exploiting social media and stoking social divisions and thereby undermining public confidence and trust in democracy. Although these tactics have not been too successful yet, we must be vigilant.

Another challenge in maintaining trust and confidence comes from the culture of secrecy that surrounds the work that Canada does to detect, deter and counter foreign interference.

To protect the vital interests of Canada and our allies, the federal government keeps many things secret: the intelligence we collect about hostile foreign states; the actions that our national security and intelligence community takes in response; and some of the plans we develop for future action.

There are often very good reasons for this. Secrecy ensures that we can effectively collect information about foreign states and their proxies. It denies our adversaries information that they could exploit to undermine Canada's democracy. It can, in fact, help ensure that Canada remains a safe and open society.

But secrecy can also go too far. Even when justified, it presents challenges. In order to have confidence in our democratic institutions, Canadians need a realistic picture of the threats that we face from foreign states. To have trust in our government, Canadians need to know what our government is doing to protect against foreign interference. In other words, some secrecy is necessary to protect our ability to counter foreign interference, but too much secrecy harms the very institutions that we seek to protect. The balance is not an easy one to strike.

This Commission was created in part to navigate the difficult path between secrecy and transparency. One of my primary objectives as Commissioner has been to maximize what the public knows about foreign interference in Canada, without compromising the government's ability to continue to defend our democracy. I hope that issuing this report will itself be a tool to strengthen Canada's democracy by promoting trust and confidence through knowledge.

In the pages that follow, I summarize what I learned over the course of nearly a year and a half of intense work about the foreign interference threat Canada faces, and what is being done about it.

I have learned that the foreign interference threat is real. There are a number of foreign states who are actively working to secretly, and often illegally, meddle in our democratic institutions. They use a wide range of strategies and tactics, some of which are incredibly sophisticated.

But I have also learned that Canada has been resilient and that our democratic institutions have held up well against these threats so far. I have found no evidence that the overall result of any election has been swung by a foreign actor and have identified only a small number of individual ridings where foreign interference may have had some impact. I did not see any evidence of federal legislation, regulation or policy being adopted or abandoned as a result of a foreign state's interference. And importantly, I have found no evidence that there are "traitors" in our Parliament who are conspiring with foreign states against Canada.

I do not say any of this to minimize the threat of foreign interference. That threat is all too real. There are examples of potentially troubling interactions between some parliamentarians and foreign actors. There is information that suggests foreign states are using a wide range of methods to influence our democratic processes, from co-opting domestic associations to evading election finance rules. There is good reason to believe that foreign states attempt to manipulate the domestic online information environment in ways that are difficult to detect and harmful in their impact. The danger of foreign interference is real, and it is a threat that extends beyond electoral processes and democratic institutions to areas that were not the focus of my mandate, such as threats to critical infrastructure, research security and, of course, transnational repression.

But the extent to which foreign interference has succeeded in permeating our democratic processes and institutions should not be overblown.

In the course of my work, I have also learned of the many activities by actors both within and outside of the federal government to respond to foreign interference. I have been deeply impressed by the dedication, competence and responsibility of many members of the public service who have worked tirelessly to defend our democracy. Their efforts have gone a long way to protecting the democratic institutions and values that we as Canadians hold so dear.

That said, the efforts of government have not been perfect.

An essential part of building trust and confidence in our institutions is being honest about their failures and shortcomings. I could not fulfill my mandate to help build public confidence in our democratic institutions if I minimized the ways in which efforts have come up short.

At times, I have found that the government reacted slowly in the face of situations that required more rapid action. At times, I have found that information has not flowed properly to policymakers and decision-makers, was not adequately tracked or may not have been properly appreciated by those who received it. I have found that coordination of efforts has been a challenge, and there has been some confusion about roles and accountabilities. And I have found that while the government has done many good things to protect our democracy, it has been bad at effectively communicating this to the public.

But I have also found that the government's work is continuing, and that genuine efforts are being undertaken to improve in areas that need it. The measures taken in the past 30 months speak for themselves. There is much more work to be done, and I hope that the recommendations in this report will help to further advance our response to foreign interference.

However, on the whole, I am satisfied that the government now appreciates the foreign interference threat that Canada faces and is serious about responding to it.

Government efforts alone, however, are not enough to protect Canada's democracy. One of the defining features of our democratic institutions is that they belong to each and every one of us. And so, we all have a role to play in defending them.

An effective response to foreign interference demands a whole-of-society response, not just a whole-of-government response. It requires governments at every level within Canada to work with each other. It requires civil society and the private sector to collaborate with government and democratic institutions. It requires government, schools and communities to equip every Canadian with the tools they need to navigate a complex information ecosystem. And it requires every Canadian to commit to engaging in democratic discourse in good faith. It requires citizens to believe in one another, and to believe in our democracy.

Achieving a whole-of-society response to foreign interference is challenging. But our democracy is strong, and we as Canadians are strong enough to defend it.

Foreign interference – and our fear of foreign interference – has taken its toll. For some, their faith in our system has been challenged. I hope that for those who take the time to read this report, what they learn – what I have learned – will not only enhance their understanding of the foreign interference threat but also go some distance in rebuilding their confidence and trust in our democracy.

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.*

Chapter 1: How the Foreign Interference Commission Came About

The events leading to the creation of the Commission are important to understand the Commission's scope, objectives and guiding principles.

Rising awareness of foreign interference

The notion that foreign states or non-state entities are attempting to interfere in Canadian democratic life and institutions is not new. What is relatively new is the rise of public awareness of this issue and the rapidly evolving technical means of interference.

In the last 10 years or so, Canadian security and intelligence agencies have become increasingly concerned about foreign interference. They have issued public reports highlighting how the scale, speed, range and impact of foreign interference have grown because of the Internet, especially social media platforms, and the availability of cheaper and more accessible cyber tools. Online disinformation campaigns are used to amplify social differences, create conflict and undermine confidence in governmental institutions. In sum, these reports show that the foreign interference threat is real and growing.

Government adopts some measures

In the wake of reported foreign interference in elections in the United States and France in 2016 and 2017, the government took measures to address foreign interference with Canada's democratic institutions. These measures include:

- June 2018: Canada leads the G7[1] in establishing the Rapid Response Mechanism, which aims to prevent, thwart and respond to malign and evolving threats to G7 democracies.

[1] The Group of Seven, or G7, is an informal grouping of Canada, France, Germany, Italy, Japan, the United Kingdom and the United States. The European Union is also represented.

- December 2018: Parliament amends the *Canada Elections Act* to address foreign interference by creating new offences and modifying existing ones.
- January 2019: the government implements the Plan to Protect Canada's Democracy, which includes mechanisms to assess federal elections and communicate with Canadians if one or several incidents threaten the integrity of a federal election.
- 2019: the government creates a Cyber Attribution Framework used to determine if identified cyber activities can be attributed to a foreign actor.

2023 becomes a pivotal year

The beginning of 2023 saw a sharp increase in media reports about possible interference by the People's Republic of China ("**PRC**") in Canadian elections, including leaks of information reported to be government intelligence.

On March 15, the government appointed an "Independent Special Rapporteur on Foreign Interference" ("**ISR**") to assess the extent and impact of foreign interference in Canada's electoral processes, including the 2019 and 2021 elections, and to consider innovations and improvements in public agencies to counter it.

On May 23, the ISR issued his initial report concluding that foreign governments are attempting to influence Canadian candidates and voters and that these efforts are omnipresent, especially from the PRC, but that there was no reason to question the validity of the 2019 or 2021 elections.

The ISR announced plans to hold public hearings with diaspora communities and other Canadians, government officials, experts and additional interested parties about foreign interference.

However, a majority of Canadians believed that a commission of inquiry was needed despite the ISR's work. Opposition parties and diaspora groups also called for a public inquiry. Media reports on foreign interference continued steadily.

On June 9, the ISR resigned.

On September 7, the government created the Commission. All four recognized political parties agreed on the Terms of Reference and the appointment of the Commissioner.

The next section reviews developments that occurred in 2023 and 2024, after the Commission published its Initial Report on 3 May 2024.

Chapter 2: Developments After the Commission's Initial Report

In 2023 and 2024, several reviews, investigations and processes relevant to foreign interference occurred in parallel with the Commission's work:

- The Office of the Commissioner of Canada Elections reviewed allegations of foreign interference in the 2019 and 2021 general elections. It closed all but one file for lack of evidence of contraventions to the *Canada Elections Act*. The file still open at the time of the Commission's public hearings concerns allegations of interference in the 2019 federal election by the PRC Consulate in the Greater Toronto Area.[2]
- The House of Commons Standing Committee on Procedure and House Affairs ("**PROC**") investigated a cyber campaign by an entity called APT 31 allegedly affiliated with the PRC. In 2021, the APT 31 campaign targeted political officials around the world, including 18 Canadian members of Parliament. The Committee has not yet issued its report.[3]
- The National Security and Intelligence Review Agency ("**NSIRA**") reviewed the flow of intelligence within government about PRC foreign interference in federal democratic institutions and processes from 2018 to 2023. It issued its report in May 2024.[4]
- The National Security and Intelligence Committee of Parliamentarians ("**NSICOP**") reviewed foreign interference in Canada's democratic processes and institutions. It issued its report in June 2024, and its conclusions include that Canada is a target of pervasive and sustained foreign interference activities aimed at democratic processes and institutions and has been slow to respond. It also concluded that it had seen troubling intelligence that some parliamentarians are "semi-witting or witting" participants in foreign state efforts to interfere in Canadian politics.[5]
- The *Countering Foreign Interference Act* (introduced as Bill C-70) received Royal Assent in June 2024. The Act makes changes to Canada's national security architecture and establishes the legislative scheme for a Foreign Influence Transparency Registry.[6]

---

2 These allegations are discussed in more detail in Volume 2, Chapters 7 and 9.
3 I discuss the APT 31 campaign in Volume 4, Chapter 15.
4 I discuss relevant findings from the May 2024 NSIRA report in Volume 4, Chapter 14.
5 I discuss the June 2024 NSICOP Report in more detail in Volume 4, Chapters 14 and 18.
6 I discuss the *Countering Foreign Interference Act* in more detail in Volume 4, Chapter 14.

- Government introduced Bill C-65, which proposes amendments to the *Canada Elections Act*, including new prohibitions relating to foreign interference in the electoral process. With the prorogation of Parliament in January 2025, Bill C-65 died on the Order Paper.[7]

Where relevant to the Commission's investigation, I consider the above reviews and legislation in Volumes 3 and 4 of this report.

Bloc Québécois motion to expand the Commission's mandate

On 11 June 2024, in response to the 2024 report of NSICOP, the House of Commons adopted a motion from the Bloc Québécois asking the Government to expand the Commission's mandate to investigate federal democratic institutions, including members of Parliament and senators who may be working in the interests of foreign powers.

On 17 June 2024, I agreed to investigate this under the Commission's existing mandate and framework.

I now turn to a summary of the Commission's mandate and related important concepts.

Chapter 3: The Commission's Mandate and Key Concepts

Terms of Reference and guiding principles

Under the Commission's Terms of Reference, I had to examine and assess the potential impacts of foreign interference on the 2019 and 2021 general elections (Clause A of the Terms of Reference) and the flow of information within the federal government before, during and after those elections and actions taken in response (Clause B).

I also had to look at the government's capacity to detect, deter and counter foreign interference targeting Canada's democratic processes (Clause C) and make recommendations on how the government can better protect federal democratic processes from foreign interference (Clause E).

[7] I discuss Bill C-65 in Volume 4, Chapter 15.

The Commission worked to fulfil the above aspects of its mandate while also fostering transparency and enhancing public awareness and understanding about the challenge of disclosing classified national security information (Clause D). I believe we have shown that it is possible to publish some sensitive information without impacting national security. However, there was still evidently information revealed during the investigation that I could not put in this report for national security reasons. This information is in a classified supplement.

In fulfilling my mandate, I was guided by five principles:

- proportionality
- transparency
- fairness
- thoroughness
- expeditiousness.

Fairness explains why I have chosen not to name people, entities or groups who would not have had a meaningful opportunity to defend themselves.

Interpretation of key terms

To fulfil my mandate, I had to interpret several key concepts in the Commission's Terms of Reference.

"Democratic institutions" and "democratic processes" are both mentioned. Considering the Commission's Terms of Reference as a whole and the fact that the federal government's use of the term "democratic institutions" expressly includes Parliament, the division of powers and the formation of government, I conclude that my mandate with respect to democratic institutions and processes was to investigate potential foreign interference with the federal election process (including the electoral system and political party processes), executive decision-making by Cabinet and its ministers in relation to their departments and, finally, law-making by Parliament.

The term "foreign interference" means different things in different contexts. In this report, I use the term to mean a 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. This covers traditional means of interference, such as direct, person-to-person activities as well as digital forms.

For the Commission's purposes, "acting on a state's behalf" means acting at the direction of a foreign state to benefit the interests of that state.

Four key observations about foreign interference

Foreign interference is not new but is evolving. Democracies have always been confronted with foreign interference, but actors, targets and methods change as the global balance of power shifts and technologies evolve. Even in the brief time between the 2019 and 2021 elections, there were significant changes to the online landscape. This rapid evolution is likely to continue.

Foreign interference happens whether or not an election is taking place. Activities targeting elections may occur months, or even years, before an election period begins.

Adherence to democratic values and the protection of fundamental rights can complicate Canada's response to foreign interference:

- The right to freedom of expression allows Canadians to express views that favour foreign states and so government officials may not respond unless they can be sure of a foreign link.
- The right to privacy may limit the tools the government can use to detect foreign interference.
- The right to a fair trial may hinder the enforcement of laws against foreign interference because in many cases the evidence derives from intelligence that cannot be used in criminal proceedings and still provide a fair trial.
- Any intervention by non-partisan public servants in response to foreign interference could be seen as favouring one party over another, thus undermining confidence in the democratic system. As a result, public servants may tend to set the bar for intervention very high.

There is a grey area between foreign influence and foreign interference. Some actions are clearly illegitimate foreign interference, and some are clearly legitimate state activities. Foreign state actions may, however, fall somewhere in between these two endpoints.

Transnational repression

One of the more troubling ways in which countries carry out foreign interference in Canada is through transnational repression. They target Canadian diaspora communities and attempt to influence voting, silence dissent, amplify preferred state narratives, control public opinion and sow discord.

Transnational repression may impact democratic institutions if it discourages diaspora communities from participating in our democratic processes, such as elections, and undermines people's trust in Canadian democracy.

Chapter 4: Balancing Transparency and National Security Confidentiality

I held public hearings in early 2024 to identify the challenges, limitations and potential adverse impacts associated with disclosing classified national security information and intelligence to the public. Chapters 4 and 5 are in large part informed by this information, which was fundamental to the Commission's work.

Several administrative and legislative standards govern the way in which sensitive information is handled and the conditions under which it may be disclosed. These standards set out a sophisticated system for protecting and classifying information, which complicates transparency. They may, for example, require the redaction of information from documents or the holding of hearings that are not open to the public or participants (called "*in camera*" hearings).

In my view, national security confidentiality did not affect my ability to seek out the truth, even if it presented real challenges in maintaining open and transparent processes and reports.

The Commission was given access to all relevant documents without redactions for national security confidentiality.[8] These documents contained a wealth of information about possible foreign interference into Canada's democratic institutions, including electoral processes, as well as measures taken by the government to detect, deter and counter such threats.

They also contained information about highly sensitive methods of collection, or information that would be particularly harmful to individuals or to Canada's national security interests, if disclosed.

The challenge was to find ways to make public as much information and as many documents as possible, in an extremely limited time frame. Most commissions of inquiry encounter little if any classified information. In our case, approximately 80% of the documents produced by the Government of Canada were classified.

The Commission took a pragmatic approach to this challenge, focusing on priority documents and negotiating with the government to determine what information had to be redacted from the documents or, depending on the situation, to find an acceptable way to summarize sensitive information. In all cases, the Commission required the government to justify the need for redaction.

[8] Except for a small number of documents that were redacted to protect Cabinet confidences, solicitor-client privilege and personal information.

The Commission also required justifications for the government's requests to hold hearings *in camera*.

This approach carefully balanced the public interest in transparency with the need to protect national security confidentiality.

In addition to national security, two considerations presented a challenge in maximizing transparency. I had to protect the legitimate interests of individuals who feared for their safety and could not disclose to participants, or the public, information that would compromise ongoing investigations.

Regarding the former, when a witness established that protective measures were required, I ordered appropriate measures. In two cases, I permitted witnesses to provide evidence by way of sealed affidavits. A summary of *in camera* testimony and sealed affidavits has been made public without identifying the witnesses.

Overall, I am satisfied with the outcome because, while taking the necessary precautions, we have been able to disclose an unprecedented amount of information about Canada's highly sensitive national security topics.

Next, I explain the nature of intelligence and the challenges arising from it that are relevant to the Commission's work.

Chapter 5: Introduction to Intelligence Concepts and Related Challenges

Intelligence has inherent limits and weaknesses, and it must be approached with caution. It can be very useful or even critical, but it can also be unreliable, incomplete or simply wrong. Thus, intelligence should not always be understood as being true and reflective of reality. Particular caution is needed when relying on intelligence to take measures that will negatively impact someone.

Given how central intelligence was to the Commission's work, a realistic understanding of intelligence provides critical context for the evidence I heard. Knowing both the strengths and the limitations of intelligence is critical for assessing how Canada has responded to foreign interference.

What intelligence is

Intelligence has no universally accepted definition. It is generally understood as information that has been collected, processed and narrowed to meet the needs of policy or decision-makers.

The categories of intelligence relevant to the Commission's work are:

- **Foreign intelligence:** relates to what foreign individuals, states, organizations or terrorist groups do, can do or intend to do in relation to international affairs, national defence or national security.
- **Security intelligence:** relates to threats to Canada's national security caused by espionage and sabotage, foreign interference and influence, terrorism, subversion and violent extremism.
- **Criminal intelligence:** relates to investigations into criminal offences, which can include some of the threats listed above, like terrorism and violent extremism.

Intelligence is the product of a sophisticated process in which information is requested, collected, analyzed and provided to policymakers and decision-makers. This process is often called the "intelligence cycle," which typically has several phases:

- **Priorities and direction.** Policymakers and decision-makers express their needs to the intelligence community, reflecting the government's policy priorities.
- **Planning.** Intelligence agencies determine how to meet the government's intelligence priorities.
- **Collection, processing and exploitation.** Intelligence agencies collect information using different methods and sources. If necessary, information is converted, translated or synthesized so it can be analyzed.
- **Analysis and production.** Intelligence analysts add context and integrate the information into reports and other intelligence products. Those products can include an assessment of the subject and its potential policy impacts.
- **Dissemination.** Finished intelligence products are shared with government policymakers and decision-makers or other officials.
- **Feedback.** Policymakers and decision-makers evaluate the intelligence, give feedback on whether it meets their requirements and suggest adjustments or improvements.

Intelligence is collected in various ways depending on the collector's capabilities, the nature of the issue, available tools and what is allowed by law. Some categories are:

- **Human Source Intelligence (HUMINT).** Information collected from human sources like a confidential informer.
- **Signals Intelligence (SIGINT).** Information collected by accessing signals between people, between machines (e.g. emails) or a combination of both.
- **Open Source Intelligence (OSINT).** Publicly available information, including traditional and social media, public records (e.g. business records), academic journals, professional resources, commercial databases or websites.

The limitations of intelligence

While intelligence is important, it has inherent limitations. Just because intelligence says something does not mean it is true, accurate or complete.

The reliability of intelligence may vary from source to source. For example, the report of a witness to an event may be unreliable if the witness did not have a good opportunity to see the event, or if it occurred quickly. Wiretaps of communications can reliably convey the exact words spoken but their meaning may be unclear.

The credibility of sources can also be a concern. Sources may, for example, attempt to intentionally mislead their audience.

Moreover, intelligence reports are often based on combining different sources of intelligence, which are pieced together to try to convey a larger picture. Each piece may have a different degree of reliability and credibility, which can make it challenging to appreciate the overall strength of a report.

Information may be incomplete or insufficient, and may also be translated from a different language, losing some of its precision, meaning and nuance.

The challenges of acting on intelligence

Intelligence is collected to help guide policy and decisions. Sometimes, intelligence can help decision-makers address particular issues. But using intelligence comes with a major challenge, which is determining if it is reliable and credible.

Further, even if intelligence is sufficiently credible and reliable to act upon, other challenges can remain. By acting on intelligence, Canada might alert foreign actors that it knows something they wish to keep secret. In turn, this can expose how Canada obtained the information and the means it used to get it. Additionally, much of Canada's intelligence comes from its foreign allies and failing to protect their sources and methods could make them hesitate to share intelligence in the future.

Protecting sources and methods is crucial for Canada to keep gathering intelligence. Without this, Canada may lose out on critical intelligence in the future.

Using intelligence in legal proceedings presents challenges

Challenges also arise when government actions based on intelligence lead to legal proceedings. Because of specific rules and procedures in these proceedings, many of which are designed to protect the rights of individuals, intelligence may not be admissible as evidence. This is known as the "intelligence-to-evidence" or "intelligence as evidence" challenge.

Intelligence is subject to disclosure

In Canada, a person charged with a crime has a constitutional right to "disclosure." This means the prosecution must provide them with all the information in its possession relating to the investigation unless it is clearly irrelevant or privileged. Thus, any relevant intelligence an agency shares with law enforcement must generally be disclosed to the accused person if charges are laid, even if the prosecution does not intend to use it. This could make the intelligence public and risk revealing intelligence capabilities, methods, sources or targets for investigation.

Further, in legal proceedings reviewing government actions, the person seeking review generally has a right to obtain some information from the government. This means sensitive intelligence may need to be disclosed, which could risk revealing classified information.

Intelligence may not be admissible as evidence

An additional challenge with using intelligence as evidence is that it may not be admissible in a legal proceeding because of the rules of evidence.

Using intelligence to make a decision that impacts someone may be unfair

Decision-makers must be cautious when using intelligence to decide issues that will directly impact a person's reputation, livelihood or rights. Courts have rules of evidence to ensure decisions are made on information that is credible and reliable. As explained above, intelligence may not satisfy these requirements.

Despite the challenges, intelligence remains valuable. Quality intelligence can be key in informing policymaking and decision-making and responding to threats like foreign interference. It can also offer valuable tips and leads for the police to follow up and potentially gather evidence with.

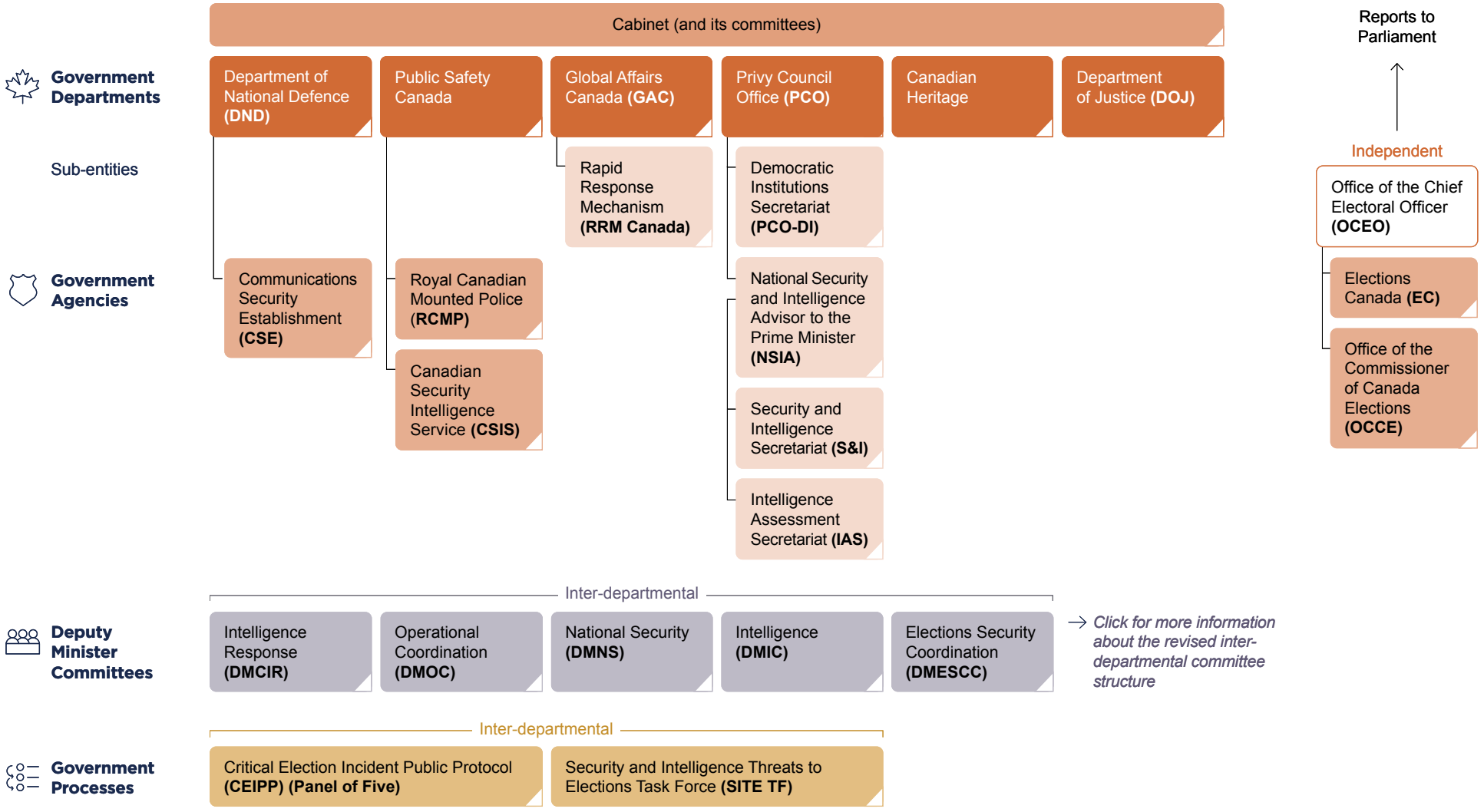
The next section describes in graphic form the primary federal entities responsible for responding to foreign interference.

Chapter 6: Federal Entities Involved in Responding to Foreign Interference

In Canada, a number of government agencies, departments, other federal entities and offices are involved in detecting, deterring and countering foreign interference. Each has a specific mandate.

The next page provides a visualization of many of the entities discussed in the report.

Main Federal Entities Involved in Responding to Foreign Interference



Chapter 7: The 2019 General Election

The Commission's investigation identified a number of alleged incidents of foreign interference in the 2019 general election.

Much of the intelligence at issue cannot be publicly disclosed or may only be disclosed in summary form. Furthermore, much of the intelligence is uncorroborated and of unknown or uncertain reliability. The Commission did not have the mandate or the capacity to verify or test the contents of the intelligence. It should not be taken as proven fact.

The Liberal Party of Canada nomination contest in Don Valley North

Canada has intelligence indicating that irregularities in the Liberal Party of Canada ("**Liberal Party**") nomination contest in Don Valley North ("**DVN**") may have included activities undertaken by individuals close to People's Republic of China (PRC) officials. This information originated from a variety of sources with various levels of corroboration.

Before the 2019 election, intelligence reporting, though not firmly substantiated, indicated that buses were used to bring international students of Asian origin to the nomination process in support of a candidate for the nomination, Han Dong, and that individuals associated with a known PRC proxy agent provided them with falsified documents to allow them to vote, despite not being residents of DVN. There were allegations that the students were told by PRC officials in Canada to support Mr. Dong if they wanted to maintain their student visas.

Mr. Dong denies any involvement in these matters.

The Canadian Security Intelligence Service ("**CSIS**") reported the intelligence that it had at the time to the Panel of Five (or "**Panel**"). The Panel of Five is part of the Critical Election Incident Public Protocol ("**CEIPP**"). It is made up of five senior public servants who may communicate with Canadians if one or several incidents threaten the integrity of a federal election.[9]

CSIS also told the Panel that election authorities were informed. The Panel indicated that the Liberal Party should be told, and CSIS then briefed security-cleared Liberal Party representatives.

[9] The Panel's members are the: 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 and Deputy Minister of Foreign Affairs.

The Panel of Five ultimately concluded that the CEIPP threshold to make an announcement was not met.

Liberal Party representatives told Jeremy Broadhurst, the National Campaign Director of the Liberal Party, about the allegations of busing. Mr. Broadhurst brought this information to the attention of Prime Minister Justin Trudeau in his capacity as Liberal Party leader.

Mr. Trudeau did not feel there was sufficient or sufficiently credible information to justify removing Mr. Dong but considered that the matter might need revisiting after the election.

After the 2019 election, the Prime Minister's Office ("**PMO**") requested, and received, a briefing from senior officials about the reported irregularities. The Prime Minister and the PMO received additional briefings about Mr. Dong.

Mr. Dong stepped aside from the Liberal Party caucus following media reporting allegedly based on leaked information related to his interactions with PRC officials and his communications respecting the detention of Michael Kovrig and Michael Spavor.

According to a government summary of intelligence relating to Mr. Dong that was made public, Mr. Dong would have expressed the view that even if Mr. Kovrig and Mr. Spavor were released at that moment, it would be viewed by opposition parties as an affirmation of the effectiveness of a hardline Canadian approach.

Mr. Dong testified that he was not sure what was meant by that, did not remember saying anything like that and added that he consistently advocated for the release of both men.

All Mr. Dong's conversations with PRC consular officials took place in Mandarin. The public summary is thus based on a summarized report written in English of a conversation that took place in a different language. It is not a transcript of a conversation.

Precision and nuance can be lost in translation. Based on the information available to me, I cannot assess the accuracy of the public summary, but I can say that the classified information corroborates Mr. Dong's denial of the allegation that he suggested the PRC should hold off releasing Mr. Kovrig and Mr. Spavor. He did not suggest that the PRC extend their detention.

The Commission's mandate is not to determine what actually took place at the DVN nomination meeting in 2019. However, this incident makes it clear that nomination contests may be gateways for foreign states that wish to interfere in our democratic processes.

The PRC's alleged support of Mr. Dong's nomination bid, including by a proxy agent, is included in the list of major instances of suspected foreign interference targeting Canada's democratic processes produced by the government at the request of the Commission. I return to this list in Volume 3, Chapter 10.

Other allegations and incidents

Several other incidents that allegedly occurred during the 2019 election were discussed during the hearings. The most significant are discussed below.

There is intelligence indicating that in the Vancouver area some PRC officials coordinated the exclusion of some political candidates, perceived as anti-China, from attending local community events related to the election.

There is also intelligence suggesting that before and during the 2019 general election, a group of both known and suspected PRC threat actors in Canada worked in loose coordination to engage in foreign interference. Eleven political candidates (seven Liberal Party and four Conservative Party of Canada) and 13 political staff members were "implicated," meaning they either had a connection with these threat actors or were directly affected by their activities. "Implicated" does not mean that these individuals were knowingly involved or complicit in foreign interference activities. Some of the threat actors may also have received financial support from the PRC, though there is no indication that any candidates did.

The Panel of Five was informed about these allegations of financial support from the PRC. The Panel decided not to make a public announcement because, in its view, there was substantial ambiguity and lack of clarity as to the intent and purpose behind financial support.

The Commission's investigation also revealed that CSIS implemented a threat reduction measure ("**TRM**") to reduce a threat in relation to Pakistan, which had attempted to clandestinely influence Canadian federal politics. The TRM was assessed to have effectively reduced the threat of interference.

There were some discussions in relation to negative articles about Prime Minister Trudeau on a website called the Buffalo Chronicle. Certain mainstream sources in Canada amplified these articles, but others debunked them. The Panel of Five concluded that the media ecosystem had cleansed itself. Facebook ultimately removed the article following discussion with Privy Council Office ("**PCO**") officials.

Media Ecosystem Observatory monitoring for disinformation

In the lead up to and during the 2019 general election, the Media Ecosystem Observatory ("**MEO**"), a joint project between McGill University and the University of Toronto, monitored the digital media ecosystem in Canada.

The MEO found that misinformation and disinformation did not play a major role in the 2019 election or impact its outcome. It did not appear coordinated and had limited impact on the information ecosystem. The MEO concluded that the Canadian political information ecosystem during the 2019 election was likely more resilient than that of other countries such as the United States.

Chapter 8: The 2021 General Election

There were several alleged incidents of foreign interference during the 2021 general election, including:

- disinformation targeting the Conservative Party of Canada ("**Conservative Party**"), its leader Erin O'Toole, and one of its British Columbian candidates Kenny Chiu
- events in the Vancouver riding of New Democratic Party ("**NDP**") Member of Parliament ("**MP**") Jenny Kwan
- potential interference activity by India and Russia.

Security and Intelligence Threats to Elections Task Force (SITE TF) briefings to security-cleared political party representatives

The Security and Intelligence Threats to Elections Task Force ("**SITE TF**") provided Secret-level briefings to security-cleared political party representatives during the 2021 elections, as it did for the 2019 election.

The evidence reveals a gulf between the political parties' expectations and what the SITE TF was able to provide to them. Party representatives felt they were not sufficiently informed by the SITE TF, and even said that they were unduly reassured by what they heard, causing them to lower their guard.

Disinformation targeting the Conservative Party and Mr. O'Toole

During the 2021 election period, the Conservative Party and its then leader, Mr. O'Toole, were the subject of inaccurate reports that circulated widely on Chinese language media outlets that are known to have, or may have, ties to the PRC or the Chinese Communist Party ("**CCP**"). The reports stated that Mr. O'Toole would ban the social media platform WeChat, that he was the "Canadian version of Trump" and that he almost wanted to break diplomatic relations with the PRC.

Mr. O'Toole believes he and his party were targeted due to positions that they had taken that were critical of the PRC.

A false narrative about Mr. Chiu and the foreign influence registry

In 2021, Mr. Chiu, the Conservative Party MP for Steveston-Richmond East, was the target of false narratives related to his proposal to implement a foreign influence registry. Reports claimed that any individual or group with ties to the PRC would be considered a spokesperson and would need to register.

Canadian intelligence holdings identified the media spreading these false narratives as having close links to the PRC government or PRC state media.

Mr. Chiu attempted to respond to this narrative in the media, but his messaging was not picked up or circulated by Chinese language outlets. Mr. Chiu said that he was shunned by Chinese language media.

He reported these issues to the Conservative Party central campaign and to CSIS. He did not hear from CSIS again until he received a briefing from them in the fall of 2023, following media reporting about alleged leaks of CSIS intelligence reports.

Office of the Commissioner of Canada Elections review of foreign interference allegations from the 2021 general election in Greater Vancouver

During the 2021 general election, the Office of the Commissioner of Canada Elections ("**OCCE**") received complaints alleging foreign interference. The OCCE initiated a review into certain of these allegations, focusing on electoral districts in the Vancouver area and the unsuccessful campaign of Mr. Chiu. The aim of the review was to determine whether there was sufficient evidence to conduct a fuller investigation into possible contraventions of the *Canada Elections Act*.

Although information received during the review led to suspicions that attempts to influence the Chinese Canadian community existed, the OCCE did not obtain sufficient evidence to support any of the elements of undue foreign influence or other contraventions of the Act.

Investigators did, however, find indications that PRC officials gave impetus and direction to an anti-Conservative Party campaign, which was then carried out and amplified by an array of associations and individuals using various communication channels.

Canadian government agencies were aware of these online narratives, and this was conveyed to the Panel of Five by the SITE TF. The Panel noted the difficulty of attributing this activity to foreign actors and, furthermore, was not inclined to intervene because the agencies could not distinguish this activity from ordinary political debate that occurs during an election. Even falsehoods

can be a legitimate exercise of freedom of expression during an election, as long as they are not state sponsored or amplified.

The Panel's conclusion was also informed by its impression that the media ecosystem had cleansed itself: Mr. Chiu made public statements responding to the online narratives, and narratives concerning Mr. O'Toole lost traction well before election day.

I am not convinced by the idea of a self-cleansing media ecosystem. By the time disinformation fades away, it may often be too late. The damage to the democratic process or to those targeted may already be done.

After the election, the Conservative Party campaign sent government officials a package with material documenting their concerns. The SITE TF's conclusions remained unchanged, though they underlined that they observed indicators of potential coordination between various Canada-based Chinese language news outlets as well as PRC and CCP news outlets. These conclusions highlight the inherent challenges in attribution.

The SITE TF's analysis is consistent with the Media Ecosystem Observatory's (MEO's) conclusions about the 2021 election.

The MEO found that PRC officials and state media commented on the election with an apparent aim to convince Chinese Canadians to vote against the Conservative Party and Mr. O'Toole, and that there was misleading information circulating on Chinese language social media platforms about Mr. Chiu. While the MEO did not find evidence that this activity had a significant impact on the overall election, it could not discount the possibility that riding-level contests could have been affected.

In light of this additional evidence, I remain satisfied that the Panel of Five's determination that the online activities observed did not meet the threshold for a public announcement was reasonable at the time it was made. However, this situation highlights a serious gap in the mechanisms available to address misinformation or suspected disinformation during the election period. It does not help that there are no clear guidelines for when government will act short of a public announcement by the Panel. These issues need to be addressed.

Suspected foreign interference in the Vancouver East electoral contest

There was also concern about foreign interference in the Vancouver East electoral contest involving Ms. Kwan, the NDP MP for that riding. Ms. Kwan believes that taking positions critical of the PRC resulted in her being targeted for foreign interference.

Since 2019, she has ceased being invited to certain key events organized by Chinese Canadian community organizations to which she was invited in the past. She also observed her constituents being more fearful of voting for her because of concerns about the safety of their families in the PRC.

Intelligence holdings indicate that the PRC worked to exclude particular political candidates from public events in 2019, and that this strategy continued in 2021.

Ms. Kwan also raised concerns about a prominent member of the Chinese Canadian community in Vancouver hosting a free lunch in support of her Liberal Party opponent. The NDP filed a complaint with the Office of the Commissioner of Canada Elections (OCCE) alleging a violation of third party election rules. The OCCE concluded that there was no violation but imposed an administrative monetary penalty to the Liberal Party campaign for not reporting the lunch as a contribution.

Ms. Kwan also reported the lunch to the Royal Canadian Mounted Police ("**RCMP**") and CSIS but, in her opinion, none of them seemed interested in the issue.

In two reports, the SITE TF noted this incident and the allegations that organizers had connections with the PRC.

Suspected foreign interference by India

Intelligence holdings indicate that India may have attempted to clandestinely provide financial support to preferred candidates during the 2021 election without the candidates' knowledge. I have not identified any shortcomings with respect to information flow or the government's response to this issue.

Suspected Russian disinformation activity

As for Russia, the Panel did not receive any evidence of a concerted Russian disinformation campaign during the 2021 election.

The MEO did not detect evidence of Russian interference either. However, it did not monitor Russian language social media posts or platforms, and thus could not exclude the possibility of a low-level Russian influence campaign.

Having described in brief the evidence relating to the 2019 and 2021 elections, I now explain my conclusions about the impacts of foreign interference on them.

Chapter 9: Assessing the Impacts on the 2019 and 2021 General Elections

Foreign interference is an ever-present reality in Canada and around the world. There is ample evidence that some countries engaged in foreign interference in the 2019 and 2021 general elections.

Did foreign interference undermine the integrity of the electoral system itself?

The answer is no. Our electoral system is robust and both elections were administered with integrity at the national and individual riding levels. Voters were able to cast their ballots, and to have their votes faithfully recorded.

Did foreign interference impact which party came into power in 2019 or 2021?

No, it did not.

Attempting to measure the impact of foreign interference on an electoral outcome is inherently difficult. It is generally impossible to draw a straight line between a particular incident and the outcome of an election, just as it is to assess how the varied, often subtle, foreign activities impacted the final seat count in the House of Commons.

However, I am confident that the Liberal Party would have formed the government with or without foreign interference in 2019 and 2021.

The Conservative Party shares my conclusions. Party representatives acknowledged to the Commission that foreign interference did not keep the Conservative Party out of power.

Did foreign interference impact any election results at a riding level?

This is a more difficult question to answer. It is possible that results in a small number of ridings were affected, but this cannot be said with certainty.

What can be said is that the number of ridings at issue is relatively small, and the ultimate effect of foreign interference on them remains uncertain.

Votes are secret in Canada. It is therefore not possible to directly link the misleading media narratives mentioned earlier with how any given voter cast their ballot. Furthermore, even assuming that some votes were changed as a result of these narratives, there is no way to know whether they were enough to affect the result.

Therefore, there is a reasonable possibility that the false narratives could have impacted the results in this riding, but I cannot go further. It shows, however, how important it is to combat disinformation.

Did foreign interference nevertheless impact the broader electoral ecosystem?

Yes, it did. Regardless of impact on specific election results, all foreign interference impacts the right of Canadians to have their democratic institutions, including electoral processes, free from covert influence, and their right to vote freely and in an informed manner.

Foreign interference has an impact when there is a single instance in which a ballot is cast in a certain way, or not cast at all, because of a foreign state's direct or indirect enticement. Foreign interference that discourages political engagement and discourse is harmful to Canadian democratic processes.

This impact has likely been slight to date but may become more severe in the future.

Did foreign interference undermine public confidence in Canadian democracy?

Regrettably, the answer is yes. This is perhaps the greatest harm Canada has suffered because of foreign interference and the public attention that it has now received. Undermining faith in democracy and government is a primary aim of many of the states that engage in foreign interference.

Much of the impact was caused by what came to light initially through the media, which did not offer a full and accurate picture of the phenomenon. That said, one cannot blame the media since they worked with what they had. However, they had only incomplete pieces of information.

The government must reestablish trust by informing the public of the threat of foreign interference, and by taking real and concrete steps to detect, deter and counter it.

Does foreign interference impact everyone equally?

It does not. The means and methods of foreign interference harm Canadians from diaspora communities in distinct ways. This includes those that are directly involved in our democratic institutions as candidates or members of Parliament (MPs). Their experiences must not be ignored, and specific attention should be given to them.

Without careful attention to the unique experiences of Canadians from diaspora communities, any understanding of foreign interference will necessarily be incomplete. Similarly, any responses to foreign interference need to be informed by the distinct ways that Canadians from different backgrounds are impacted by foreign interference.

Chapter 10: The Foreign Interference Threat

Before I review the evidence and my findings in relation to Clauses C and D of my mandate, it is first necessary to understand the nature of the threat of foreign interference in Canada's democratic institutions and processes.

Foreign interference has many aspects, but the Commission's Terms of Reference set the scope of my inquiry. My mandate is to focus on foreign interference 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.

Threat actors targeting Canada

People's Republic of China (PRC)

At the time of writing this report, the People's Republic of China (PRC) is the most active perpetrator of foreign interference targeting Canada's democratic institutions. The PRC views Canada as a high-priority target.

After the arbitrary detention of Michael Spavor and Michael Kovrig, Canada's diplomatic relations with the PRC changed dramatically. However, the PRC is also inescapably an important actor on the global stage. Since the release of both men in 2021, Canada and the PRC have been attempting to come to terms with their damaged relationship.

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": it supports those it believes helpful to its interests at the time, and those it believes are likely to have power, no matter their political party.

The PRC uses a wide range of actors for foreign interference. Both its 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 Chinese Communist Party (CCP), tries to control and influence Chinese diaspora communities, shape international opinions and influence politicians to support PRC policies.

The PRC relies on proxies, individuals or organizations, taking explicit or implicit direction from it to engage in foreign interference.

The PRC poses the most sophisticated and active cyber threat to Canada and CSIS assesses it as increasingly using social media and the Internet for disinformation campaigns involving elections.

India

India is the second most active country engaging in electoral foreign interference in Canada.

Like the PRC, India is a critical actor on the world stage. Canada and India have worked together for decades, but there are challenges in the relationship. Many of these are long standing and inform India's foreign interference activities. India perceives 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.

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

Like the PRC, India conducts foreign interference through diplomatic officials in Canada and through proxies. A body of intelligence indicates that proxy agents may have, and may continue to be, clandestinely providing illicit financial support to various Canadian politicians in an attempt to secure the election of pro-India candidates or gain influence over candidates who take office. The intelligence does not necessarily indicate that the elected officials or candidates involved were aware of the interference attempts, or that the attempts necessarily succeeded.

India also uses disinformation as a key form of foreign interference against Canada, a tactic likely to be used more often in the future.

Until recently, Canada was trying to improve its bilateral relationship with India. However, the assassination of Hardeep Singh Nijjar, coupled with credible allegations of a potential link between agents of the Government of India and Mr. Nijjar's death, derailed those efforts. India has repeatedly denied these allegations.

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.

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. It also has sophisticated cyber capabilities. For the last two years, Russia's war in Ukraine has driven much of its disinformation effort.

Even though Russia has the capability to engage in significant foreign interference against Canada, it appears to lack the intent, since Canada is not perceived as an existential threat to Russia.

Until now, the government has not observed Russian interference specific to democratic processes. Russian cyber threat activity has been observed in Canada, but not against Canadian democratic institutions. However, Canada's strong support of Ukraine could affect whether Russia tries to influence the next federal election.

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 artificial intelligence, to facilitate its foreign interference.

Iran

Iran is not, 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 activities and conducts psychological harassment online. Such tactics may very well prevent people from participating in Canadian democratic processes, but this is difficult to determine with certainty.

Canada recently listed the Iranian Revolutionary Guard Corps as a terrorist entity. This could result in increased foreign interference activity leading up to an election, among other potential reactions.

Foreign interference tactics

Foreign countries use a range of tactics to interfere with Canada's democracy. They do so directly or through proxies or co-optees. Examples of tactics include:

- long-term cultivation of long-lasting relationships with their target
- eliciting information from targets
- covert financial support
- mobilizing and leveraging community organizations
- exploiting opportunities in political party processes
- extortion
- threats
- cyber threats
- media influence, misinformation and disinformation.

The six identified major instances of suspected foreign interference in Canada's democratic processes

As part of its investigation, the Commission asked the government to list and describe all major instances of suspected foreign interference targeting Canada's democratic processes from 2018 to the present.

The list was the result of consensus reached among senior officials from CSIS, the Communications Security Establishment ("**CSE**"), Global Affairs Canada ("**GAC**") and Public Safety Canada ("**Public Safety**"). I note that this is not an exhaustive catalogue of potential foreign interference in Canada's democratic processes and institutions. To be on the list, an instance had to be circumscribed in time, and the government had to have intelligence about the impact of the activity.

The list initially had seven major instances of suspected foreign interference, but one was deleted after CSIS reviewed public records. Those records contradicted a significant element of the intelligence underlying the alleged instance.

This situation illustrates the frailty of intelligence noted above. This frailty exists even when the information is collected from sources considered reliable. For example, in this instance, information available at the time but only discovered several years later changed the government's understanding of what happened.

Ultimately, the frailty and limits of intelligence mean considerable care is required when relying on intelligence to draw conclusions or make allegations about the actions of an individual, particularly where the consequences for the individual and for public trust in Canadian democratic institutions will be significant.

Of the remaining six instances, four are discussed above, and relate to suspected foreign interference in the 2019 or 2021 elections.

During its investigation, the Commission received and reviewed CSIS's intelligence reporting about the other two suspected instances. The Commission also examined CSIS and other government officials *in camera* on this. As the suspected instances are based on highly classified information, the descriptions below represent as much information as I can publicly disclose. I discuss these 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 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 foreign government's activities likely had a negative impact on the individual's political career. No information about this was passed to the political level until the list of major suspected foreign interference instances was prepared for the Commission.

The second instance involved a former opposition parliamentarian who was suspected of working to influence parliamentary business for a foreign government.

All the instances were assessments based on intelligence reporting, not proven fact. 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, levels of knowledge and motivations of the individuals involved. Moreover, assessments were based on information government had at the time, but they can evolve, sometimes drastically, over time.

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

It may seem easy to draw the line between legitimate foreign influence and foreign interference, but it is not. Diplomacy, even aggressive attempts to influence other countries, is legitimate when it is done in the open and does not involve threats to individuals or groups. Foreign interference is done covertly, deceptively or involves threats.

But there is often a grey zone: foreign interference and foreign influence exist along a continuum and are much easier to define in theory than to apply in specific circumstances.

There is no common international definition of foreign interference. Indeed, 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 PRC maintains that it is foreign interference for other countries to criticize it for failing to adhere to international human rights obligations. Canada views such criticism as a legitimate way to hold the PRC accountable as a member of the international community.

A concept viewed through different lenses

I found Canada's working definition of foreign interference is generally consistent across government departments and agencies. It is based on legislation (the *Canadian Security Intelligence Service Act*) and 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.

Nevertheless, different government departments and agencies can differ about whether a set of facts constitutes foreign interference and, if it does, how serious the interference is.

As long as it does not paralyze decision-making, I believe that debate within government about whether something constitutes foreign interference can be positive. Different views facilitate a coordinated response that considers all relevant risks, priorities, values and interests, and generally lead to a better outcome. In matters of national security, it can be dangerous to accord too much weight to any one point of view.

Increased discussions over the past three to four years have led to greater agreement and understanding across government about what constitutes foreign interference. As I heard that the 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.

In the next chapter, I summarize the key players involved in the national security and intelligence community that respond to foreign interference and the government's national security coordination and governance processes.

Chapter 11: How Canada Protects Against Foreign Interference

Federal entities have specific powers and authorities to respond to foreign interference. There are also processes to coordinate and govern the work of these entities.

The Intelligence cycle

Cabinet sets intelligence priorities every two years. Producers of intelligence use these priorities to collect and assess intelligence and share products with consumers.

Key players in the national security and intelligence community

Canadian Security Intelligence Service

The Canadian Security Intelligence Service (CSIS) is Canada's domestic intelligence service. Its primary mandate is to collect, analyze and retain information and intelligence about activities that may reasonably be suspected of being threats to the security of Canada. Foreign interference is considered a threat to the security of Canada. CSIS can investigate threats within or outside Canada.

In addition to the above mandate, CSIS also has a very limited foreign intelligence mandate. Under the *Canadian Security Intelligence Service Act*, 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.[10] However, CSIS can only do so within Canada.

Prior to the *Countering Foreign Interference Act*, CSIS could only collect information located within Canada. Now, in some circumstances, the assistance CSIS provides at the request of the Minister of Foreign Affairs or National Defence may include collecting, from within Canada, intelligence located outside of Canada.

[10] Foreign intelligence is defined as intelligence in relation to the defence of Canada or the conduct of Canada's international affairs relating to the intentions, capabilities or activities of foreign individuals, 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.

CSIS collects information from various sources, including human and technical sources, as well as from open source materials. It also relies on warrants, which allow for more intrusive investigations. And it can partner with others, like foreign states and other agencies, to further its investigations.

CSIS assesses and analyzes intelligence to inform government policy development and operational decisions.

Response toolkit

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

CSIS must have reasonable grounds to believe that the activity the TRMs address constitutes a threat to the security of Canada, and the TRMs 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.

Since 2015, CSIS has undertaken 20 TRMs related to foreign interference that did not require warrants. It has not undertaken any requiring warrants.[11]

The *Countering Foreign Interference Act* expanded CSIS's information-sharing capabilities. If certain conditions are met, it can now share information with a person or entity for the purpose of building resilience against threats to the security of Canada. This allows CSIS to share classified information with those who do not hold security clearances, and who are outside the federal government. When and how this will be done remains to be seen.

When CSIS has information regarding a physical threat to an individual, it can share that information with law enforcement, and can do so quickly, or take other steps to address the threat. However, CSIS does not have a specific policy on sharing threat to life or physical integrity information with police.

Communications Security Establishment

The Communications Security Establishment (CSE) collects foreign signals (electronic communications and information) intelligence. It works in accordance with the government's intelligence priorities. CSE cannot direct its activities at Canadians or at anyone in Canada.

---

[11] Under section 12.1 of the *Canadian Security Intelligence Services Act*, if a TRM would limit a *Charter of Rights and Freedoms* right or freedom, CSIS must get a warrant before taking any measures.

CSE also assists federal security and law enforcement agencies, including CSIS and the RCMP. When a requesting agency has authority to target persons in Canada, including Canadians, CSE may assist that agency by collecting signals intelligence about those persons. Any information gained by CSE belongs to the requesting agency and not to CSE.

CSE also provides advice and assistance to federal and certain designated non-federal systems to defend against cyber attacks and engages in defensive and active cyber operations.

CSE reporting does not include assessments or analysis of intelligence.

Response toolkit

CSE's Canadian Centre for Cyber Security ("**CCCS**") has a variety of sophisticated automated sensors to defend federal government systems. They help detect suspicious activity and cyber attacks. CCCS has recently begun installing these sensors on government laptops.

Since 2015, CCCS has worked with Elections Canada to reinforce Canadian electoral infrastructure. CCCS also works with provincial and territorial governments, including using sensors on their systems. On request, it advises political campaigns and parties about cyber security. There is a CCCS guide for campaign teams.

Defensive cyber operations ("**DCOs**") allow CSE to take online actions to disrupt foreign cyber threats to protect Canadian infrastructure. 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.

CSE uses its technical expertise to try to identify those responsible for a cyber event, but this is challenging, and most cyber threat activity is unattributed. Attribution of misinformation and disinformation campaigns is even more challenging than for cyber threats.

Global Affairs Canada

Global Affairs Canada (GAC) is Canada's international relations department. It is one of the largest consumers of intelligence. It focuses on intelligence about the capabilities, intentions and activities of foreign states. GAC receives intelligence from government agencies like CSIS and CSE, as well as from partner agencies.

GAC's Intelligence Bureau assesses intelligence and shares it internally and externally. These assessments 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* (collectively, "**VCCR**"). These are the "rules of the road" for state interactions. If countries do not abide by the VCCR or otherwise present a threat to Canadian security, GAC can use its diplomatic toolkit.

GAC's primary diplomatic tools are different types of 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 position on an issue.

Other bilateral responsive actions include:

- canceling 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.

GAC can also declare diplomatic or consular staff *persona non grata*.

Additionally, GAC can impose sanctions on companies or individuals. Sanctions have not yet been used to counter foreign interference targeting democratic institutions and processes but are fairly common in other circumstances.

The essence of diplomacy is maintaining discussions with foreign states, even adversarial ones, to advance Canada's interests. Thus, while public measures such as declaring a diplomat *persona non grata* or imposing sanctions on a diplomat or country may help deter or counter foreign interference, they can also come at significant cost to Canada.

Using GAC's diplomatic tools to deter and counter PRC foreign interference

Canada's relationship with the PRC is an example of how GAC has used diplomatic tools to deter and counter foreign interference while maintaining a relationship with a foreign state.

While there was some diplomatic activity in response to PRC foreign interference before the return of Mr. Kovrig and Mr. Spavor, until they returned, Canada had to be prudent in its interactions with the PRC, because the priority was getting them home. Immediately after their return 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 continued to systematically warn the PRC that foreign interference is a core issue for Canada, and that if the PRC did not address it there would be consequences. Canada's response progressed to concrete actions such as denying visas to PRC officials and denying a request to create new positions in the PRC's Embassy in Canada.

In the fall and summer of 2023, GAC officials demarched the PRC Ambassador regarding the WeChat disinformation campaign targeting Member of Parliament (MP) Michael Chong and a spamouflage campaign that targeted various MPs. GAC subsequently issued public statements to denounce these two campaigns.

While some might be of the view that most diplomatic measures are not sufficient deterrents to foreign interference activities, it must be borne in mind that taking forceful measures generally leads to retaliatory measures against Canada.

Declaring Zhao Wei persona non grata

On 8 May 2023, Canada declared PRC diplomat Zhao Wei *persona non grata*. The timing was such that some, including Mr. Chong, considered this a direct response to a *Globe and Mail* article published on 1 May 2023 about Mr. Zhao's interest in Mr. Chong and his family.

GAC witnesses testified that Mr. Zhao was declared *persona non grata* as part of a series of escalatory diplomatic steps to condemn the PRC's foreign interference. They said there was a discrepancy between what the newspaper reported and what the intelligence suggested. Critically, I was told that the consensus view of the national security and intelligence community in Canada was that Zhao Wei did not engage in foreign interference with respect to Mr. Chong. However, when the news article came out, Mr. Zhao's position in Canada became untenable and so he was chosen for the declaration.

Further, the evidence suggests that the declaration was one of the diplomatic tools already under consideration when the newspaper article was published and was not issued in response to the story. Mr. Zhao was declared *persona non grata* as part of a series of escalating diplomatic steps, most of which had not been announced publicly, to condemn and deter PRC foreign interference activities.

Rapid Response Mechanism (RRM) Canada

Global Affairs Canada (GAC)'s Rapid Response Mechanism ("**RRM**") Canada contributes to Canada's foreign interference response by monitoring publicly accessible online information to identify misinformation and disinformation during federal election periods. GAC also works with CSE on attributing responsibility for cyber attacks against the federal government.

RRM Canada does not do baseline monitoring of the domestic online information 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 this with the SITE TF.

The Royal Canadian Mounted Police

The Royal Canadian Mounted Police (RCMP) detects, deters and counters foreign interference through enforcement of several Acts, including the *Foreign Interference and Security of Information Act* ("***FISOIA***"), the *Criminal Code* and the *Canada Elections Act*.

The RCMP's Federal Policing branch has responsibility for criminal foreign interference threats. Since 2020, the RCMP has had a Foreign Actor Interference Team which educates and guides investigative units about foreign interference. The RCMP is also working on developing an advanced national security criminal investigator's course and more specialized foreign interference training.

There is a growing recognition within the RCMP that a level of specialization in foreign interference and dedicated foreign interference-related resources are required. The Deputy Commissioner said the need for these resources exceeds capacity.

Response toolkit

The primary responsibility for foreign interference investigations lies with the RCMP's Federal Policing National Security unit. It brings together trained law enforcement or national security and intelligence personnel from the federal, provincial and municipal levels.

At my request, the RCMP reviewed its investigative holdings since 2018 for work on foreign interference. It identified over 100 investigations. Out of these, there were only six occurrences of possible foreign interference targeting Canada's democratic processes. Five were closed because the RCMP concluded that the allegations were unfounded. One is ongoing.

As I explained earlier, there are significant challenges associated with prosecuting foreign interference-related offences when they are based on intelligence. The RCMP acknowledged that prosecutions are no longer necessarily the "gold standard" of threat mitigation. Disruption measures such as regulatory sanctions, financial intervention, immigration inadmissibility and community policing may be used in the foreign interference context.

Another means by which the RCMP counters foreign interference is by engaging with the public and stakeholders within the community to build resilience.

Public Safety

Public Safety develops and provides advice to the Minister of Public Safety on national security matters. The Minister is responsible for the RCMP and CSIS, as well as three other portfolio agencies (the Canada Border Services Agency, Correctional Service of Canada and Parole Board of Canada).

Policy development and coordination

Public Safety's primary function is to facilitate the operations of the entities under the Minister's responsibility through the development of policy. It also develops policy to counter threats and advises the government on national security, among other areas.

Public Safety is not directly accountable for operational responses to intelligence and does not direct immediate threat responses. It compiles information and convenes discussions and contributes to decisions about government's response.

Privy Council Office

The Privy Council Office (PCO) is the central agency that coordinates public service support to the Prime Minister and Cabinet. It has a convening function, bringing together other departments and agencies in the national security and intelligence community to ensure inter-departmental coordination and awareness of threats and responses.

PCO also has a challenge function, which means that it asks questions, offers advice and gives guidance to other departments or agencies based on a broad, whole-of-government perspective.

PCO does not develop or initiate policy but flags competing tensions and priorities for ministers, which gives them the opportunity to debate, discuss and weigh various considerations when making decisions.

The branch of PCO most directly involved in matters of national security is the office of the National Security Advisor to the Prime Minister ("**NSIA**"). The NSIA provides the Prime Minister and Cabinet with strategic assessments, policy advice and operational advice in relation to national security and intelligence, foreign policy and defence.

The NSIA has a strong coordination role in the national security and intelligence community and can bring departments and deputy ministers together to look at issues, respond to current events and manage crises.

The NSIA oversees several secretariats, of which four are relevant to foreign interference:

- Security and Intelligence Secretariat
- Intelligence Assessment Secretariat
- National Security Council Secretariat
- Foreign and Defense Policy Advisor Secretariat.

Open source intelligence (OSINT)

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 can and do use it to advise their ministers and deputy ministers. However, there are gaps in the coordination of OSINT activities occurring across the government. There is no assessment secretariat for domestic OSINT like Canada has for foreign intelligence.

OSINT is seen as increasingly valuable and critical to understanding societal cohesion, impacts on democratic processes and public confidence in institutions, particularly with respect to social media.

There are several challenges to mining open source data, including definitional and legal issues, particularly with respect to privacy. However, if approached in the right way, I strongly believe that it could give senior decision-makers tools to speak to the public and increase public confidence in government.

National security coordination and governance

There are a several ways in which government coordinates and governs national security matters with respect to foreign interference.

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. They are a key part of how the departments and agencies involved in national security and intelligence communicate with each other, keep each other informed of issues and decide what to do about them.

In 2023, PCO began a restructuring of the inter-departmental committees related to national security, as the structure had become cumbersome and somewhat duplicative. The intent of the restructuring was to improve information flow and increase overall efficiency and effectiveness.

The new governance structure reduces the number of deputy ministers to five instead of approximately a dozen. All are chaired by PCO.

The evolving role of the NSIA

Over the last year, steps were taken to strengthen the coordination role of the NSIA. The current NSIA is now also a deputy clerk, which, I was told, signals the importance of the position and strengthens the NSIA's influence within the deputy minister community. The NSIA is also the secretary of Cabinet's National Security Council.

In November 2024, the Prime Minister published a mandate letter to the NSIA, which reflects the NSIA's responsibilities and sets out specific priorities. One priority is the production of a renewed National Security Strategy in 2025, with an integrated framework for Canada's national security, defence and diplomatic position.

Some of the other priorities are refreshing Canada's intelligence priorities on an annual basis, modernizing the intelligence assessment process, systematizing the flow of information across government and improving communications and engagement.

The publication of a public document such as a mandate letter in this instance strikes me as a very good initiative that should become standard practice.

The evidence and review of the processes put in place to counter foreign interference satisfy me that the function of the NSIA is critical. This position is always entrusted to a senior and very experienced public servant. I note that many individuals have filled this position in a relatively short time. In my opinion, the high turnover rate probably played a part in some of the communication issues that were identified by the National Security and Intelligence Review Agency (NSIRA), the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the Commission itself.

Role of the National Counter Foreign Interference Coordinator (NCFIC)

The position of National Counter Foreign Interference Coordinator ("**NCFIC**") was created in March 2023. The NCFIC is part of Public Safety and the role is one of policy coordination. The NCFIC is a regular participant in assistant deputy minister level inter-departmental committees.

That said, the role of the NCFIC is still very new, and remains a work in progress. In my view, 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. At the time of this Final Report, the ones relevant to foreign interference were the:

- Cabinet Committee on Global Affairs and Public Security[12]
- Incident Response Group[13]
- National Security Council.

The National Security Council, created in 2023, is a forum for a strategic whole-of-government approach to national security. I heard that it is a significant innovation that has already proven useful. It was described as "extraordinarily important" by the current Clerk of the Privy Council. It creates a standardized process for bringing intelligence to Cabinet and is focused on long-term strategic planning.

The above shows that for some time, government has been striving to strengthen and simplify its governance structure relevant to countering foreign interference. It is too early to assess the changes made or under discussion, but it seems to me that giving it further thought was necessary. The complexity of the structure that was in place up until recently complicated decision-making.

The next chapter reviews the government's policy and legislative responses to foreign interference.

Chapter 12: Policy and Legislative Responses to Foreign Interference

Two key parts of the government's work to detect, deter and counter foreign interference are the Plan to Protect Canada's Democracy ("**Plan**") and the Countering Hostile Activities by State Actors Strategy ("**HASA Strategy**").

Plan to Protect Canada's Democracy

The Plan created two important processes to respond to foreign interference threats during an election period: the Security and Intelligence Threats to Elections Task Force (SITE TF) and the Critical Election Incident Public Protocol (CEIPP).

[12] This committee considers issues about Canada's engagement with the international community. It is responsible for issues related to domestic and global security and sets intelligence priorities.

[13] An *ad hoc* Cabinet committee that can be activated in response to a specific situation to provide a tactical, operational forum for ministers and deputy ministers to coordinate a response to a specific incident.

The SITE TF is made up of representatives from CSE, CSIS, the RCMP and GAC. During general elections and by-elections, it coordinates the review of election-related intelligence, provides situational awareness and shares information. Individual members maintain their independent authorities to act.

The CEIPP established a panel of five senior public servants, called the "Panel of Five" or the "Panel," who review information received from the SITE TF and other sources and assess whether the CEIPP threshold for a public announcement has been met. That threshold is met when an incident or incidents threaten the integrity of the election, and if this occurs, then the Panel must ensure Canadians are informed. The Panel was established to remove political interests from the evaluation and announcement of threats to the electoral process.

The threshold for an announcement is high because intervening in an election is not something that can be done lightly. There is a risk that Panel intervention might do more harm than good since the moment a public announcement about foreign interference is made, confidence in the election could be undermined and negatively affect public confidence in Canada's democracy. There is also the potential that the Panel itself would be viewed as partisan and interfering in the election. In addition, foreign countries might intentionally try to cause an announcement to undermine confidence in elections or amplify disinformation.

The Plan also included a bundle of initiatives designed to build societal resilience against misinformation and disinformation, among them the Canada Declaration on Electoral Integrity Online ("**Declaration**")[14] and the Digital Citizen Initiative ("**DCI**"). The DCI is a strategy of the Department of Canadian Heritage ("**Canadian Heritage**") that aims to support democracy and social inclusion by building resilience against online disinformation and supporting a healthy information ecosystem.

The Plan in operation: 2019

In advance of the 2019 general election, the four major United States social media companies – Microsoft, Twitter, Facebook and Google – signed the Declaration.

The SITE TF's work began well before the election. For example, in November 2018, it began to develop a range of analytic products to help define threats to the election. 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. It also provided Secret level briefings to security-cleared political party representatives.

[14] A voluntary agreement which establishes a set of commitments between platforms and the government to safeguard federal elections from malicious interference and build a healthier online ecosystem. It does not have the force of law and not all social media platforms are signatories.

As for the Panel of Five, meetings started immediately before the election period and, once the election period began, it met weekly and was always on call.

In 2019, the Panel concluded that the threshold for an announcement had not been met. It found that some foreign interference had occurred, but nothing that threatened Canada's ability to have a free and fair election.

While the SITE TF saw foreign interference activities targeting certain ridings and candidates, the Panel concluded those activities were not part of a broad-based electoral interference campaign and did not impact the outcome of the election.

The Plan in operation: 2021

The Declaration was updated and TikTok, LinkedIn and YouTube joined the original four members.

The SITE TF operated in a similar manner to 2019 but, as a lesson learned from the 2019 election, it acknowledged the importance of sharing information at the lowest classification level possible.

The SITE TF concluded that the PRC 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 done so.

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.

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

The evolution of the Plan after 2021

Many changes to the Plan have occurred since the last general election in 2021, including:

- The SITE TF now provides enhanced monitoring with respect to by-elections and produces unclassified after action reports. So far, it has not observed any indication of foreign interference in by-elections.
- New Panel members receive 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 said they value these regular briefings.
- Canadian Heritage established the Digital Citizen Contribution Program to administer funding for applied research and citizen-

focused activities. It also funds the Canadian Digital Media Research Network ("**CDMRN**"), a network of academic and civil society groups that monitor and analyze the information ecosystem in Canada. The CDMRN is part of the Media Ecosystem Observatory (MEO).

- The government also created the Protecting Democracy Unit within the Privy Council Office (PCO), which coordinates, develops and implements government-wide measures designed to protect Canada's democratic institutions, as well as a whole-of-society approach to protect democracy.

Looking to the future of the Plan

The government is working to develop a third version of the Plan. Policy options are being regularly discussed at both the civil service and ministerial levels. Some of these may impact the Plan's future development. There are currently discussions about the membership and mandate of the SITE TF, including whether it should be made permanent and, if so, how it should be structured and where it should be located within government.

Consideration is also being given to how to increase public awareness of the measures the government has in place to protect elections, including the role of the SITE TF and the mandate of the Panel of Five. Other discussions are about the possibility of a lower CEIPP threshold for public announcements and how to engage more effectively with political parties.

Another discussion within government is whether it should monitor Canada's domestic online information environment for disinformation outside of elections and, if so, which federal entity might do it. While RRM Canada's expertise has been highly useful for the SITE TF, monitoring the domestic online information environment is not the function it was originally intended to perform. RRM Canada's work during elections comes at a cost to its ability to focus on its international mandate.

Finally, there are discussions on whether Canada should renew the Declaration on Election Integrity Online for the next general election, and what changes could be made in terms of updates or new signatories. Another option for dealing with social media platforms would be regulation, which the government has considered, although there are possible issues around censorship and regulation of free speech.

The government has started regulating some online content and social media. In 2023, the government amended the *Broadcasting Act* to regulate streaming services. Also, under the *Online News Act*, if a social media platform meets certain criteria, it must notify government and negotiate with news companies whose content is posted on the platform.

The Countering Hostile Activities by State Actors Strategy

Starting in 2018, the government began to develop the Countering Hostile Activities by State Actors Strategy (HASA Strategy). 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 facing Canada. The overarching objective was to pursue a whole-of-government and whole-of-society approach involving the national security and intelligence community, private entities and other levels of government. As part of this strategy, Public Safety was to also develop a broader communication approach, which could include a public-facing version of the HASA Strategy and a communications strategy.

A Memorandum to Cabinet titled, "Modernizing Canada's Approach to Addressing Threats from Hostile Activities by State Actors" was submitted to Cabinet in May 2022, almost four years after the work to develop the HASA Strategy began. It included a number of proposals, including one to consult on legislative amendments.

Implementation of the legislative proposals took some time. Marco Mendicino, former Minister of Public Safety, said this was because a whole-of-government response was needed to help facilitate public engagement and deal with concerns that the HASA Strategy might be overreaching, run afoul of the *Charter* or discriminate against diaspora communities.

Two rounds of public consultations were launched: a first in the spring of 2023 regarding the creation of a foreign agent registry and the second in the fall of 2023 focused on other legislative changes that were ultimately included in Bill C-70.

Despite advancements on the legislative side, to date there is unfortunately no document that comprehensively sets out the government's counter foreign interference strategy. The public-facing element has not been finalized. There is also no strategic communication and engagement plan.

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

The *Countering Foreign Interference Act* (introduced as Bill C-70) received Royal Assent in June 2024. It amended the *Canadian Security Intelligence Service Act* in several major ways. It:

- expanded CSIS's ability to collect information located outside Canada as part of its foreign intelligence assistance mandate.

- expanded CSIS's authority to disclose information to any person or entity outside the federal government to build resilience against threats to the security of Canada.
- added new search and seizure powers.

The Act also amended existing foreign interference offences in the *Foreign Interference and Security of Information Act* and created new ones.

The Act 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.

The Act created new rules in the *Canada Evidence Act* about how sensitive information is handled in a range of legal proceedings in the Federal Court.

The Act creates the *Foreign Influence Transparency and Accountability Act* ("***FITAA***"), which, once in force, will establish a public Foreign Influence Transparency Registry. *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 provide information to the government that will be maintained in a registry.

The legislation is not currently in force, and important aspects of it will be set out in regulations that have not yet been drafted.

A renewed National Security Strategy

In November 2024, the Prime Minister's mandate letter to the NSIA tasked her with working through the National Security Council to deliver a renewed National Security Strategy in 2025. The last time Canada's National Security Strategy was updated was 20 years ago.

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

Federal departments, agencies and other entities are not the only institutions that play a role in protecting Canada from foreign interference. There are many others that contribute to this effort.

Elections Canada

Elections Canada administers Canada's federal electoral system under the *Canada Elections Act*, which includes elections and the rules around political party registration and financing.

A core element of its mandate is to provide Canadians with information on the electoral process. Recognizing that foreign interference can deter members of diaspora communities from voting, it has multilingual guides to communicate information about election integrity measures and educational programming targeting diaspora communities.

Elections Canada monitors traditional media and the online environment for inaccurate information about the electoral process, such as an incorrect election date. When this happens, its main response is to communicate accurate information to the public.

Political financing

Regulation of federal political financing aims to establish a level playing field and prevent the undue influence of money. A key feature relevant to foreign interference is that the system excludes the use of foreign money in Canadian elections.

Canadian elections law regulates some aspects of parties, electoral district associations, candidates, nomination and leadership contestants and third parties. Except for third parties – entities like unions, corporations and community organizations – they can only accept contributions from citizens and permanent residents. Third parties can receive contributions from non-citizens but cannot use funds from foreign sources for regulated activities, like election advertising. Third parties must have a separate bank account for all contributions and expenditures for regulated activities, but it can be challenging to identify foreign funding, especially when it is in the form of in-kind contributions. This could present a foreign interference risk.

Proposed legislative amendments

In March 2024, the Government introduced the *Electoral Participation Act* (Bill C-65). Though not specifically targeted at foreign interference, several proposed amendments to the *Canada Elections Act* could have played a role in countering foreign interference. While this proposed legislation was before Parliament for most of the Commission's work, it died on the order paper when Parliament was prorogued in January 2025.

The Office of the Commissioner of Canada Elections

The Commissioner of Canada Elections is the independent officer responsible for enforcing the *Canada Elections Act*. Most complaints submitted to the Office of the Commissioner of Canada Elections (OCCE) relate to political finance rules.

Foreign interference and the *Canada Elections Act*

While the *Canada Elections Act* has no specific offences in relation to foreign interference, it has prohibitions that apply specifically to foreign nationals, including prohibitions on undue influence and making political contributions or expenditures, as well as prohibitions of foreign broadcasts during election periods. The Act also has prohibitions that apply to both Canadians and foreigners – such as intimidation of an elector – 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 it has additional supervision. The OCCE receives many complaints purportedly about "foreign interference" that do not in fact allege an offence under the *Canada Elections Act*. These are generally closed without further action.

Because 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, it does not receive direct disclosures of things like suspicious transaction reports and must go through the RCMP to get the information. It recently asked to be added as a designated recipient of FINTRAC information. 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.

The OCCE is also trying to better equip itself to use classified intelligence in its investigations and strategic planning.

The OCCE has a range of tools to ensure compliance with the *Canada Elections Act*. Among them, are administrative monetary penalties ("**AMPs**"), meant to promote compliance with the Act, and prosecutions. The OCCE has recommended raising the maximum penalties for AMPs and convictions under the criminal regime.

Digital platforms

The OCCE engages with digital platforms to ensure a rapid response to online activities that contravene the *Canada Elections Act*. 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 *Canada Elections Act*.

Since the 2019 election, the OCCE has been concerned about manipulated imagery or videos. It has an analytical team responsible for tracking all artificial intelligence and deepfakes it finds related to elections.

The Canadian Radio-television and Telecommunications Commission (CRTC)

Much of government's policy framework for media is the responsibility of the Canadian Radio-television and Telecommunications Commission ("**CRTC**"), a tribunal that operates independently of government. It 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. Another guiding principle is that the CRTC should not interfere with freedom of expression.

The CRTC's greatest challenge in responding to foreign interference is its inability to react quickly. Its regulatory processes are based on public procedures and records and it does not have foreign language expertise. If it receives a complaint that a foreign state has instructed a station to broadcast something false that could affect an election or other democratic process, the CRTC cannot do anything about this in real time. This is likely to discourage the filing of complaints.

The CRTC enforces regulations that prohibit false and misleading news. These rules could potentially prohibit the broadcast of misinformation and disinformation. But bearing in mind the objectives of the *Broadcasting Act*,[15] I was told that the CRTC is very reluctant to become the arbiter of truth and act as a censor.

Moreover, even where the CRTC acts to remove foreign stations from the list of authorized stations in Canada, this will not necessarily block them from Canada. A station may remain accessible online since this type of decision does not apply to the Internet. This is a problem to be considered but, as discussed, regulating the Internet is not an easy task.

The House of Commons

The House of Commons ("**House**") is the elected assembly of the Parliament of Canada. As a democratic institution, both the House and its members may be targets of foreign interference.

Foreign interference issues involving members of Parliament (MPs) are handled as part of 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.

The Sergeant-at-Arms acts as liaison with intelligence and law enforcement agencies to address security matters, including foreign interference. It monitors open source intelligence for threats and harassment towards 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 House is responsible for its own information and cyber security. It provides IT security infrastructure, applications and support to MPs, House employees and MPs' staff. It also provides cyber security training to MPs and staff.

House IT systems are independent from government. It shares network infrastructure with the Senate, the Parliamentary Protective Service and the Library of Parliament.

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. However, the line between parliamentary and partisan affairs can sometimes be blurred and there will inevitably be times where House equipment is used for activities viewed as partisan.

---

[15] Supporting cultural expression in English, French and Indigenous languages and upholding and persevering freedom of the press to the greatest extent possible.

The House does not have oversight over MPs' personal electronic devices, even though these may be used for parliamentary activities. However, if an MP suspects that a personal device has been hacked, they can ask the House administration to examine and analyze the device.

If the House detects or becomes aware of a cyber attack it does not necessarily notify parliamentarians. There is no notification about unsuccessful cyber attacks because of the sheer number of them that occur. 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.

The House coordinates with security, intelligence and law enforcement agencies to give unclassified briefings about foreign interference to MPs and staff. Unclassified briefings about foreign interference have also been given to the caucuses of all recognized parties, the Green Party of Canada ("**Green Party**"), independent members and House staff.

The Senate

The Senate is the Upper House of the Parliament of Canada.

As with the House, the Senate handles foreign interference concerns as matters of general security. Like the House, the Senate is responsible for its institutional security and the personal security of senators. This includes accreditation, as well as residence and travel security for senators. When senators are appointed, they and their staff are offered optional onboarding training. This includes foreign interference content.

The Senate is responsible for IT equipment for all senators and Senate employees, cyber security and IT security, including IT-related foreign interference issues.

The Senate provides essentially the same equipment and support to senators as the House does for MPs. It 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.

Political parties

Political parties are on the frontlines of our democratic institutions. They are also a potential target of foreign interference. Political parties are self-governing entities. They are essentially free to make and enforce their own rules to regulate their membership, choose their candidates and select their leaders.

All political party representatives who testified at the public hearings expressed some concern about political parties potentially being a target for foreign interference.

That said, they were all firmly opposed to regulation of leadership and nomination races, and they all stated that the internal measures that have been put in place to ensure the integrity of these races were sufficient, whereas in my view, they are not.

Parties set their own rules for who may become a member of the party and therefore become candidates or vote in nomination contests. Today, most parties with representation in the House of Commons limit membership to citizens and permanent residents, though in some cases this is a recent change, and this requirement is not set out in law.

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.

Parties generally have a vetting process before someone can run in a nomination contest. Although parties do not vet for foreign interference concerns specifically, the vetting process could uncover such information.

Each party uses different verification processes to confirm voting eligibility for nomination contests. Most require members to show identification displaying their name, address and photograph.

Party leaders have the final say on who will be a candidate in an election. This power has been suggested as a way to defend against foreign interference: if the leader is aware of foreign interference concerns early enough, they can prevent someone from running for the party.

Although the Security and Intelligence Threats to Elections Task Force (SITE TF) suggests that nomination contests could be used by foreign states to influence who could become an MP, the evidence did not indicate that this has been widespread to date. In fact, the evidence disclosed only one such potential case: the 2019 nomination contest in Don Valley North, which was mentioned in the government's list of six major instances of suspected foreign interference.[16] This does not mean, however, that this is a vulnerability that should not be corrected.

I also heard that leadership contests may be a source of political party vulnerability to foreign interference. Political parties run their own leadership contests and are free to determine their rules.

[16] See Volume 3, Chapter 10.

The Commission heard testimony about allegations of Government of India interference into a Conservative Party leadership race. CSIS witnesses noted that they had no reason to believe the impacted candidates would have been aware of the alleged support. They also noted that, while they were concerning, not all of India's activities in this matter were covert. CSIS witnesses had no recollection of this intelligence being briefed to the political level, including the candidates themselves.

In June 2024, CSIS delivered a classified briefing to the Conservative Party Leader's Chief of Staff to provide general information about foreign interference threat activities and tactics. The Chief of Staff was advised of the allegations of interference in the leadership race.

The media

Because misinformation and disinformation can have a significant impact on all Canadians, a healthy media ecosystem is important to build citizen resilience to foreign interference. Resilience in this context has been described as ensuring the population is properly equipped to know when and how to validate information with credible sources of information before accepting certain information as true.

Canadians must be equipped to understand that not all information is necessarily true or 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. I would add that it is also important that the media be independent from government and political parties.

Civil society organizations

Many witnesses said civil society is crucial for a whole-of-society approach to detect, deter and counter foreign interference. The Commission could not examine all types of civil society groups as part of its proceedings but did focus on groups that help defend against misinformation and disinformation.

The Media Ecosystem Observatory (MEO) was created in the lead up to the 2019 federal election. It studies the flow of information in the media ecosystem and behavioral responses to that information. One of its conclusions from monitoring the 2021 election was that the ability to quickly understand and contextualize interventions in the media ecosystem would be useful, as compared to having to wait for analysis after the fact.

In April 2022, the MEO received a grant from Canadian Heritage's Digital Citizenship Contribution Program to develop the Canadian Digital Media Research Network (CDMRN) in partnership with other organizations. The

CDMRN 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.

The government expects the CDMRN to play an important role during the next election but the CDMRN does not know if its funding will continue after the end of March 2025. In my view, it is essential to address this issue urgently.

I now turn from reviewing the ways government protects Canada from foreign interference in democratic institutions to look closely at how intelligence about this issue flows within government, including during the 2019 and 2021 general elections.

Chapter 14: Intelligence Flow Within Government

The sheer volume of intelligence, the pace at which it is collected and processed, the complications of classification and the sensitivity of intelligence operations mean that effective information sharing in the national security realm poses a significant challenge. But it is a challenge that must be met – an effective response to national security issues depends on the right people getting the right information in the right way at the right time.

A centralized intelligence distribution system

In the fall of 2023, the government started using a new process to track all formal intelligence reports through an updated CSE centralized database system. This system ensures government knows when and how a piece of intelligence is shared and who has accessed it.

CSE manages this central database and determines who can access intelligence based on sharing policies and an individual's need-to-know. CSE is also responsible for the Client Relations Officer ("**CRO**") system. CROs are CSE employees stationed in other departments who are generally responsible for sharing intelligence to senior government officials and ministerial offices.

Intelligence is often brought to the attention of very senior decision-makers, such as Cabinet ministers or Prime Minister, by way of oral briefings rather than written intelligence products.

Communications Security Establishment

CSE has strict requirements about how CSE products may be shared. It distributes intelligence to the national security and intelligence community through its centralized database.

Intelligence flow to the ministerial level

CSE reports to the Minister of National Defence. The Chief of CSE, or their delegate, decides what intelligence is shared with the Minister. The Minister is alerted if a report requires the Minister's urgent attention. All intelligence products are dated and signed by the Minister to indicate what they have received and read.

Canadian Security Intelligence Service

CSIS produces a significant amount of intelligence. In 2022, it produced over 2,500 threat assessments and reports, including on foreign interference.

CSIS's Assistant Director Requirements decides whether intelligence should be shared, and which product is best suited to a given situation based on several factors, one being source reliability. Source reliability is a very important consideration when sharing and interpreting intelligence.

From what I have seen, CSIS relies heavily on standard caveats and wording to convey source reliability. I do not view this as sufficient.

A dedicated CSIS unit is responsible for distributing CSIS intelligence products across government. The unit has a list of designated individuals within each government client who act as CSIS's primary points of contact, and who are responsible for receiving CSIS products and sharing them. When intelligence products contain sensitive information CSIS uses a restricted distribution list of named identified recipients.

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

CSIS uses CROs to personally give intelligence to ministers and others. It also now has a Liaison Officer posted at Public Safety, which has improved its ability to share and track intelligence sent to that department.

In addition to sharing written intelligence products, CSIS provides oral briefings to ministers and their offices, deputy ministers, the Privy Council Office (PCO) and the Prime Minister's Office and will meet with these individuals and their offices at their request.

I heard evidence that, at times, it has been challenging for CSIS to receive feedback from government clients. Clients now can, and do, give feedback through the new CSE centralized database. CSIS said this feedback is important because it informs its future collection and reporting and gives it insight into the types of information recipients want.

In setting Canada's intelligence priorities, PCO has a feedback process between the intelligence agencies and their regular clients. Feedback is vital and should be encouraged at all levels regularly and frequently.

Intelligence flow to the ministerial level

CSIS reports to the Minister of Public Safety. CSIS meets regularly with the Minister and their office to inform them of national security developments and CSIS's operational activity, as well as to flag emerging issues.

One type of document produced by CSIS is called an Issues Management Note ("**IMU**"). These are meant to alert the Minister of Public Safety and senior officials at PCO when CSIS is going to take specific action. CSIS relied on these products as a way of informing the Minister of Public Safety.

However, information that CSIS believed would be brought to the Minister's attention did not always make it to them. There appears to have been a lack of understanding between CSIS and its clients in relation to IMUs. The information in IMUs did not always reach the Minister and IMUs were not always considered by recipients at Public Safety as particularly significant, among the many intelligence products received.

Global Affairs Canada

Global Affairs Canada (GAC)'s Intelligence Bureau prepares weekly binders for the Foreign Minister's office and for the Deputy Minister. These include the most relevant raw and assessed intelligence.[17] GAC keeps a record of the products in its binders but cannot confirm whether the contents have been read.

Foreign intelligence assessments produced by the Intelligence Bureau are distributed throughout government using CSE's secure database and are shared with like-minded countries. If the Intelligence Bureau considers a product particularly important, it flags it to senior officials on an *ad hoc* basis or in the weekly binder and sends it via a CRO to make sure it is read.

The Intelligence Bureau gives verbal briefings to senior officials at the assistant deputy minister level and above on its own initiative or by request.

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

Intelligence flow to the ministerial level

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

The evidence before the Commission with respect to how much exposure Minister Mélanie Joly had to intelligence about foreign interference before May 2023 was not entirely clear. She said she first began to consider foreign interference when she was working on the Indo-Pacific Strategy (released in November 2022), but that she did not receive intelligence until March or May 2023. There was no evidence that she received *specific* intelligence briefings on foreign interference before May 2023, but documentary evidence tended to show she was nevertheless exposed to the topic of foreign interference before this time in the context of her ministerial work.

Specific intelligence briefings should have begun much earlier in her tenure as Minister of Foreign Affairs. Being exposed to the topic of foreign interference is one thing, but receiving specific intelligence briefings about it is quite another. As the official minister responsible for Canada's relations with foreign states, the Minister of Foreign affairs ought to have been in receipt of intelligence about these activities to inform her deliberations and actions.

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

Royal Canadian Mounted Police

Units within the RCMP's Federal Policing and National Security program consult and use all available reporting to produce criminal intelligence assessments and products to inform senior management.

The RCMP uses distribution lists and chooses a distribution system based on the classification of the product. Products classified Secret or Top Secret are shared internally through the RCMP's Classified Environment or via the Canadian Top Security Network ("**CTSN**"). Externally, the RCMP shares intelligence products via CTSN.

The RCMP also shares information with local police forces about foreign interference. This is important since local police may often be the first to respond to the problem in its various forms.

The One Vision Framework governs intelligence sharing between the RCMP and CSIS. It aims to ensure the two organizations are coordinated and de-conflicted in their responses to threats to public safety. Under the One Vision Framework, intelligence is shared through meetings or "use letters."

Intelligence flow to the ministerial level

The RCMP reports to the Minister of Public Safety and may provide reports or briefings on classified or sensitive information to the Minister where appropriate. However, the relationship between the RCMP and the Minister is limited by the principle of police independence.[18]

Public Safety

Given its broad mandate and that of the Minister of Public Safety, the amount of intelligence received by Public Safety is vast.

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

The unit within Public Safety primarily responsible for receiving intelligence and distributing it to senior officials within the department perform a triage function, elevating particularly sensitive or action-oriented intelligence.

It does not seem necessary or advisable to me to bring every piece of intelligence to the minister. A selection should be made to ensure that they only receive the intelligence of which they must be aware and do not already know.

Intelligence flow to the ministerial level

The Minister of Public Safety receives intelligence from CSIS and the other portfolio agencies they oversee, as well as from Public Safety.

Before the pandemic, Public Safety officials were responsible for directly transmitting intelligence marked for the Minister's attention. Public Safety staff were also responsible for selecting a filtered subset of products, from the river of intelligence sent to Public Safety. A weekly binder was delivered to the Minister's office by a Departmental Liaison Officer. Public Safety staff did not track what happened after information was provided to the Minister's office.

Witnesses had different recollections of how intelligence was shared with then-Public Safety Minister Bill Blair during the pandemic.

Some said that Public Safety continued to produce binders of intelligence, which were delivered to the Minister at the CSIS Toronto Regional Office or brought to his home in Toronto. They were of the view that the pandemic did not have a material impact on the flow of intelligence.

Others said the weekly binders stopped coming during the pandemic. The Minister's office would receive smaller subsets of intelligence, on a less than weekly basis, and not in a binder. Another said the flow of paper intelligence

[18] This principle requires police be free from the direction or influence of the executive in exercising their police powers or making decisions related to law enforcement and the investigation of individual cases.

largely stopped during the pandemic, save for *ad hoc* readings, at CSIS's request, which occurred in a secure facility.

Clearly, there are different recollections as to whether or how routine intelligence was provided to the Minister's office at the height of the pandemic. In my view, given that so few staff were working in person, and that the Minister himself was in Toronto, it is possible that while Public Safety continued to print and provide intelligence to the Minister's office, this was not done systematically, as it had been before the pandemic. It could also be that Public Safety did continue to send binders of intelligence to the Minister's office, but that for some reason they never reached the Minister's Chief of Staff. In any event, this difference in recollection shows a significant communication breakdown in this period.

From what I heard over the course of the Commission's proceedings, written intelligence products were not a reliable way of conveying information to ministers. On the evidence before me, when something urgent had to be brought to the Minister's attention, it was generally done by a verbal briefing, not by sending a written intelligence product. Therefore, the real issue was not so much whether an intelligence report had reached the Minister, but whether the information itself had been shared with him. The fact that some information did not reach him in due time is concerning. However, there is no evidence that any information was withheld intentionally.

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

Recent modifications to intelligence flow at Public Safety

Public Safety now uses CSE's centralized intelligence database and there is a CSIS Liaison Officer posted at Public Safety who is responsible for curating intelligence for senior officials, including the Minister. This strikes me as good practice.

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

Public Safety witnesses told me the Liaison Officer has good awareness of their interests and requirements and understands the broader context in which Public Safety operates. They see this system as more responsive than the previous one. I cannot say whether this is the case, but a close look should be kept on how the new system works to prevent the intelligence flow problems seen in the last years.

Privy Council Office

Intelligence Assessment Secretariat

The Intelligence Assessment Secretariat ("**PCO-IAS**") publishes a variety of intelligence assessment products, including the Daily Foreign Intelligence Brief ("**Daily Brief**") and the Prime Minister's Weekly Intelligence Brief ("**Weekly Brief**").

All PCO-IAS products are now on CSE's database. PCO-IAS mostly shares intelligence via this system because tracking of distribution, readership and feedback is automated.

Security and Intelligence Secretariat

Much of the reporting PCO's Security and Intelligence Secretariat ("**PCO-S&I**") receives is circulated through electronic tools, which automatically record when a user has opened a document or report.

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

Former National Security and Intelligence Advisor to the Prime Minister (NSIA) Jody Thomas explained how she received intelligence during her tenure (January 2022 to January 2024).

PCO-IAS gave her a daily intelligence package that could contain up to 100 reports. If Ms. Thomas was a named recipient of a report, her staff would bring this to her attention. Highly classified intelligence products with limited distribution would be brought to her directly by CROs. She also received information as a member of the Deputy Minister Committee on Intelligence Response.

The NSIA has primary responsibility for determining what intelligence needs to go to the Prime Minister, though others in the Prime Minister's Office or senior public servants can also flag matters for his attention.

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

The NSIA determines what will go into the Prime Minister's weekly reading package and provides the identified products to a CRO. The CRO notes any questions the Prime Minister has and passes them on to the NSIA or Deputy NSIA's attention.

The NSIA and Deputy NSIA also provide their own weekly briefings to the Prime Minister and his senior staff.

In triaging intelligence for the Prime Minister, Ms. Drouin and her team consider several factors including, what the Prime Minister is about to do, what needs to be done in response to the intelligence, if there is anything imminent he needs to know, the reliability of the intelligence, whether it is corroborated and whether it is something he knows about already.

Not every piece of intelligence needs to go to the Prime Minister. In Canada's Westminster system, ministers also have accountabilities. Moreover, if the head of either CSIS or CSE and the NSIA were unable to agree on whether to send intelligence to the Prime Minister, the agency head could go to their respective minister or to the Clerk of the Privy Council and raise the issue and they would decide whether to inform the Prime Minister.

Democratic Institutions

PCO Democratic Institutions ("**PCO-DI**") is not a regular consumer of national security intelligence, but it regularly receives intelligence assessments. PCO-DI requires an understanding of intelligence trends or the threat landscape for its policy work but does not need to see raw intelligence. PCO-DI's conduit into the national security agencies is PCO-S&I because it deals directly with the national security and intelligence agencies at an operational level.

The Clerk

The Clerk receives a daily package of intelligence from national security and intelligence agencies and may receive further intelligence directly from agency heads.

When Ms. Thomas was NSIA, she would flag intelligence for the Clerk's attention. The Clerk at that time was Janice Charette. Ms. Thomas and Ms. Charette would then decide whether it should go to the Prime Minister. Ms. Charette might also have other information about upcoming issues or the Prime Minister's concerns, which could indicate that a specific report needed to be shared with him.

The Prime Minister's Office

Senior staff in the Prime Minister's Office (PMO) rely on PCO, chiefly the NSIA, to identify intelligence and brief them.

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

During the pandemic, the PMO did not get the same amount of intelligence in paper form. When PCO or security agencies determined staff needed to know about a piece of intelligence, they would make arrangements to brief the PMO.

After the 2021 election, the system became more hybrid. The Prime Minister's staff used secure phones for sharing intelligence below the Top Secret level and received intelligence in paper form.

The PMO also started receiving more raw intelligence products. This was partly due to the NSIA at the time, since each NSIA has their own style and focus, and partly due to events going on in the world.

After the media leaks in 2023, intelligence sharing protocols become much stricter. Now, intelligence is shared through a CRO. The CRO brings the Prime Minister's Chief of Staff an organized and prioritized package of information and tracks each piece she reads. The CRO also flags intelligence that the Prime Minister has or is about to read, as well as any comments he has made about it.

The Prime Minister

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

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

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

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

Specific instances where concerns about intelligence flow were raised

During the Commission's investigation, four specific instances of potential problems with the flow of intelligence within government were highlighted.

I first examine the distribution of two intelligence products within government. Both the National Security and Intelligence Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP) reviewed these events and drew certain conclusions about them in their 2024 Reports about foreign interference.

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

The PCO Special Report

The "PCO Special Report" is a PCO Intelligence and Assessment Secretariat (PCO-IAS) product about People's Republic of China (PRC) foreign interference prepared in late 2021 and early 2022. It was never finalized. An early draft was referred to in media reports in early 2023. PCO-IAS labelled the report "special" because it had two novel features: was the result of collaboration between PCO-IAS and CSIS, and because it combined domestic and foreign intelligence.

In the fall of 2021, David Morrison, who had recently been appointed Acting NSIA, asked PCO-IAS to prepare a report that would give him a global perspective on PRC foreign interference and help him assess its severity. Mr. Morrison was the intended audience. He noted that while "much has been made subsequently [...] as to why this document didn't make it to X person in the political level," that was not his intention in requesting the PCO Special Report.

The head of PCO-IAS at the time, Martin Green, had a different recollection. He said he suggested to Mr. Morrison that PCO-IAS should produce a paper putting together what was happening internationally and domestically with PRC foreign interference. In his view it was intended for a senior-level discussion.

PCO-IAS worked with CSIS to produce the PCO Special Report. Sometime in December 2021, a draft was ready. Mr. Morrison met with PCO-IAS and provided feedback, including comments on the tone, which he found to be somewhat hyperbolic, and said he wanted another draft. He also said he viewed some of the activities described as legitimate and common diplomatic activity. Mr. Morrison then had no more involvement with the PCO Special Report because he was no longer Acting NSIA. He was appointed Deputy Minister for International Trade shortly after the meeting.

Mr. Morrison has since read the second draft of the PCO Special Report and said it still does not respond to his original questions about the size, scope and effectiveness of PRC foreign interference. He does not think it should have been shared with the Prime Minister.

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

Mr. Green shared the draft PCO Special Report shortly after Jody Thomas succeeded Mr. Morrison as NSIA in January 2022. Mr. Green recommended Ms. Thomas share the PCO Special Report with certain ministers and senior public servants.

When Ms. Thomas read the PCO Special Report, she thought it was useful but contained nothing particularly new. It was a collection of previously available information. She was concerned generally that some of the language being used in intelligence products was too broad and inflammatory.

Still, she thought the PCO Special Report was a useful primer for policy discussions and asked it to be put through the usual PCO governance process for intelligence products. This is an essential element of processing intelligence within PCO and the intelligence world. The process ensures that intelligence products are peer-reviewed before they are broadly distributed.

The PCO Special Report was not distributed to ministers or the Prime Minister

Ultimately, the PCO Special Report did not go through the PCO governance process and was not distributed to ministers or the Prime Minister.

Ms. Thomas explained that discussion about the PCO Special Report was put on hold because of major events: the Freedom Convoy's arrival in Ottawa on 27 January 2022, and Russia's invasion of Ukraine occurred in February 2022.

Since the NSIA does not formally approve PCO-IAS products before distribution, Ms. Thomas did not think PCO-IAS was waiting for her approval to share the PCO Special Report. She only learned it had not continued through the governance process through the NSICOP and NSIRA reviews.

Ms. Thomas said PCO-IAS had the authority to distribute the PCO Special Report if it had wanted to. PCO-IAS is independent from the NSIA and has the authority to share its assessments as it likes.

Mr. Green said he did not feel comfortable sharing the PCO Special Report any further because of the sensitivity of the issue. However, according to Ms. Thomas, the sensitivity of intelligence did not change the governance process.

The Prime Minister's view of the PCO Special Report

The Prime Minister has now read the PCO Special Report. While some details were new to him, its general contents were not. He described the Report as useful and a good compilation of information that would have been important for someone new to his job. He does not believe that reviewing it sooner would have changed the government's response to foreign interference.

The Targeting Paper

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

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

The Targeting Paper was prepared by a CSIS analyst in 2021, but CSIS did not distribute it until 13 February 2023. The report's classification level made its distribution challenging. In the fall of 2022, considering the public conversation on foreign interference, the author got the support needed to move it out of CSIS, and it was subsequently made available to certain public servants.

The NSIA reviews the Targeting Paper

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

- The distribution list was both relatively extensive and inaccurate. People who no longer held certain positions were still listed. At a time when the government was experiencing significant leaks of classified information, Ms. Thomas was particularly concerned about the size, inaccuracy and currency of the distribution list.
- The paper included the names of individual MPs who were "targeted." This was contrary to the usual CSIS practice of masking names and was occurring at a time when there were significant leaks of information. Sanitization was important because the point of the Targeting Paper was the behaviour of the hostile state actor, not the targets.
- Ms. Thomas had some questions about whether the Targeting Paper was describing foreign interference or legitimate foreign influence and wanted to discuss this with other deputy ministers.

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

Deputy ministers review the Targeting Paper

Accordingly, the Targeting Paper was then discussed at a deputy ministers' meeting on 24 February 2023. They agreed that the distribution list should be reduced and that CSIS should create a less sensitive version, without some information like the names of the MPs.

Distribution of the sanitized Targeting Paper

It seems that there were differing understandings of the intended distribution of the sanitized Targeting Paper – specifically, whether the new version would go to the Prime Minister. CSIS was under the impression that it would. It conveyed this to NSIRA and NSICOP during their reviews. These bodies then concluded that the Targeting Paper was supposed to go to the Prime Minister but did not. NSIRA suggested it was the NSIA who decided not to share the Targeting Paper with the Prime Minister.

Neither NSIRA nor NSICOP had the opportunity to speak with Ms. Thomas, who had retired as NSIA. The Commission had the opportunity to hear from her.

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

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

David Vigneault, CSIS Director at the time, only learned through the NSIRA and NSICOP review processes that the sanitized version had not been distributed. He told the Commission that he understood from the NSIRA and NSICOP reports that Ms. Thomas had decided not to share the paper with the Prime Minister because she determined the conduct described was more legitimate diplomatic effort than foreign interference. However, he acknowledged he had no personal knowledge of this – his source of information was the NSIRA and NSICOP reports.

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

My understanding of the evidence is that the NSIA never decided that the material should not be provided to the Prime Minister. She just never received the revised version.

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

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

Differing perspectives on foreign influence vs foreign interference

I also find there were different perspectives about the Targeting Paper's significance, and, in particular, whether some or all the activities described in it were foreign interference or legitimate diplomatic activity.

Multiple witnesses testified that the practice of creating different lists of legislators based on their positions on certain issues is commonplace diplomacy. The fact of creating or keeping a list of legislators is not in itself foreign interference; what matters are the reasons for making such a list and the use to which it will be put, which are very difficult to determine. Ms. Thomas said that convincing parliamentarians to vote in favour of another country's interest or change their vote or opinion on an issue is not necessarily foreign interference. She said Canada's diplomats regularly engage in similar behaviour.

According to Mr. Morrison, Deputy Minister of Foreign Affairs, the concept of "target" lists is normal in the world of diplomacy. The issue is not the existence of this type of list, but rather how such lists are used. The Targeting Paper did not involve information about threats to individuals.

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

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

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

The Prime Minister reviewed the Targeting Paper in the context of the Commission's proceedings. He said it shows that PRC diplomats research and categorize members of Parliament (MPs), which is not particularly revelatory and is part of what diplomats do in every country around the world. Nothing in it altered his perception of the PRC's behaviour, focus or engagement in foreign influence and interference, and the document did not significantly add to his understanding of the situation.

Targeting terminology

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

To any but the most experienced readers of intelligence – and perhaps even to them – this will result in confusion and misunderstandings. For the layperson, "target" will sound very alarming, as it suggests a threat. The intelligence community should make efforts to clarify terms like these and ensure this is communicated to the reader.

Uyghur Motion

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

In the aftermath, Canada and the PRC engaged in "tit for tat" sanctioning.

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

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

Flow of intelligence within government

Prior to May 2021, CSIS distributed intelligence products about the PRC's interest in MPs, including Mr. Chong and Mr. Chiu, to Mr. Blair, then the Minister of Public Safety. CSIS used the Canadian Top Secret Network (CTSN) to email the products to the named recipients. Three of these products reference Mr. Chong.

Intelligence, collected at various times, indicates that:

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

Mr. Blair testified that he never received the three intelligence products disseminated prior to May 2021 referencing Mr. Chong. It happened during the pandemic, and he was no longer receiving classified information sent over CTSN. Other senior officials could not remember whether they had received or read these reports at the time.

In response to the intelligence, CSIS decided to provide defensive briefings to the MPs to sensitize them to PRC foreign interference. CSIS sent, again via CTSN, a 31 May 2021 Issues Management Note ("**IMU**"), explaining its plan for the defensive briefings. The IMU said both MPs were targets of PRC foreign interference threat actors and that the PRC's interest in Mr. Chong included interest in his relatives who may be in the PRC.

Again, Minister Blair testified that he never received this material and others could not remember whether they received or read these reports at the time.

On 20 July 2021, CSIS issued a lengthy intelligence assessment on PRC foreign interference in Canada. This product was distributed more broadly throughout the national security and intelligence community. It briefly mentioned the above intelligence about the PRC's interest in Mr. Chong but did not mention him by name.

Government response to the intelligence

Prior to the enactment of the *Countering Foreign Interference Act*, CSIS could only have shared classified information with Mr. Chong under its threat reduction measures (TRM) authority. CSIS concluded in 2021 that the threshold to conduct a TRM was not met here, as it did not have reasonable grounds to believe that the PRC's activity amounted to a threat.

CSIS provided Mr. Chong an unclassified defensive briefing in June 2021 and had subsequent discussions with him following that briefing. In those encounters, CSIS did not reveal the intelligence about the PRC's interest in him. In CSIS's view, the interactions with Mr. Chong were positive, and he was aware of the risks of foreign interference.

As mentioned above, on 1 May 2023, the *Globe and Mail* article based on allegedly leaked CSIS intelligence came out.

On 2 May 2023, the Prime Minister, then-NSIA Ms. Thomas and then-CSIS Director Vigneault met with Mr. Chong to discuss the news article.

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

Mr. Vigneault told Mr. Chong that the media reports did not accurately reflect CSIS's 2021 assessment. There was no information suggesting a risk of physical harm to Mr. Chong or his family. Importantly, he told Mr. Chong that the media's understanding of the word "target" in the intelligence reports did not align with CSIS's use of the term.

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

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

Mr. Morrison said merely researching politicians is not foreign interference. It is something all diplomats do. He also said sanctions are common diplomatic practice and can legitimately involve a principal's family.

Mr. Vigneault told me that the media reporting sensationalized the intelligence about Mr. Chong and presented information without context. CSIS's assessment was that there was never any physical threat. Mr. Vigneault also noted that there had been several discussions between CSIS and Mr. Chong. While the intelligence was important and resulted in the unclassified defensive briefing, it was not the "biggest red flag ever" the way the media made it seem.

Minister Blair said that after seeing the July 2021 assessment, he had no concerns about anyone's safety. For him, research into an MP for the purpose of sanctions did not raise concerns. Canada also imposes sanctions on foreign nationals.

Mr. LeBlanc who was the Minister of Public Safety from 2023 to December 2024, said in his view open source research was different from the public discourse of a "threat." His understanding from a meeting with CSIS in May 2023 discussing the incident was that there was some distance between CSIS's explanation about the research and what Mr. Chong and others saw as threats.

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

Conclusions

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

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

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

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

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

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

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

A warrant

I received evidence about an application for a CSIS warrant that then-Minister of Public Safety Bill Blair approved for submission to the Federal Court in 2021. There was a very significant delay between when Public Safety sent the application to the Minister's office and when the Minister approved it.

The *Canadian Security Intelligence Service Act* requires approval of all warrant applications by the Minister of Public Safety.

How the warrant approval process unfolded

On "Day 0" the application was submitted to Public Safety. Then-CSIS Director Vigneault recommended the Minister approve the application within six days. CSIS generally builds in 10 days for the Minister to review and approve warrant applications. Typically, the expectation is that it would take one to two weeks to have a warrant application approved by the Minister.

The Deputy Minister of Public Safety at the time, Rob Stewart, said CSIS normally gave fairly tight timelines for ministerial decisions about warrant applications, but these were meant to be instructive, not hard deadlines. During the pandemic, deadlines were more aspirational than real.

Mr. Stewart signed the warrant application on Day 4 in his capacity as Deputy Minister. He then arranged for it to be sent to the Minister's office in Ottawa, with a cover note asking the Minister to approve it that day. The Minister was in Toronto at the time.

According to Mr. Stewart, once the warrant application package was sent to the Minister's office, it was essentially the responsibility of that office and CSIS to coordinate putting it before the Minister.

Zita Astravas, Minister Blair's Chief of Staff at the time, did not remember exactly when she first received the application; she said that it may not have been on Day 4.

As per the usual process, CSIS briefed her on the application before it went to the Minister. This took place on Day 13 ("**Initial Briefing**"). Ms. Astravas asked questions about the warrant. Her questions were about whether the activities described met the threshold to obtain a warrant, and about other information underlying the application.

Ms. Astravas said these questions were for her information. She did not intend to convey that the warrant was at risk of not being approved until her questions were answered. Michelle Tessier, CSIS's Deputy Director of Operations at the time, who was present at the Initial Briefing, testified that she did not interpret her questions as indicating a risk the warrant would not be approved.

In an internal CSIS email, the individual who signed the affidavit supporting the warrant application (i.e. the affiant), who was also present at the Initial Briefing, but who did not testify before me, seemed to have had a different impression. They wrote in an email that in their view, the application was in danger of not getting signed by the Minister, and it would be necessary to make additional arguments as to why CSIS needed warrant powers. Ms. Tessier testified that she did not agree with the affiant's email.

Between Day 17 and Day 21, CSIS followed up on Ms. Astravas's questions from the Initial briefing. They viewed them as important because these were questions that could very well be asked by the judge reviewing the warrant application.

There is little information in the record about what occurred in the weeks between Day 21 and Day 48, when the CSIS Director discussed the warrant again with Ms. Astravas. Their discussion was about how to manage the complexity of the file in terms of logistics like distribution lists. The Minister's briefing was scheduled approximately one week later, on Day 54.

The Minister's briefing about the warrant application happened on Day 54. Minister Blair reviewed the application in a secure facility, was briefed and approved it that day.

The warrant was presented and issued by the Federal Court approximately three weeks after Day 54.

When did Minister Blair learn about the warrant?

Minister Blair testified that he did not learn that there was a warrant requiring his review until two or three days before his briefing occurred. When he learned he would have to attend a secure facility in Toronto to review a warrant application, he did not know what the warrant was about.

Ms. Astravas agreed that Minister Blair was not aware the warrant application was waiting for his approval until he saw the application on Day 54.

Delay in the warrant approval process

CSIS officials testified that the delay in getting the Minister's signature was highly unusual especially given there had been so much discussion before the application was submitted.

However, neither CSIS nor Public Safety staff raised any concerns about the delay with Minister Blair or Ms. Astravas during the 35-day period between Day 13 (the Initial Briefing) and Day 48 (the discussion between the CSIS Director and Ms. Astravas) or otherwise suggested that it was urgent.

Mr. Vigneault said he was letting the process follow its course and he understood that this was a "more complicated" warrant and was not surprised the Minister was giving the matter "a sober second thought." He only learned in June 2023 that Minister Blair became aware of the warrant application on the day he signed it.

Public Safety officials also never raised the warrant with the Minister after they sent the application to his office. Although Ms. Astravas attended a number of briefings with the Minister and the CSIS Director in classified spaces between days 13 and 54, she did not recall raising this warrant application.

Ms. Astravas explained the length of time for the warrant to be approved by the fact it had not been identified as a priority item by the CSIS Director. She noted that Public Safety was managing several other issues during this time frame: the pandemic, as well as Canada's withdrawal from Afghanistan, border security, gun control, the mass shooting in Nova Scotia, economic security, updating the terrorist organization listing and security risks resulting from 5G technology. Public Safety officials made a similar point.

Minister Blair could not comment on whether the delay was abnormal here; he expected that all officials involved – Ms. Astravas, Mr. Vigneault and Mr. Stewart – ensured that he saw what he needed to see.

Allegations of interference

In internal CSIS email exchanges between Days 13 and 48, the warrant affiant expressed concern about the possibility of interference in the warrant process. Similar concerns were voiced by Participants in the Commission's public hearings. Those concerns are legitimate and understandable given the unusual delay. Furthermore, interference in a warrant application would be very serious.

Ms. Astravas categorically denied having stalled the warrant. She reiterated that she disclosed her relevant personal knowledge to CSIS before the warrant application and when it came to the Minister's office and had also disclosed this to Minister Blair. Mr. Vigneault confirmed that Ms. Astravas disclosed this to him.

Minister Blair said the warrant was never in danger of not being approved, and that he only considered his statutory duties in assessing the application. Both he and Ms. Astravas categorically said they did not tell anyone, including at PCO or the Prime Minister's Office, about the warrant application.

CSIS officials were not under the impression that Minister Blair or Ms. Astravas had any reservations about the warrant. They were quite categorical in dismissing allegations of interference by Ms. Astravas. Mr. Vigneault noted that unless things change drastically in the coming years, if the Minister of Public Safety were to refuse to approve a warrant application for illegitimate reasons, the CSIS Director would know, and it would be extremely problematic.

Conclusions

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

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

What this event shows, however, is that there was an urgent need to put in place a more systematic and stringent process for tracking and keeping a record of warrant applications from the moment they leave CSIS to their submission to the Federal Court. I understand from the evidence offered by Public Safety officials and Mr. LeBlanc, who was until recently Minister of Public Safety, that such a process is now in place.

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

Chapter 15: Information Sharing with Parliamentarians and Political Parties

Informing parliamentarians, their political staff and political parties about foreign interference is an important part of Canada's efforts to protect our democratic institutions.

Unclassified briefings to parliamentarians

Disclosing sensitive information to parliamentarians is not straightforward. Most parliamentarians do not have security clearances. Even if CSIS could provide classified information to them, it would still need to protect sources and methods. Parliamentarians consider they are protected by parliamentary privilege when they speak on the floor of the House of Commons or the

Senate, which means that they might not suffer legal consequences for disclosing classified information. This changes the risk calculation when government must decide whether to share sensitive information with them.

One way the government addresses these considerations is by giving parliamentarians unclassified defensive briefings, also called protective security briefings ("**PSBs**"). Their purpose is to inform recipients about foreign interference in Canada, how to detect it and how to defend against it.

In response to National Security and Intelligence Committee of Parliamentarians (NSICOP) recommendations in 2018 and 2019, CSIS and its government partners began working on a plan to brief all parliamentarians. But unfortunately, and for no good reason, these PSBs were not delivered until June 2024.

I heard that there was some uncertainty within government about whose approval was required. Before providing briefings to all parliamentarians, CSIS sought approval first from the Prime Minister and then from the Minister of Public Safety. However, I also heard that CSIS has the authority to brief members of Parliament (MPs) as it sees fit.

In any case, memoranda from PCO asking the Prime Minister to approve the PSBs never reached him and were never answered. I did not hear any satisfactory explanation as to why.

The first memorandum, from December 2019, fell by the wayside when the COVID-19 pandemic hit and MPs were no longer in Ottawa. The second memorandum, from December 2020, was under discussion for months and was ultimately overtaken by the 2021 election. A third memorandum was prepared in draft form in January 2022 but apparently never finalized.

Nevertheless, in 2021, CSIS went ahead with a campaign to give PSBs to MPs in high priority ridings and to those who could potentially be impacted directly by foreign interference activities.

Ultimately, when the NSICOP *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* was released in 2024, the Prime Minister's Office, the Prime Minister and the National Security and Intelligence Advisor to the Prime Minister (NSIA) discussed briefings to parliamentarians and agreed that they should happen.

In June 2024, briefings were delivered to each caucus. They were high-level and discussed what constitutes foreign interference and why states do it, with examples.

The National Counter Foreign Interference Coordinator (NCFIC) at Public Safety is now responsible for coordinating PSBs to caucuses in the House of Commons and to senators.

Several witnesses said that the failure to start PSBs in 2019 may have had limited impact. They emphasized that the information was at a relatively high-level, and that it was available to parliamentarians from a range of other sources.

Nevertheless, I find the briefings should have happened and I find the explanation about why the Prime Minister's Office did not respond to CSIS's requests for approval unsatisfactory. Many actors believed from as early as 2018 that parliamentarians should be briefed more consistently about foreign interference.

Classified briefings to parliamentarians

Providing classified information to parliamentarians is a very sensitive issue for CSIS because parliamentarians may decide to rely on parliamentary privilege to disclose it. CSIS said it is trying to identify the best ways to address this issue.

As mentioned earlier, CSIS had the authority to provide individuals with classified information in order to reduce threats to the security of Canada under its threat reduction measure (TRM) authority. CSIS has used TRMs to brief individuals about foreign interference. A TRM briefing allows CSIS to provide more specific information than PSBs. This may include classified information, even if the recipient does not have a security clearance.

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

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

Ministerial accountability

Following the media leaks in 2023, the Prime Minister asked the intelligence services to brief four ministers (Minister Blair, Minister Dominic LeBlanc, Minister Joly and former Minister Mendicino) on the relevant intelligence. Witnesses said that there was a recognition at this time that, while the Prime Minister was being briefed on much of this information, other key ministers were either not getting the information in real time or were still, to a certain extent, in the dark about the allegations in the media. Thus, the Clerk started a series of meetings so that these Ministers would be brought up to speed on things that had already been briefed to the Prime Minister and could discuss what to do about it. While this is a small example, it may illustrate a larger issue regarding intelligence flow to ministers.

The Ministerial Directive and Governance Protocol

Following the 2023 media reporting about possible interference by the PRC in Canadian elections, the Prime Minister asked the Minister of Public Safety to issue a directive to CSIS to ensure that all information, regardless of its credibility or reliability, about threats to parliamentarians or their families would be disclosed to them.

CSIS was concerned that information would have to be shared regardless of whether it was corroborated, verified or credible, but the *Ministerial Directive on Threats to the Security of Canada Directed at Parliament and Parliamentarians* ("**Ministerial Directive**") was nevertheless issued quickly.

The Directive instructs CSIS to, wherever possible, "ensure that Parliamentarians are informed of threats to the security of Canada directed at them." This signaled that threats to parliamentarians would not be tolerated.

The Ministerial Directive requires CSIS to act when it becomes aware of a threat. In deciding what to do, CSIS considers the risks of disclosing classified information and any alternatives that may achieve the desired result without such disclosure.

In May 2023, following a speech in the House of Commons by Mr. O'Toole, in which classified information was apparently disclosed, Public Safety and CSIS paused briefings under the Ministerial Directive to develop a Governance Protocol. The Governance Protocol is intended to address CSIS's concerns about disclosing all information about threats to parliamentarians regardless of its reliability and about the risk of MPs relying on their privilege to divulge sensitive information. It now requires extensive consultations within government before CSIS may disclose information under the Ministerial Directive. The Governance Protocol recognizes the possibility for conflicts of interest during this consultation process. It allows deputy ministers to not advise their ministers if doing so could create a potential conflict of interest for the minister.

APT 31 cyber campaign targeting members of the Inter-Parliamentary Alliance on China

Email campaign in 2021

In January 2021, Advanced Persistent Threat 31 ("**APT 31**") conducted an email campaign targeting members of the Inter-Parliamentary Alliance on China ("**IPAC**"), an organization of parliamentarians from around the world who share a common view that the People's Republic of China (PRC) represents a threat that should be dealt with in a stronger and more risk-conscious way. APT 31 sent emails with tracking links to IPAC members. The idea was to get the recipient to open the email, at which point APT 31 could

validate the email and gather certain basic information about the recipient, such as their IP address. This can be a precursor to follow-up activity by a threat actor, including foreign interference activity. It cannot, however, compromise an account or device by itself.

The evidence before me indicates that APT 31 is a group of malicious cyber actors who work at the direction of the PRC's Ministry of State Security. The group is focused on espionage and foreign interference, targeting the governments of many Western countries, including Canada.

Several Canadian parliamentarians are members of IPAC and were sent emails by APT 31. They first learned of it in the spring of 2024. This incident, and the absence of communication to parliamentarians about it, raises questions about whether the parliamentarians targeted ought to have been informed earlier about the email campaign and, if so, who was responsible for telling them.

The nature of the threat

APT 31 activities have been consistent with espionage and intelligence collection that seeks to provide an economic or diplomatic advantage. Therefore, CSE has previously assessed this type of activity through the lens of espionage and not foreign interference. GAC similarly views APT 31's cyber activities as espionage, which is not necessarily viewed as contrary to international norms. Its legality is a complex legal question, and beyond the scope of the Commission's mandate.

However, while espionage is not necessarily foreign interference, information obtained through espionage could be used to carry out foreign interference activities. Determining the intent behind this type of cyber activity can be difficult but there was no indication that it was done to directly interfere in democratic processes. However, a malicious email can be a means to securing a foothold on a network.

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

CSE's Canadian Centre for Cyber Security (CCCS) emailed an unclassified Cyber Event Report to House of Commons IT ("**House IT**") officials on 22 January 2021. The report stated that emails with tracking links had been sent to parliamentary email accounts, provided technical information and recommended that House IT take certain steps in response. The report did not attribute the activities to APT 31, as this was classified information.

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

A little less than a month later, CCCS and CSIS met with House IT to deliver a Secret level classified briefing. Agency officials told House IT that they suspected APT 31 was responsible for the email campaign and briefed House IT on APT 31's suspected links to the PRC, its tactics and its historical targets. This meeting took time to organize because of the impact of the pandemic on organizing and holding classified meetings.

Neither House IT nor CCCS informed the Senate of APT 31's involvement at this time. The Senate only learned of APT 31's involvement in April 2024 from the media, and then subsequently in May or June 2024 from House of Commons officials.

Should parliamentarians have been notified?

I heard a range of views about whether MPs should have been notified in 2021 of the APT 31 campaign.

As targets of the email campaign, MPs and IPAC national co-chairs John McKay and Garnett Genuis felt that they should have been notified.

Moreover, both the Chief of CSE and the NSIA viewed the campaign as the type of activity intended to be captured by the Ministerial Directive (which was not in force in 2021). This suggests that the APT 31 campaign was something that parliamentarians should have been briefed about.

As for CSIS, it said that if a similar campaign occurred today, there would likely have to be a discussion between it, CCCS and House of Commons officials about whether to inform MPs.

However, witnesses from House IT said since there are hundreds of millions of cyber attacks in a year, briefing on all of them would be operationally impracticable. House IT did not inform MPs about APT 31 because the campaign had been unsuccessful.

Who is responsible for notifying parliamentarians of a cyber threat?

The APT 31 incident speaks to the broader issue of who was, and who currently is, responsible for informing parliamentarians of this type of cyber threat. The evidence suggests that, at the time of the email campaign, it was unclear who was responsible.

I heard from several witnesses that this issue would not arise today since, if CSE identified intelligence about a threat to parliamentarians, it would go through the Ministerial Directive and Governance Protocol. However, CSE witnesses told me that under the Ministerial Directive, CSE would not likely brief individuals. It remains within the authority of CSE's clients to determine what measures, including briefing a parliamentarian, they can take within their own authorities. CSE ordinarily provides classified information to security-cleared IT service providers or provides them with steps to take.

Providing CSE or other departments with additional authorities to engage parliamentarians may still be worth considering. While it is clear that CSIS has the authority to engage with parliamentarians about threats, it is less clear if other departments can do so. Nevertheless, CSIS told me if it learns of a threat from CSE, CSIS will ensure there is a discussion to determine if parliamentarians should be informed and by whom.

Briefing political party representatives during elections

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

The Security and Intelligence Threats to Elections Task Force (SITE TF) offered Secret level briefings to security-cleared representatives of the Conservative Party, Liberal Party and NDP for both the 2019 and 2021 general elections. These briefings provided a bit more information than could be found in publicly available sources and open communications so that if political parties had concerns, they could tell the SITE TF.

The government has also offered unclassified briefings to political parties.

Classified briefings to political party leaders

The leaders of political parties have unique powers and responsibilities within Canada's democratic system, which may give them a special role to play in responding to foreign interference. Several witnesses said leaders had potential tools to address foreign interference targeting parliamentarians. For example, a party leader can remove an MP from positions of power (other than their status as an MP) or avoid putting them there in the first place. Leaders can also discuss concerns with parliamentarians.

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

For the party that forms government, giving such intelligence to the party leader is possible since the prime minister can be briefed as necessary. However, it is more complicated when the intelligence concerns an opposition MP or candidate.

Merely giving opposition parties access to intelligence is not as simple as it sounds. One challenge is that providing classified information to party leaders, who are often sitting MPs, comes with the risks that I discussed earlier about sharing classified material with parliamentarians.

There are also challenges for party leaders who receive intelligence, particularly if they are told that, due to secrecy concerns, there are limits to how they can use it.

Even when something can be done, having sensitive intelligence about an MP can put a leader in a challenging position because any decision affecting the MP may have to be made without providing them with due process. Further, significant suspicion could arise from the unexplained removal of a candidate from a ballot or caucus. That said, taking action may be prudent, even if it is unfair. It all depends on the specific circumstances.

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

Briefing opposition leaders

Currently, briefings to opposition leaders are given on an *ad hoc* basis. However, PCO is now finalizing a protocol for regular classified briefings to leaders of all recognized parties. I heard that it poses a challenge for the government if a party leader does not have a security clearance.

In May of 2023, opposition leaders were offered the opportunity to obtain Top Secret security clearances. Leaders of the Green Party, NDP and Bloc Québécois now have Top Secret clearance. While the Leader of the Conservative Party has declined to apply for such a clearance, his Chief of Staff has obtained one.

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

Discussions continue within government about how to bring intelligence reporting of foreign interference, including disinformation, to the attention of a political party. I heard that, in May 2024, PCO was preparing to share a protocol to provide regular classified briefings to the leaders of all political parties with representation in the House of Commons at least twice a year. These would be in addition to *ad hoc* briefings.

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

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

Chapter 16: Information Sharing Outside of the Federal Government

Engaging with other levels of government in Canada

Foreign interference does not simply target federal institutions and processes. Foreign actors target institutions at every governmental level in Canada. Provincial, territorial, Indigenous and municipal governments are therefore important in a whole-of-society response to foreign interference. There is a shared interest in building resiliency and a healthy democracy and ensuring that Canada has free and fair elections at all levels. A wide range of federal government entities are making efforts to engage with provinces, territories, Indigenous governments and municipalities in relation to foreign interference.

Collaboration is essential, even if it can sometimes be difficult, such as when sharing classified information. Even though the *Countering Foreign Interference Act* is expected to facilitate the information flow between security agencies and subnational government officials, challenges remain. One of these is that non-federal governments do not have the infrastructure and capacity to process and store classified information.

I note, however, that the government is currently seeking to build information-sharing networks and has offered communications systems for provinces and territories up to the Secret level. In the meantime, however, challenges remain.

Engaging with the public

All federal agencies and departments who testified emphasized that public outreach was a key component of a whole-of-society response to counter foreign interference.

The government, including its national security, intelligence and law enforcement agencies, is now trying to engage with the public, including diaspora communities, in a variety of ways both informally and formally.

However, public engagement will continue to present serious challenges, particularly when members of the public want to receive more specific information but are not security-cleared and do not have a "need-to-know." Thus, in practice, sharing information with the public will likely have to be done at the unclassified level. I heard testimony about work being done to ensure that government produces more information at the unclassified level to facilitate this.

These are good intentions, but a more formal and organized plan is needed. Up until now, communication with the public has, in my view, been lacking.

The importance of building public trust was a constant theme in the evidence before me, especially in relation to Canadian diaspora communities. CSIS witnesses acknowledged that the agency must overcome distrust from diaspora communities, which may stem from problematic treatment in the past by law enforcement or security agencies in Canada.

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

Building trust is a particularly relevant consideration to keep in mind when considering transnational repression, which the next part of this report summary addresses.

Chapter 17: Transnational Repression

There is currently no legal definition of transnational repression in Canada. It has been described as foreign state activity to monitor, intimidate and harass diaspora communities to achieve foreign state objectives.

Government witnesses recognized the seriousness of the threat that transnational repression poses to diaspora communities, the Canadian public and Canadian society overall. I agree. It would be challenging to overstate its seriousness, or the impact it has on individuals and our social

fabric. Transnational repression threatens individuals' freedom to engage in legitimate democratic practices and threatens to undermine democratic society and the sovereignty of states.

Government witnesses described it as one of the most prevalent types of foreign interference, as the real foreign interference threat to Canada (rather than the targeting of parliamentarians that has garnered so much public attention) and as one of the greatest strategic challenges to Canada's sovereignty and democracy.

Not all transnational repression activities fall within my mandate. However, the Commission's Terms of Reference direct me to examine and assess supports in place for members of vulnerable diaspora communities who may be victims of foreign interference in Canada's democratic processes. In the course of my work, I received evidence related to transnational repression.

Transnational repression threat actors and their tactics

Assessing the extent of transnational repression in Canada is difficult. Targeted individuals are often reluctant to report their experiences. People may fear reprisals against individuals or their relatives abroad if they speak out. In addition, many targeted people come from communities who, for both cultural and historical reasons, may distrust law enforcement and security agencies.

I discuss the evidence that I can make public. These examples are not exhaustive and should not be read as indicating that other countries are not active in perpetrating transnational repression in Canada:

- **Iran**. The government assesses Iran as a considerable transnational threat because it is likely monitoring, influencing, collecting information on, harassing and intimidating the Iranian diaspora community to prevent criticism of Iran.
- **The People's Republic of China (PRC).** The PRC targets members of Chinese Canadian diaspora communities for the purposes of repression, influence and forced return of targeted individuals to the PRC. It deploys a wide range of tradecraft to carry out its activities, one of which is to use a person's family and friends living in the PRC as leverage against them. The PRC uses its diplomatic missions, PRC international students, community organizations and private individuals, among others, to carry out its transnational repression activities.
- **India.** India's activities primarily target the approximately 800,000 members of the Sikh diaspora in Canada and aim to promote a pro-India and anti-Khalistan narrative. The RCMP's statement in October 2024, on violent criminal activity in Canada, including homicides and extortion, with connections to agents of the Government of India, is consistent with the classified evidence. Further, the national security and intelligence community assesses India as an emerging cyber threat actor.

How Canada responds to transnational repression

Canada's efforts to counter transnational repression are wide ranging and come from different sectors within government:

- The National Counter Foreign Interference Coordinator is bringing a transnational repression action plan to the Deputy Minister of Public Safety for consideration and Public Safety has re-established the "Cross-Cultural Roundtable."
- CSIS has established a hotline for anonymous reporting on foreign interference.
- GAC has frequently raised foreign interference in its diplomatic engagements with certain countries, including the PRC.
- Canadian Heritage's Digital Citizen Initiative has funded projects to understand PRC transnational repression in Canada.
- Elections Canada has published voting guides available in 51 languages and engages with diaspora communities through various mechanisms.
- While CSE does not have a domestic mandate, some of its cyber operations have repercussions for transnational repression. CSE also works with global and federal partners to mitigate risks posed by transnational repression.
- The government works with international partners (for example, at G7 summits) to discuss global responses to transnational repression.

Specific examples of transnational repression in Canada

I received evidence on several notable examples of transnational repression in Canada that, while not necessarily directly related to democratic institutions, provided important insight into the kinds of clandestine and threatening activities foreign states are engaged in. I discuss two examples.

PRC overseas police stations

In September 2022, the Spanish non-governmental organization Safeguard Defenders published a report alleging that so-called overseas police stations were used by the PRC to harass, intimidate and punish individuals around the globe with the aim of returning "fugitives" to the PRC.

But overseas police stations also performed functions not directly related to transnational repression, including administrative services like driver license renewals. While this was a violation of the *Vienna Convention on Consular Relations*, it illustrates how local organizations, integrated into the community, can be used as effective tools for the PRC to engage in transnational repression under the guise of providing useful services.

The overseas police stations presented challenges to the government's ability to use traditional tools to respond. Certain operations were run by Canadian citizens, so expelling those responsible from Canada was not an option.

The RCMP responded instead by using disruption tactics. They deployed uniformed officers to the stations to make their presence known and engaged with the local community directly and through published materials.

Opinions on the RCMP's actions diverged. For example, one community member described it as irresponsible and damaging to vital community institutions. Conversely, one of the Commission's Participants suggested to RCMP witnesses that the response was too "diplomatic," and therefore distinguishable from how the RCMP responds to organized crime.

The assassination of Hardeep Singh Nijjar

On 18 June 2023, Hardeep Singh Nijjar was killed in British Columbia. The initial assessment of Canada's security and intelligence agencies was that this was gang or criminal activity, and the Prime Minister Trudeau was informed of this. Over the course of the summer, however, intelligence revealed India's involvement. The Prime Minister was promptly briefed on the updated assessment.

The government wanted India to acknowledge its involvement in the killing but also needed a pragmatic approach to resolve the issue. The Prime Minister testified that the immediate approach was to engage with India and communicate the need for the two countries to work together while ensuring there was accountability. Canada also reached out to its allies to ensure a collective and coherent response. A number of meetings took place between the National Security and Intelligence Advisor to the Prime Minister (NSIA), the CSIS Director, the Deputy Minister of Foreign Affairs and their Indian counterparts in August and September 2023. India did not acknowledge that it was involved in Mr. Nijjar's killing.

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

India responded not only by declaring a Canadian official *persona non grata*, but by lifting the diplomatic immunity of a further 41 Canadian diplomats in India, effectively expelling them. India may also have launched a disinformation campaign against the Prime Minister.

The question of Indian transnational repression further evolved in a rather dramatic fashion during the Commission's public hearings in the fall of 2024. On 14 October 2024, the RCMP publicly released findings about agents of the Government of India being involved in serious criminal activity in Canada. Simultaneously, GAC announced that Canada had expelled six Indian diplomats and consular officials in relation to a targeted campaign against Canadian citizens by agents linked to India. These individuals were identified as persons of interest in the killing of Mr. Nijjar.

The Prime Minister said the decision to make this announcement was anchored in public safety considerations. Its objectives were to disrupt both the chain of criminal activities with ties to India, which primarily target the Sikh community in Canada, and also the covert collection of information by Indian diplomats about Canadians opposed to the Government of Narendra Modi.

My terms of reference did not allow for an in-depth study of transnational repression in Canada. Thus, the work that the Commission did in this respect likely only scratched the surface of this phenomenon. What this work has made clear to me, however, is how serious a problem transnational repression is, how harmful its impacts are on individuals in Canada and how important it is for the government to meaningfully respond to it.

Any effective response to foreign interference must consider the realities of transnational repression in Canada.

In the next chapter, I address the part of my mandate that flowed from the 2024 NSICOP *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* ("**NSICOP Report**").

Chapter 18: The NSICOP Report

On 3 June 2024, a redacted public version of the NSICOP Report on foreign interference was published. It was the culmination of a significant amount of very important work. It is an impressive and detailed synthesis of a vast amount of information. And it has made a considerable and valuable contribution to advancing public awareness of foreign interference.

The NSICOP Report's impact on the discussion surrounding foreign interference was immediate, as it contained assertions that some elected officials were "semi-wittingly" or "wittingly" assisting foreign interference efforts. These statements led to significant concern in the media, the public and in the halls of Parliament itself.

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

The Commission reviewed the classified version of the NSICOP Report and the intelligence that NSICOP considered. It also requested and reviewed considerable additional information that NSICOP did not have, including the raw intelligence and operational reporting underlying the allegations. The Commission obtained further written information from the Government of Canada and conducted *in camera* examinations of CSIS representatives and senior Privy Council Office officials.

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

Further, the Commission's mandate was not to attempt to expose and identify specific individuals or organizations as alleged foreign interference agents. My mandate did not include passing judgment on the culpability of any elected official. Indeed, judging the culpability of an elected official or of any other person would violate the Commission's legal obligations and the requirements of procedural fairness.

What I learned from the Commission's investigation was both surprising and insightful. The most important observations I made had to do with the nature of intelligence – what it is, and what it is not, how it should be used, and how it should not.[19]

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

The NSICOP Report made strongly worded and unequivocally stated allegations against individual parliamentarians. These assertions had the (perhaps unintended) effect of causing widespread public consternation, casting a cloud of suspicion over all parliamentarians and contributing to the erosion of Canadians' trust in their democratic institutions.

The Commission's investigation led me to conclude that the consternation caused by the NSICOP Report, while understandable, is in some important respects unwarranted. The situation is perhaps not as clear-cut, nor as extreme, as the fears provoked by the NSICOP Report would suggest.

---

[19] For general context and background about the nature of intelligence and its limitations see Volume 2, Chapter 5.

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

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

NSICOP has made an important contribution to raising the profile of, and advancing, public discussion over foreign interference. It provided Canadians with a significant amount of information about this topic. Indeed, I note that most of the information in the NSICOP Report did not relate to allegations about specific parliamentarians.

Unfortunately, the comments about parliamentarians attracted the greatest public attention, with troubling consequences. This is particularly true for members of Parliament who are members of certain diaspora communities. For instance, I heard evidence from Jenny Kwan – herself an alleged victim of foreign interference – that the NSICOP Report had cast a cloud of suspicion on parliamentarians. As Ms. Kwan explained, the issue with the cloud of suspicion, beyond the personal ramifications, is that the integrity of Parliament itself is called into question. And undermining democratic institutions and elected officials is exactly what threat actors want.

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

Volume 6: The Public Consultation Process

An important part of the Commission's mandate was to examine and report on the experiences of members of diaspora communities across Canada who may be especially vulnerable to foreign interference.

Contributions from members of the Canadian public, including those who identify as members of diaspora communities, provided crucial input to the Commission, and helped contextualize the phenomenon of foreign interference. At a human level, the information I received through the public consultation process also illustrated the impacts that foreign interference

may have on the daily lives of many individuals and communities in our society.

Below is a very brief overview of the information the Commission received to give readers an understanding of how foreign interference, in particular transnational repression, is deployed against people in Canada.

Use of the public consultation information

What I heard during the Commission's public consultation process was information rather than evidence. It was not provided under oath or further to a solemn promise to tell the truth. Moreover, this information was not tested by cross-examination, and the Commission did not independently verify it.

I want to stress, however, that although not evidence, this information was crucial to the Commission's investigation, as well as to the formation of my recommendations.

Who I heard from

The Commission heard from a broad range of individuals. They were from every Canadian province and ages ranged from 16 to over 80. Information came from individuals and groups who self-identified as belonging to a number of diaspora communities, including Chinese, Eritrean, Ethiopian, Falun Gong, Hong Kong, Indian, Iranian, Russian, Rwandan, Sikh, Taiwanese, Tamil, Tigrayan, Tibetan, Ukrainian and others.

What I heard – transnational repression and foreign interference

Foreign interference targeting members of the Canadian public, and in particular diaspora communities, has three characteristics: its severity, its impact on people and Canadian society more generally and its prevalence.

Severity

The breadth of incidents attributed to foreign state actors and their proxies range in scope, severity and intensity. A substantial proportion of the incidents can be qualified as very severe and shocking.

Threats take multiple forms, including threats of physical and sexual violence, and even threats to life, and are perpetrated in Canada and abroad, in person or online.

Foreign interference also took the form of harassment, exclusion and shunning of activists and dissidents within diaspora communities, attacks on reputations and defamatory campaigns.

Another recurring theme was the monitoring of individuals in Canada either by physical or electronic surveillance.

Finally, some people indicated they were denied consular services from foreign state consulates and embassies because of their criticism, or perceived criticism, of those states.

Impact on people and Canadian Society

I heard that because of foreign interference, individuals live in fear for themselves or their loved ones, leaving them feeling unable to freely exercise their rights and freedoms in Canada, including freedom of expression, freedom of assembly and protest, religious freedom and their right to engage in Canadian democratic life and electoral processes.

On a societal level, participants explained that their confidence in Canada's democracy and electoral processes had been reduced by the fact that some within society cannot enjoy their rights and freedoms to their fullest extent.

Prevalence

Information received through the public consultation process reflected the fact that, for many diaspora community members, foreign interference, often in the form of transnational repression, is a daily reality.

People also told me that the tactics used by foreign states and their proxies are varied and evolving. These tactics are often a reflection of the complex and nuanced sociocultural, political and economic forces at play in the foreign states. We also heard that experiences of diaspora community members vary significantly, even within the same ethnic or cultural community.

Another issue is the pervasive nature of some foreign interference threats impacting crucial spaces such as community organizations, religious and spiritual communities, artistic and cultural spaces and academic institutions, among others.

Conclusions

The public's engagement in the consultation process showed a strong willingness to contribute to a whole-of-society approach to address foreign interference. This willingness can be a great advantage in Canada's ongoing efforts if conditions are put in place to enable this participation.

The government must continue to involve individuals, groups and communities in a whole-of-society approach to addressing foreign interference, especially transnational repression. Facilitating the involvement of individuals and groups, including those directly impacted, will be crucial to Canada's ongoing efforts to detect, deter and counter foreign interference.

Conclusions on Government's Capacity to Detect, Deter and Counter Foreign Interference

The Order in Council establishing the Commission first directed me to examine and assess interference by China, Russia and other foreign states or non-state actors, including any potential impacts, in order to confirm the integrity of, and any impacts on, the 43rd and 44th general elections (the 2019 and 2021 elections) at the national and electoral district levels.

This examination was carried out mainly during the first phase of the Commission's work. As a result of this work, I concluded in my Initial Report that the 2019 and 2021 general elections were without a doubt subject to foreign interference. However, I found that this interference did not undermine the integrity of the electoral system itself, nor did it have any bearing on which party came to power. While it was difficult to ascertain whether or not this interference had any bearing on results of elections at the riding level, I acknowledged the possibility that it did, but only in a small number of ridings.

The Commission's work since the tabling of the Initial Report has not altered these conclusions. Nor has it led me to alter my conclusion that foreign interference had an impact on the electoral ecosystem as a whole and has undermined public confidence in Canadian democracy. Indeed, my work since the initial report has only reinforced this conclusion.

The Order in Council also directed me to examine and assess the flow of information to senior decision-makers, including elected officials, and between the Security and Intelligence Threats to Elections Task Force ("**SITE TF**") and the Critical Election Incident Public Protocol panel during the election periods leading up to the 43rd and 44th general elections, in the weeks following those periods and actions taken in response. I have done this.

The evidence presented to me did not reveal any particular issues with the way in which information flowed during these periods. With the exception of one report that was not passed on to the SITE TF in a timely fashion, the way in which information flowed was satisfactory.

The Order in Council also directed me to examine and assess the capacity of relevant federal departments, agencies, institutional structures and governance processes to permit the Government of Canada to detect, deter and counter any form of foreign interference directly or indirectly targeting Canada's democratic processes, including:

- the creation, sharing, assessment and distribution of intelligence and the formulation of advice to senior decision-makers, including elected officials
- the supports and protections in place for members of a diaspora who may be especially vulnerable and may be the first victims of foreign interference in Canada's democratic processes
- the mechanisms that were in place to protect the integrity of the 43rd and 44th general elections from foreign interference as compared to those in place in previous recent federal elections that I determined to be relevant.

My review has shown that some of the processes through which intelligence was supposed to be passed to senior officials had some shortcomings. Information that should have reached ministers and even the Prime Minister did not. I was unable to ascertain from the evidence exactly why this happened in each case. The evidence did show, however, that the systems in place at the time were not particularly robust. There was no way of knowing who had received a particular report, whether those who had received it had read it and whether any action had been taken as a result.

In some cases, the impression that emerges from the evidence is that the various persons involved in the process felt they had fulfilled their duties as soon as they had delivered the information, without otherwise making sure that it had been received and understood.

I have no evidence to suggest that anyone acted in bad faith. The shortcomings observed appear to have been systemic ones, the consequences of which were exacerbated by various external factors, including the COVID-19 pandemic, which required a significant reorganization of work. Clearly, this reorganization of government work was in several ways less than optimal.

Fortunately, the intelligence delivery system has since been completely redesigned. I have not been able to put this new system to the test to see how effective and resilient it is, but the evidence suggests that it is much more suitable than the previous one. In my view, the government will have to monitor the system very closely and measure its effectiveness on a regular basis.

Of course, when information did not reach the person who would have been in a position to act on it, I could not assess the adequacy of any government response to it. If information does not reach a decision-maker, it cannot be acted upon.

I was nevertheless able to examine and assess several measures taken in response to information that was received relating to foreign interference. My observation is that the significance attributed to this information has fluctuated significantly over the years, indicating that the government has been slow to fully recognize the threat posed by foreign interference to Canadian democratic processes and institutions.

The government apparatus has reacted much more swiftly in recent years, although it still has some way to go. Governments, because of their size, are not generally known for their ability to react quickly. I appreciate that. Nevertheless, foreign interference is an increasingly prevalent and rapidly evolving phenomenon. The government needs to find ways of reacting more swiftly. The restructuring the government has undertaken of its national security governance system, which has reduced the number of committees directly engaged in combating foreign interference from approximately a dozen to five, is a step in the right direction. But it is also important not to let endless discussions and consultations get in the way of action. The machinery of government must facilitate action, not paralyze it. Among the various measures put in place by the government, the establishment of a National Counter Foreign Interference Coordinator should, I hope, go a long way towards achieving this.

As part of my assessment of the government's ability to detect, deter and counter foreign interference in democratic processes, my mandate required me to examine the mechanisms in place to protect the integrity of the 43rd and 44th general elections from foreign interference, compared with those in place to protect the integrity of previous federal elections. I should mention that it was difficult to conduct this comparative review. Aside from some mechanisms to protect electoral infrastructure, there were virtually no specific measures to protect electoral processes from foreign interference prior to 2017.

Indeed, I gathered from the evidence that it was in the wake of allegations of foreign interference in the US presidential election in 2016, the UK's Brexit referendum on European Union membership in 2016 and the French presidential election in 2017, that Canada began to take a more active interest in foreign interference in democratic processes.

The government of the day acted rather swiftly back in 2017, when the Prime Minister tasked the then Minister of Democratic Institutions with leading the government's efforts to defend Canada's electoral process against cyber threats.

In 2018, the G7 countries, meeting in Charlevoix, agreed to establish the G7 Rapid Response Mechanism to strengthen coordination and better detect threats to democracies. Canada acts as its permanent secretariat.

In 2019, the Plan to Protect Canada's Democracy was announced and implemented. In my opinion, this initiative marks a significant milestone as it both recognizes the risk that our elections might be the target of foreign interference and specifically addresses that risk. The plan was not perfect, but it has since been regularly reviewed and improved, and continues to be used to protect our democratic processes and institutions from foreign interference.

My review of the resources available to the government, with a particular focus on those available to the intelligence community, also leads me to conclude that Canada has the means necessary to detect, deter and counter foreign interference. Some of these means can be improved, of course, but they do exist.

This does not mean, however, that the fight against foreign interference has been won. In fact, it is likely to be an endless fight, as the states that seek to interfere in democracies, including our own, are sophisticated actors who constantly refine their methods.

I also note from the evidence that this threat has evolved and now rears its ugly head through disinformation campaigns in the media and on social networks. This emerging trend is quite concerning because disinformation is especially challenging to combat, and efforts to regulate social media platforms to curb it have been unsuccessful so far. Canada needs to reflect on this threat and find ways of dealing with it. This will probably require a great deal of cooperation between democracies around the world.

In short, the fight against fight foreign interference requires relentless effort and perseverance. Trust in our democracy depends on it.

In this Final Report, I make a number of recommendations that I hope will also help improve Canada's ability to detect, deter and counter foreign interference.

Finally, I would like to reiterate what I have already said at various points in the Final Report: transnational repression is a scourge that extends beyond the Commission's mandate. It is, however, a form of foreign interference that the government must quickly address. While the government has been doing so for some time, it needs to ramp up its efforts.

List of Recommendations

The recommendations I believe can and should be implemented promptly, perhaps even before the next election, are identified with this visual:

Intelligence

1 The Canadian Security Intelligence Service (CSIS) should develop mechanisms to clearly flag reports that it views as particularly relevant for some or all senior decision-makers and advisors. CSIS should also clearly flag reports that it views as time sensitive.

CSIS should be more judicious in the type and number of reports it flags as particularly relevant for senior decision-makers and advisors, to ensure that the flag is meaningful.

CSIS reports intended for senior decision-makers and advisors should include a concise and direct executive summary using precise, non-technical language. The executive summary should include any assessment CSIS has made.

The reliability of the intelligence in reports should be addressed candidly and directly, report by report, rather than relying on broad, standardized caveats that do not adequately inform readers of issues related to the reliability of intelligence in reports. Any doubts as to the reliability of the information should be clearly indicated.

When CSIS concludes that intelligence must be brought to the political level, it should recommend that an oral briefing be arranged, and send an oral report containing this recommendation to the client.

2 Intelligence collectors should encourage their regular intelligence clients, such as the Privy Council Office, Public Safety Canada and Global Affairs Canada, to provide feedback on the intelligence they receive, whether by using existing feedback mechanisms and channels or by creating new ones.

3 Agencies that share intelligence with non-traditional security partners should increase their use of open source information. They should also place greater emphasis on producing relevant products that, even if they originate from classified information, are "written to release" so that they may be published and shared at a lower level of classification or at an unclassified level.

4 The government, with the national security and intelligence community, should prioritize developing a declassification system that allows the government to make certain information public where it is in the public interest and where it would not unduly prejudice national security.

5 The Privy Council Office should convene the national security and intelligence community to develop a protocol that governs the collection, handling and dissemination of intelligence about foreign interference targeting political institutions and actors. This protocol should address, *inter alia*, the sharing of intelligence about opposition parties with the governing party. It should also address sharing intelligence with other levels of government in Canada.

The National Security and Intelligence Advisor to the Prime Minister

6 Prime ministers should continue to set out the National Security and Intelligence Advisor to the Prime Minister (NSIA)'s role and responsibilities in a public document. This should occur with the formation of every new government and on the appointment of every new NSIA.

Clarifying coordination roles

7 Clarify the respective roles and responsibilities of the Privy Council Office and Public Safety Canada regarding policy and operational coordination in relation to foreign interference.

Foreign interference strategy

8 The government should make it a priority to develop a whole-of-government Foreign Interference Strategy and provide a public timeline for its completion. This strategy should be integrated into a renewed National Security Strategy.

Communications strategy

9 Develop a government-wide communications strategy to publicize the measures taken and mechanisms in place to protect our democratic institutions and processes from foreign interference.

Awareness of the domestic online information environment

10 The government should develop a legislative framework to authorize collecting and assessing open source domestic intelligence in a way that respects the privacy rights of Canadians.

11 The government should consider creating a government entity to monitor the domestic open source online information environment for misinformation and disinformation that could impact Canadian democratic processes. The entity should be structured to comply with applicable law. The entity should have the authority to give and receive intelligence and information. It would do this with national security and intelligence agencies and international partners as well as with appropriate civil society or private organizations. Giving the entity authority to interact with social media platforms should also be considered. This entity should sit on the Security and Intelligence Threats to Elections Task Force. The expertise acquired by the Rapid Response Mechanism Canada over the years should be shared with this entity.

The Critical Election Incident Public Protocol and the Panel of Five

12 The government should publicize the Panel of Five's existence, as well as the process it uses to decide whether the Critical Election Incident Public Protocol (CEIPP) threshold is met.

13 The CEIPP should set out the central elements of the Panel of Five's decision-making processes and the factors that it considers in determining whether the threshold has been met. This information should be made public. The Panel of Five should issue a statement when the writ is dropped.

14 The government should consider whether the CEIPP should be amended to provide that the Panel of Five may take a less drastic measure than a public announcement in appropriate circumstances.

15 The government should consider adding a member external to government to the Panel of Five. This member could be designated to communicate with the public when an announcement is necessary under the Critical Election Incident Public Protocol. Cabinet should consider appointing this sixth member through a process that would include consultation with all recognized political parties in the House of Commons, as well as with senators.

The Security and Intelligence Threats to Elections Task Force

16 The terms of reference of the Security and Intelligence Threats to Elections Task Force (SITE TF) should be formally amended to:

- provide for a permanent chair
- provide for a representative from the new body that I recommend be responsible for monitoring open source domestic online information for disinformation
- continue to provide for a representative from Global Affairs Canada
- provide for a "succession" mechanism to ensure that not all SITE TF representatives change at the same time
- be stood up for all federal general elections and any by-elections that the SITE TF decides may be vulnerable to foreign interference
- describe the SITE TF's reporting process to deputy ministers during by elections and the resulting responsibilities of those deputy ministers
- require the SITE TF to formalize and make public how it operates during federal general and by-elections
- require the SITE TF to issue a public after action report after each election, and if possible, by-election.

Building trust with the public and stakeholders

17 There should be a single, highly visible and easily accessible point of contact or hotline for reporting foreign interference to the government, which is responsible for engaging the appropriate agency or department. Follow-up with those who seek support should be systematic and ensure that those who make reports fully understand what can and cannot be done in response

18 Intelligence agencies should continue to diversify their personnel based on cultural, ethnic and linguistic background.

Duty to warn

19 Public Safety Canada should develop a Duty to Warn policy. The policy should apply to credible threats of serious harm potentially attributable to a foreign entity, directly or indirectly, made to any Canadian or to any person within Canada. This policy should be published online.

Parliamentarians

20 The Ministerial Directive and/or its Governance Protocol should be amended to ensure that, in cases of imminent treats, parliamentarians will be advised in a timely way.

21 Public Safety Canada, the Communication Security Establishment and the Canadian Security Intelligence Service should work with the House of Commons and Senate administrations to develop a Duty to Inform policy about cyber campaigns targeting specific parliamentarians. This policy should confirm that the government must – where national security considerations permit – inform the appropriate House of Commons or Senate security official about cyber threats specified in the policy. The policy would also state that the House of Commons and Senate are responsible for informing parliamentarians.

22 The Privy Council Office and Public Safety should convene the national security and intelligence community to develop a similar policy to inform the following, where national security considerations permit:

- the appropriate House of Commons or Senate security officials, about disinformation campaigns potentially attributable to a foreign state and targeting parliamentarians
- a federal election candidate or political party when a disinformation campaign potentially attributable to a foreign state targets the candidate or party

23 The policy should state that the House of Commons and Senate administrations are responsible for informing parliamentarians. The Security and Intelligence Threats to Elections Task Force should be responsible for informing political parties and, jointly with political parties, election candidates.

24 The government, in consultation with the House of Commons and the Senate, should continue to offer all parliamentarians, training and regular briefings on foreign interference.

Training could include information about the nature of intelligence and its limits, how it is collected and the consequences of revealing classified intelligence.

In consultation with Global Affairs Canada, training should also specifically address appropriate and inappropriate interactions with foreign diplomats and officials.

25 Members of Parliament, senators and their staff should be encouraged to check whether those with whom they interact are listed on the Foreign Influence and Transparency Registry. They should also be encouraged to inform the Foreign Influence Transparency Commissioner of any suspected contraventions of the *Foreign Influence Transparency and Accountability Act*.

Political parties

26 The government should prepare a guide about best practices against foreign interference specifically designed for political parties and their processes. This guide could, for example, cover subjects including foreign interference risks involving the use of personal devices, interacting with foreign officials and travel abroad.

Political parties in turn should provide this guide, or specific training materials included in it, to their staffs and to all nomination candidates and candidates for office.

27 The Canadian Center for Cyber Security should proactively provide parties with a regularly updated compilation of best practices.

28 Leaders of all political parties represented in the House of Commons should be encouraged and given the opportunity to obtain Top Secret security clearances as soon as possible after they become leaders.

29 Political parties are encouraged to take steps to be able to receive and act upon classified information.

30 All political parties represented in the House of Commons should always have at least two security-cleared individuals designated to liaise with government security and intelligence agencies.

31 The government should implement the following recommendations made by the Chief Electoral Officer:

- Only Canadian citizens and permanent residents should be eligible to vote in nomination and leadership contests.
- Registered political parties should be required to obtain a declaration from their members regarding their status as Canadian citizens or permanent residents. Parties should be required to maintain records of who has voted in their contests, as well as voter declarations of eligibility, for a minimum period, such as seven years.
- Section 282.4 of the Canada Elections Act should be amended to apply at all times (not just during an election period) and apply to influencing any person to vote for or against a nomination or leadership contestant.
- The prohibitions found in Part 11.1 of the Canada Elections Act should be expanded to nomination and leadership contests. The offences are sections 282.7 (bribery), 282.8(a) (intimidation) and 282.8(b) (pretence or contrivance).
- Sections 480.1, 481 and 482 should be expanded to prohibit efforts to lie or commit fraud in a nomination or leadership contest in a manner that is equivalent to the way in which they currently apply to elections.
- Parties and electoral districts should be required to file their rules for nomination and leadership contests with Elections Canada.
- The entity holding a nomination or leadership contest should file a notice with Elections Canada before the contest. This duty would apply in addition to the existing requirement to file a notice after the contest with information about contestants and the winner.
- All nomination and leadership contestants should be required to file a financial return with Elections Canada.

32 The government should consider whether it would be appropriate to create a system of public funding for political parties.

Foreign embassies and consulates

33 Global Affairs Canada should engage directly with foreign consulates in Canada to ensure that the line between legitimate diplomatic activity and foreign interference is well understood by consulate staff.

International declaration

34 Global Affairs Canada should engage with like-minded countries to determine the feasibility of developing a broadly-based, non-binding definition of foreign interference. The definition would reflect the intent of the Canadian approach to foreign interference and acknowledge the legitimacy of publicly criticizing another government's policy that may violate international norms.

Inter-governmental cooperation

35 The federal government should continue and intensify its efforts to engage and collaborate with provincial, territorial, Indigenous and municipal governments to counter foreign interference.

The RCMP

36 All Royal Canadian Mounted Police officers working in affected communities should receive training about foreign interference, including transnational repression.

37 The government should ensure that the Royal Canadian Mounted Police is adequately resourced to investigate and disrupt foreign interference activities.

38 The Royal Canadian Mounted Police should prioritize the recruitment, training and retention of staff with the skill sets required to investigate and disrupt foreign interference activities.

The intelligence-to-evidence challenge

39 The government should continue to consult on and implement measures to address the intelligence-to-evidence challenge, such as those it identified in its public consultations on foreign interference, or others that it assesses as having the potential to allow for the effective management of intelligence in the investigation and prosecution of national security offences.

Prohibitions

40 Sections 480.1 and 481 of the *Canada Elections Act* should be expanded to apply outside an election period and within and outside Canada.

41 Section 480.1 (impersonation) of the *Canada Elections Act* should be expanded to apply to any misrepresentations of the individuals listed in paragraphs (a) to (e) involving the manipulation, by any means, of a voice or image. The current exemption for parody or satire should be maintained and applied to manipulated content.

Third party political financing

42 The government should implement the following recommendations by the Chief Electoral Officer about political financing:

- The *Canada Elections Act* should provide that third parties, other than individuals, who wish to rely on their own funds to finance regulated electoral activities, provide Elections Canada with audited financial statements showing that no more than 10 percent of their revenue in the previous fiscal year came from contributions. All other third parties that are not individuals should be required to incur expenses to support or oppose parties and candidates only from funds received from Canadian citizens and permanent residents.
- Foreign entities should be prohibited from contributing to a third party for the purpose of conducting regulated activities.
- The *Canada Elections Act* should clarify that a third party is prohibited from using property or services provided by a foreign entity for regulated activities.

Penalties

43 The government should increase maximum administrative monetary penalties as well as fines for violations of *Canada Elections Act* prohibitions applicable to foreign interference.

Navigating the information environment

44 The government should pursue discussions with media organizations and the public around modernizing media funding and economic models to support professional media, including local and foreign language media, while preserving media independence and neutrality.

45 The government should consult with media organizations and others about funding the development of a reliable artificial intelligence translation tool that could broaden access to French language or English language professional media for individuals who currently face language barriers.

46 The government should also consider funding language training for new Canadians specifically aimed at promoting their access to professional media.

Developing digital and media literacy

47 The government should consider requiring news and social media outlets to label altered content.

48 The government should explore existing technologies and consider assisting civil society organizations (such as media observatories and universities) to develop a publicly available tool to help citizens verify whether digital content is fabricated or altered.

49 The government should implement the following recommendations made by the Chief Electoral Officer:

- All paid and unpaid electoral communications (image, audio, video or text) distributed during a regulated pre-election and election period, or a contest, which have been generated or manipulated by artificial intelligence should include a clear transparency marker. This requirement would also apply to nomination and leadership contests during the contest period. In this context, electoral communications should be understood to include: (1) all communications to the public made by or on behalf of a political entity, including a registered third party; and (2) communications by any other entity whose purpose is to influence electors to vote or not to vote, or to vote for or against a candidate or party. Platforms that have artificial intelligence-generated chatbots or search functions should be required to indicate in their responses where users can find official or authoritative information.
- During pre-election and election periods, any electoral communication (regardless of whether it is paid) made by registered political entities, or by political entities that are required to register (third parties who spend above the statutory registration threshold), should include a tagline or a source of information on or embedded in the message (for example, a link to an address) that indicates its origin.
- The *Canada Elections Act* should be amended to prohibit false information being spread to undermine the legitimacy of an election or its results. The prohibition should capture situations where it is shown that: (1) the person knew the statement to be false; and (2) the statement was made with the goal of undermining trust in the election and its results.

50 Federal, provincial, territorial and Indigenous governments should continue to work together on strategies to build and support education programs in relation to social media.

Protecting and promoting online information integrity

51 The government should consult with the public and with private industry on steps that may be taken to implement the principles of the Global Declaration on Information Integrity Online.

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