

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

The Honourable Marie-Josée Hogue,
Commissioner

VOLUME 5

CHAPTER 19

Recommendations to Better Protect Against Foreign Interference in Canada's Democratic Institutions and Processes



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

Volume 5: Recommendations to Better Protect Against Foreign
Interference in Canada's Democratic Institutions and Processes.

© His Majesty the King in Right of Canada (2025).

All rights reserved.

All requests for permission to reproduce this document of any part
thereof shall be addressed to the Privy Council Office.

Cette publication est également disponible en français :

*Volume 5 : Recommandations pour mieux protéger les processus et les
institutions démocratiques du Canada de l'ingérence étrangère*

CP32-169/2-2025E-5-PDF

ISBN 978-0-660-75083-5

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

Table of Contents

CHAPTER 19 RECOMMENDATIONS	4
19.1 Introduction	5
19.2 Three Lines of Effort	6
19.3 Institutional Resilience	7
Intelligence	7
The National Security and Intelligence Advisor to the Prime Minister (NSIA)	12
Clarifying coordination roles	13
Foreign Interference Strategy	14
Communications strategy	15
Awareness of the domestic online information environment	16
The Critical Election Incident Public Protocol and the Panel of Five	17
The Security and Intelligence Threats to Elections Task Force	20
Building trust with the public and stakeholders	22
Duty to warn	24
Parliamentarians	24
Political parties	28
Foreign embassies and consulates	35
International declaration	35
Inter-governmental cooperation	36
19.4 Enforcement	36
The Royal Canadian Mounted Police	37
The intelligence-to-evidence challenge	38
Prohibitions	39
Third party political financing	40
Penalties	41
19.5 Civic resilience	41
Navigating the information environment	42
Developing digital and media literacy	44
Protecting and promoting online information integrity	46
19.6 Call to Action on Transnational Repression	47
19.7 Evaluation and Assessment	48
LIST OF RECOMMENDATIONS	49

CHAPTER 19

Recommendations

19.1	Introduction	5
19.2	Three Lines of Effort	6
19.3	Institutional Resilience	7
19.4	Enforcement	36
19.5	Civic resilience	41
19.6	Call to Action on Transnational Repression	47
19.7	Evaluation and Assessment	48

19.1 Introduction

The Government of Canada and the leaders of all recognized parties in the House of Commons agree on the importance of preserving the integrity of Canada’s democratic institutions, including its electoral processes. This is why an important part of the Commission’s mandate is for me to recommend any means I consider appropriate to better protect Canadian federal democratic processes from foreign interference. In the preceding chapters, I summarized the evidence and other information I received and set out my findings. In this chapter, I revisit only those findings that led to recommendations.

The Commission’s investigation looked at how Canada responds to foreign interference. A wide range of information laid the groundwork for my recommendations. This included evidence from extensive factual hearings, expert views provided during policy hearings and insights from members of the public.

Many recommendations set out here are designed to correct a problem or fill a gap identified by the witnesses. Other recommendations flow from reviewing the extensive range of documents entered as evidence. Still others respond to observations and suggestions by individuals with a variety of academic expertise or field experience.


I am aware that the government is actively working on many of the issues that arose in the Commission’s proceedings. It is possible that some of the measures recommended to me will already have been adopted when this report is released or are being pursued. In these cases, the relevant recommendations should be read as an endorsement of these recent initiatives.

In several cases, I have recommended that the government continue with or improve on a measure already put in place. I have done so to underline that these measures are in keeping with the evidence before me and to emphasize their importance, both to decision-makers and to the public.

I must also stress that the government has introduced several measures to combat foreign interference over the past two years, many of them while the Commission was carrying out its work. These welcome initiatives very often filled a gap or corrected a problem that came to light during the hearings. Generally, however, they have not been in place long enough for the Commission to assess their effectiveness. The government should make this assessment within the next few years. I identify these measures below.

I must also caution that my mandate necessarily limits my recommendations. My mandate was to examine foreign interference in Canada’s democratic institutions, including its electoral processes. It was not intended to be a review of the entirety of foreign interference issues. Exploring them all in depth would take several years. Consider, for example, the complexities of understanding and addressing misinformation, disinformation and transnational repression.

I believe my recommendations can contribute to improving Canada's capacity to combat foreign interference. At the same time, I recognize that the means used by foreign states constantly evolve. The government will need to regularly assess the adequacy and effectiveness of its measures and modify them as necessary. Foreign interference is an ever-changing phenomenon. The means to combat it must change in tandem.

Below are my recommendations and the reasons behind them. There is also a list of the recommendations at the end of this chapter. I have identified those that I believe can and should be implemented promptly, perhaps even before the next election, with this visual: 

I have not set precise deadlines for implementing my recommendations, but I recommend the government report to Parliament within one year on its progress. After that, the government should determine the process for reporting further progress on implementation.

19.2 Three Lines of Effort

Foreign interference is complex and multifaceted. Foreign entities seeking to interfere with Canada's democratic processes and institutions do so by identifying and exploiting vulnerabilities in our society and our institutions. The central challenge for government is to reduce those vulnerabilities and disrupt foreign attempts to exploit them. At the same time, government must uphold and reinforce the fundamental rights, principles and values that make our democracy possible. Notably, these include freedom of opinion and expression, freedom of the press and the right to privacy. Maintaining this delicate balance is a challenge.

I have sought to formulate recommendations that respond to this challenge.

Witnesses and experts before the Commission underlined the critical importance of resilience to counter the corrosive effects of foreign interference (see, for example, Volume 3, Chapters 11 to 13, and Volume 4, Chapter 16). In my view, resilience means the ability to uphold core democratic and constitutional principles and values, preserve institutions and maintain public accountability, even in the face of threats.

Witnesses and experts before the Commission also stressed that building resilience against foreign interference must go beyond a whole-of-government approach to a whole-of-society effort. Different parts of society and government need to work with a shared vision and common goals.

There are no doubt several ways to frame such a strategy. My vision involves three lines of effort:

- **Institutional resilience.** This concept encompasses our democratic institutions and those tasked with defending them.
- **Enforcement.** This means adherence to rules, norms and law.
- **Civic resilience.** This is the capacity of Canadian society to withstand and repel foreign interference.

Each line of effort is necessary. All are mutually reinforcing. None is sufficient alone.

19.3 Institutional Resilience

As explained in Volume 2, Chapter 6 and Volume 3, Chapter 11, many federal entities have responsibilities relating to foreign interference. To ensure cooperation among them, the government has established certain procedures and processes. I considered what entities could do to improve their foreign interference responses and how they could more effectively collaborate and cooperate with other entities. I decided it would be unproductive to introduce a completely new set of structures and mechanisms, ignoring those now in place. My recommendations build on what is already here. Although these structures can be improved, they are well thought-out, sound and efficient.

Intelligence

Dissemination

The first step in detecting, deterring and countering foreign interference is the collection of intelligence.

The Canadian Security Intelligence Service (“**CSIS**”) plays a crucial role here. The mandate of CSIS is to investigate and report to the government on activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. Foreign interference is one such activity (see Volume 3, Chapter 11).

The way in which CSIS shares the intelligence it collects is a crucial element in fighting foreign interference (see Volume 4, Chapter 14). The evidence shows that in the years under review by the Commission, the flow of intelligence from CSIS to the rest of government was sometimes problematic:

- Some reports did not reach intended recipients.
- Some reports requesting a response from the recipient(s) went unanswered.
- At times, it was impossible to determine who received or read CSIS reports.

In addition, the evidence before me shows that Canada’s intelligence agencies disseminate a vast amount of intelligence. Some witnesses assured me that processes are in place to ensure that the products sent are relevant to specific individuals and senior decision-makers. However, I have seen that these processes are not without shortcomings.

I have seen instances where senior decision-makers did not view reports that CSIS flagged for their attention as particularly relevant. I also heard evidence that, at times, too much intelligence is directed at senior officials, leading them to review many reports that, ultimately, they do not need to see. Not every report needs to be read by the prime minister, a minister or a deputy minister. When too much intelligence is directed at decision-makers, there is an increased risk that the intelligence that they do need to see may not be given the consideration it requires. The challenge is in getting the balance right.

I understand that the national security and intelligence community has taken steps since 2023 to improve the government’s distribution system for intelligence and that records are now kept about who has accessed intelligence (see Volume 4, Chapter 14). Efforts are underway to enhance intelligence sharing within government by using Client Relations Officers and the new CSIS Liaison Officer at Public Safety Canada (“**Public Safety**”) and other key departments and using the same Top Secret centralized database system to share classified information and to keep better track of oral briefings.

I find these efforts necessary but not sufficient to improve intelligence sharing within the government. There is always room for improvement, especially in terms of agencies’ efforts to help their clients understand intelligence and to enhance agencies’ ability to generate products that respond to client needs and priorities. It is not enough to send and receive information. To be effective, information must be read and understood by the appropriate people and, where necessary, acted on through feedback, direction or requests for additional information.

In particular, I note that CSIS does not have a uniform system for identifying what it thinks is the product’s level of importance for its primary clients. Without some indication of the report’s specific relevance to the client’s operational or policy interests, its distribution alone is not enough.

Also, although it was not said directly, I understood from various witnesses that senior decision-makers would like to receive more concise and direct reports and assessments from CSIS without too much technical, repetitive or overstated language. I also found that the reliability of intelligence and the assessment of it in reports was often unclear. The current practice of repeating the same long list of general caveats in every report makes it too easy to skip past these warnings after a time.

Recommendation 1

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 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 a written report containing this recommendation to the client.

Feedback

I also understand that, in setting Canada’s intelligence priorities, the Privy Council Office (“**PCO**”) has a feedback process between the intelligence agencies and their regular clients (see Volume 4, Chapter 14). This process is vital and should be adhered to. Furthermore, feedback should be encouraged at all levels, regularly and frequently. Feedback received should be provided to those responsible for preparing reports. This will allow them to integrate the feedback into their work and ensure that future products better respond to the client’s intelligence needs.

I further note that the feedback process may assist in bridging divides, such as differing views across government about whether an activity reported on constitutes foreign interference. I heard evidence that, where intelligence concerns potential foreign interference, there was sometimes disagreement between CSIS and its clients about what constituted foreign interference warranting government attention (see Volume 4, Chapter 14). I also heard that the key to building shared understandings is increased communication and discussions, such as those that have been occurring between government

departments in the last few years. Regular feedback at all levels may assist in encouraging these discussions.

That being said, I expect healthy debate to continue. So long as debate does not impede decision-making, it is not only healthy but necessary. Witnesses noted, and history has shown, that there is a real danger of groupthink in matters of national security.

Recommendation 2

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.

Transparency and disclosure

Countering foreign interference involves a wide variety of stakeholders, both within and outside government. Some stakeholders may have the necessary security clearances to see intelligence, but lack the physical and technological infrastructure to receive, handle or store materials with higher levels of classification. Other stakeholders may not have security-cleared personnel at all (see, for example, Volume 4, Chapters 15 and 16).

Amendments to the *Canadian Security Intelligence Service Act* made by the *Countering Foreign Interference Act* gave CSIS greater authority to share information outside the federal government, but barriers to sharing classified information remain (see Volume 3, Chapter 12 and Volume 4, Chapter 16).

These barriers are amplified by what some experts at the Commission's national security confidentiality hearings referred to as a tendency within Canada's national security community to overclassify information. I heard that CSIS has a history of defaulting to high levels of protection for potentially sensitive material.

I have noted that documents are classified based on the most sensitive information they contain, and that Canada does not have a declassification system like that of some other countries. My understanding is that the government has done some work on this issue but that a declassification system was never fully developed or implemented. The Commission also heard evidence calling for the national security and intelligence community to try to make greater use of open source products alongside classified information (see Volume 3, Chapter 11).

I would say that the evidence overall reveals a strong culture of secrecy within the Canadian national security and intelligence community, a culture that can impede the dissemination, use and understanding of intelligence about foreign interference.

CSIS witnesses spoke about the agency moving to a “sunlight policy” to be more direct and clearer in its dealings with the client community and more transparent with Canadians about foreign interference (see Volume 4, Chapter 16). I was told that CSIS now understands that it needs to be able to share information to better protect Canadians and to build their trust. Indeed, many government witnesses stressed the importance of increased transparency. I note that, for this sunlight policy to succeed, those who hold the information must be willing, and find ways, to share it.

Recommendations 3 and 4

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.

Protocol for intelligence regarding political institutions and actors

I have also seen that the collection, handling and dissemination of intelligence about political institutions and actors can involve particular sensitivities and challenges (see Volume 4, Chapter 15).

For instance, the Prime Minister noted that it was awkward in some respects for him to be advised of intelligence relating to other political parties. CSIS and PCO officials similarly discussed the sensitivity of sharing intelligence with the governing party about other political parties. Witnesses from the Prime Minister’s Office described this as an issue that needs to be resolved.

There may also be occasions where sharing intelligence with the governing party about potential foreign interference in their own party will give rise to particular sensitivities. How to resolve these sensitivities also needs to be addressed.

CSIS officials also described the particular challenges involved in sharing classified information with parliamentarians, knowing that parliamentarians may be able to rely on parliamentary privilege to avoid legal consequences for disclosing classified information.

I also heard about the need to improve intelligence sharing with other levels of government in Canada and political actors about potential foreign interference in their processes.

In my view, the national security and intelligence community should establish a protocol for the collection, analysis and distribution of intelligence about potential foreign interference with political institutions and actors. This protocol should cover issues such as providing members of the governing party with intelligence about opposition parties and managing the risks of disclosure when sharing classified information with parliamentarians. The existing Governance Protocol to the Ministerial Directive (see Volume 4, Chapter 15) does not address these complexities of sharing intelligence with political actors.

I note that the Governance Protocol provides for possible modifications of its procedures for conflicts of interest. This is a good start, but a more comprehensive framework is needed.

Recommendation 5

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 (NSIA)

The National Security and Intelligence Advisor to the Prime Minister (“**NSIA**”) plays an important role within the intelligence community, along with national security and intelligence agencies (see Volume 3, Chapter 11). The current NSIA is also a Deputy Clerk of the Privy Council.

The position of NSIA is given to an experienced public servant. The NSIA’s role is to advise the Prime Minister on matters of national security. The NSIA therefore has a key function in combating foreign interference.

I heard evidence that the role of the NSIA has evolved and continues to evolve and grow in importance to meet the Prime Minister’s needs and priorities on national security issues. That the NSIA is now a Deputy Clerk, and the addition of a Deputy NSIA, reflects the increased significance of the NSIA function and communicates this to the rest of Canada’s national security and intelligence community.

The duties of other senior national security and intelligence appointments – for example, the CSIS Director or the Chief of the Communications Security Establishment (“**CSE**”) – are set out in legislation. The mandate, responsibilities and limits of the NSIA are not. Some, like the National Security and Intelligence Review Agency, have recommended that the NSIA role be formalized in a legal instrument, especially as the role relates to sharing intelligence.

I am not convinced that legislation is the correct approach. The role of the NSIA should reflect the priorities of the prime minister of the day. As well, the coordination and policy functions of the role should remain flexible to allow adaptation to a constantly evolving threat environment. Legislation, which is complex to create and not easily modified, seems unsuited to this.

However, I agree that it would be helpful to have the NSIA, others in government and the public understand the prime minister's expectations for the NSIA. For this reason, the Prime Minister's public mandate letter to the current NSIA in November 2024 was a good initiative. This practice of expressing in writing what is expected of the NSIA should continue.

A public statement of the NSIA's mandate is crucial not only to clarify their role for the public and across the national security and intelligence community, but to make them accountable for coordinating the prime minister's national security agenda.

For this reason, a public mandate letter or other non-legislative instrument should be issued with every new government and every time a new NSIA is appointed. This document should articulate the NSIA's role, how the position relates to other entities in the national security and intelligence community and what the prime minister expects the NSIA to accomplish.

I note that on 10 October 2024, the National Security and Intelligence Committee of Parliamentarians ("**NSICOP**") began a review of the NSIA role. NSICOP is reviewing the legislative, regulatory, policy, administrative and financial framework of the NSIA, as well as their activities.

Recommendation 6

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

Several government departments, agencies and other entities are involved in detecting, deterring and countering foreign interference (see Volume 3, Chapter 11). Their roles and responsibilities are generally well defined, but there are exceptions.

In particular, I find that the respective roles and responsibilities of the Privy Council Office (PCO), including the NSIA, and their supporting secretariats, and Public Safety are somewhat unclear. The lengthy inter-departmental discussion about where to house the National Counter Foreign Interference

Coordinator (see Volume 3, Chapter 11) is an example of this lack of clarity about whether PCO or Public Safety is responsible for coordinating government responses to foreign interference.

While that particular issue may have been more or less resolved, the evidence before me indicates that there is still work to be done in unpacking responsibility for strategic and operational coordination around foreign interference. Indeed, this has been the subject of discussion at the deputy minister level over the past year, which does not appear to have clarified the situation.

The principle of ministerial responsibility and accountability, so important in our democracy, requires clearly defining the roles and responsibilities of each department. A lack of clarity creates a significant risk that decisions necessary to counter foreign interference will not be made in a timely fashion.

Clarifying the respective roles and responsibilities of PCO and Public Safety in foreign interference matters would make their work more effective and make it easier to determine the accountability of each.

Recommendation 7

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

The government has taken several positive steps since 2018 to combat foreign interference. These include policies like the Plan to Protect Canada's Democracy and its amendments, the *Ministerial Directive on Threats to the Security of Canada Directed at Parliament and Parliamentarians* and its related Governance Protocol, and the *Countering Foreign Interference Act* (see Volume 3, Chapter 12 and Volume 4, Chapter 15).

However, the measures to date have been piecemeal. This is not surprising since the foreign interference threat has both increased and evolved over the last decade. The time has come to develop a comprehensive, well-articulated and responsive strategy to combat foreign interference.

As I discuss in Volume 3, Chapter 12, the government began working on a whole-of-government strategy to counter foreign interference in 2018. Cabinet endorsed the principles of such a strategy in the spring of 2022. Despite this, the government has not finalized a public-facing foreign interference strategy. It is time to do so. This strategy should form part of the renewed National Security Strategy that the Prime Minister recently directed the National Security and Intelligence Advisor to the Prime Minister (NSIA) to develop in 2025.

Recommendation 8

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

The evidence before the Commission also reveals that the Canadian public is largely unaware of the positive measures taken by the government to counter foreign interference. The government has done the work but failed to communicate its efforts to the public effectively. As a result, many Canadians may believe that nothing – or very little – is being done to combat foreign interference. This, in my opinion, contributes to diminishing public confidence and trust in our democratic institutions and processes.

Civic resilience requires trust among citizens. It also requires that Canadians trust that our institutions will promote the public interest and hold office-holders accountable for their decisions and actions in detecting, deterring and countering foreign interference.

To earn the public's trust, democratic institutions need to be effective, transparent and accountable. Trust depends on the public understanding democratic institutions, how they function and why they are designed the way they are. It also depends on the representatives of these institutions communicating effectively with the public and taking responsibility, publicly, for their policies and actions, whether successful or not. Finally, trust is maintained through strong, independent oversight. All this requires transparency and effective communication.

Like its response to foreign interference, the government's communications efforts to date have been fragmented, with each department and agency responsible for its own communications strategy. This lack of coordination in communications about foreign interference risks and countermeasures has led to inconsistent messages.

The government has long recognized the need for a government-wide communications strategy regarding countering threats such as foreign interference. In 2022, Cabinet ratified the Countering Hostile Activities by State Actors Memorandum to Cabinet, which recommended the implementation of a whole-of-government communications approach. This has not yet been achieved.

I note that Elections Canada has an effective multi-pronged communications strategy, particularly in and during the run-up to an election period, to remind the public about the features that keep elections secure. This is a good

example of how democratic institutions and government as a whole can communicate effectively with Canadians.

In my view, a government-wide communications strategy is needed to strengthen the trust of Canadians in our democratic institutions. The strategy would aim specifically at informing the public about foreign interference, the measures taken and the mechanisms put in place to protect these institutions from foreign interference.

Recommendation 9

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

During federal general elections and by-elections, the Rapid Response Mechanism (“**RRM**”) Canada is the entity that monitors the domestic online information environment for foreign misinformation and disinformation. RRM is part of Global Affairs Canada (“**GAC**”).

However, this work is not RRM Canada’s primary purpose. Domestic baseline online monitoring for misinformation and disinformation is also not part of GAC’s mandate. This work reduces GAC’s ability to focus on its formal mandate – dealing with international affairs (see Volume 3, Chapter 12). Foreign interference is mainly a domestic issue.

It is also important to keep in mind that disinformation campaigns targeting democratic discourse are not limited to the period just before and during an election. Foreign interference can occur in an election context, but its impact on democratic processes and institutions extends well beyond elections.

No government body has a mandate at present to monitor the Canadian online information environment to identify foreign-based disinformation campaigns that may affect federal democratic institutions, including electoral processes. I find this is a gap in Canada’s capacity to identify and counter foreign interference in democratic processes, especially when misinformation and disinformation seem increasingly common as techniques for foreign states to interfere with democracy. This was evident in recent elections around the world. Open source, online disinformation campaigns by foreign states targeting Canada’s democratic institutions interfere with our sovereignty. It is in the public interest to identify and have government respond to these activities.

However, Canada does not have a clear legislative framework or appropriate policies to collect and assess open source domestic online information in a way that respects privacy rights. Such laws and policies are critical.

I stress that I am not recommending that the government monitor all social media activity or private or semi-private communications of Canadians. Canadians have the right to freely associate and express themselves online, and the right to privacy extends to online spaces.

Recommendations 10 and 11

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

Intelligence collected over the years has led to several measures to counter foreign interference. These include the 2019 implementation of the Plan to Protect Canada’s Democracy (“**Plan**”). One of the Plan’s key measures was the establishment of the Critical Election Incident Public Protocol (“**CEIPP**”). This protocol establishes a process to communicate transparently and impartially with Canadians during an election if an incident or a series of incidents threaten the election’s integrity. A group of five senior public servants (“**Panel of Five**” or “**Panel**”) is responsible for determining if this threat to integrity has occurred (see Volume 3, Chapter 12).

Public communication

The CEIPP is a very good initiative, but is unknown to too many Canadians, as are the existence, role and decision-making processes of the Panel of Five.

I agree with the findings of the Rosenberg Report (see Volume 3, Chapter 12) that those within government responsible for implementing the CEIPP should generally communicate more with the public about the risk of foreign interference and the measures the government is taking to protect the integrity of federal elections. Publishing notices on government websites is not enough. Better ongoing engagement with the public about the Plan should help normalize communications that may have to take place during an election campaign. It will also increase trust in federal electoral processes. It is especially important in the lead-up to elections but should not be limited to the election period.

The Panel of Five must also do a better job of informing the public about its role and decision-making processes. It should do this periodically, and, at a minimum, make a specific statement at the outset of each general election campaign. This could help ensure that, if an announcement under the CEIPP is required during an election, the public will better understand the context in which it is made. The Panel of Five's communications should also clearly explain that foreign interference that does not reach the threshold for a public announcement will be dealt with through the national security and intelligence community's normal methods, channels and authorities.

Both the CEIPP itself and how the Panel of Five determines whether the CEIPP threshold is met during election periods should be widely publicized to enable the public to understand how this process helps protect federal elections from foreign interference, as well as from domestic threats.

Recommendations 12 and 13

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.

Threshold

The threshold for a public announcement set out in the CEIPP is very high. It would be useful to consider and clarify whether the Panel of Five should have the authority to consider measures other than a public announcement. There

may be a level of interference that is not sufficient to affect the integrity of the elections overall but is nonetheless significant enough to warrant some action by the Panel itself rather than an individual government department or agency. This could, for instance, be an option where the interference affects only one or a few ridings. If the government decides to allow this type of response, it should also identify the measures that might be taken.

Recommendation 14

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.

Composition

I find the composition of the Panel of Five to be appropriate. Having five deputy ministers as members makes sense, since during election periods deputy ministers are those tasked with continuing the affairs of the Government of Canada. That said, although I have no doubt about the experience, impartiality and good judgment of the Panel's current or past members, they are all relatively unknown to the public. This may make it more difficult for some Canadians to accept the Panel's decisions.

Furthermore, not everyone understands that public servants are non-partisan, and some individuals may not believe that they are. Even though this is unjustified, some may associate public servants with the Government of the day. For these reasons, the government should consider adding a sixth member to the Panel from outside government. This member should be a distinguished Canadian in whom the public has confidence and who could be the face of the Panel if an announcement is needed during an election period.

To assure legitimacy and “buy-in,” Cabinet should consider appointing the sixth member through a process that would include consulting all recognized political parties in the House of Commons as well as with senators.

Recommendation 15

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

When it established the CEIPP, the government also created the Security and Intelligence Threats to Elections Task Force (“**SITE TF**”). As explained in Volume 2, Chapter 6 and Volume 3, Chapter 12, the SITE TF is an information sharing and coordinating group with representatives from CSE, the Royal Canadian Mounted Police (“**RCMP**”), GAC and CSIS. It reviews election-related intelligence, provides situational awareness and regularly reports its observations and the intelligence it receives to the Panel of Five.

The SITE TF has proved to be a useful initiative. It preserves the integrity and independence of all the agencies represented on it. It benefits from the expertise within each agency and improves information flow about potential electoral interference. It also guarantees the nimbleness needed to adapt to evolving situations while keeping a sharp, action-oriented and well-coordinated focus on the task at hand.

Process and continuity

I heard that there have been discussions about whether the SITE TF should be formally designated a permanent body. For some, a permanent SITE TF could do more robust national threat assessments, would be better positioned to share information with stakeholders and the public and could have greater engagement with international partners.

Although the evidence shows that the SITE TF is already active outside election periods, I believe that, for now, the level of threat of foreign election interference may not be high enough to justify the SITE TF becoming a standalone and permanent body.

However, there would be value in evolving the SITE TF into a more structured organization. This would avoid continuing to rely mostly on the goodwill of the partners represented on the SITE TF.

The evidence shows that the SITE TF adversely affected the usual operations of some of its members. SITE TF members should identify more clearly which positions they can staff when needed and what back-up they have internally to offset the surge of work required. This would permit better planning (both financially and for human resources) and offer greater stability between periods of mobilization. It would also secure a pool of readily available talent and greater capacity to expand if the need or the threat increases over time. Finally, it would facilitate planning, training and table-top exercises between mobilization periods.

For by-elections, the SITE TF should assess the riding's vulnerability to foreign interference before the by-election starts. The SITE TF should be activated if it assesses that the by-election may be vulnerable to foreign interference.

Because the SITE TF was not designed to be active throughout the year, its current structure of a rotating chair and membership make developing institutional memory difficult. It also makes it harder to build and maintain trust with external partners such as political parties. For these reasons, I believe having a permanent chair would be helpful.

Unlike during a general election campaign, the caretaker convention is not in effect during by-elections. This means that the CEIPP is not activated. In this situation, the SITE TF reports to an inter-departmental committee of deputy ministers instead of the Panel of Five. The way the SITE TF reports to deputy ministers during by-elections and the responsibilities of those deputy ministers should be formalized in its Terms of Reference.

The SITE TF's Terms of Reference should formalize its methods of functioning during federal general and by-elections.

Membership

Earlier in my recommendations, I proposed that the government consider creating a new body to monitor open source domestic online information for disinformation potentially attributable to foreign states. Just as the Rapid Response Mechanism (RRM) Canada does now, this body would have an important role to play on the SITE TF and should be added to its permanent membership.

GAC should continue to have a representative on the SITE TF so it can provide international and diplomatic context and advice to other members and, during elections, to the Panel of Five. This would also ensure that the SITE TF continues to receive relevant information obtained by RRM Canada. This information may be critical input for the Panel of Five as it assesses the impact of certain activities or a public announcement.

Organizations and agencies participating on the SITE TF should ensure that their participation does not occur to the detriment of their ongoing mandates, and they should explain how they intend to do this. The government should ensure that these additional duties are properly resourced, if necessary.

To ensure continuity, the SITE TF's Terms of Reference should also be amended to ensure that not all its members are replaced at the same time.

Public communication

The public should be made aware of the SITE TF's work and, to the extent possible, its methodology. The SITE TF's practice, since the June 2023 by-elections, of issuing public after action reports is a step in the right direction. This practice should be included in the SITE TF's Terms of Reference.

Recommendation 16

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.
-

I wish to emphasize the importance of having the measures outlined above in place as soon as possible. Other than adding the representative of the newly recommended monitoring body, these recommendations should be implemented before the next election.

Building trust with the public and stakeholders

The Commission heard repeatedly that, in many of the communities most vulnerable to foreign interference, targeted individuals are reluctant to report their experiences. They lack trust in national security and law enforcement agencies and fear reprisals. This may deprive CSIS of significant information.

Many also mentioned that they do not know where to report an incident or information and would like access to a designated resource (see Volume 4, Chapters 16 and 17 and Volume 6). These stories highlight two important issues.

The first relates to how government agencies coordinate and collaborate among themselves. Having multiple points of access to government is unhelpful if a member of the public is repeatedly told by those that they reach

out to that their complaint should be directed elsewhere or worse, they get no response. It is easy to see why they might then feel confused or abandoned by the government.

The second issue is that of public expectations. The reality is that different agencies do, in fact, have different mandates, and what they can do in response to reports differs significantly. What law enforcement can do is different from what an intelligence agency can do. Further, it may well be that no federal agency has a mandate to or is able to assist with some issues. This is a fact that is understandably challenging for the public to appreciate and accept, particularly when they are trying to get help.

I understand that CSIS has already established a hotline for anonymous reporting of foreign interference. This is an excellent initiative but does not fully address the above two issues. While there is merit to a more coordinated system of reporting in which members of the public can engage with a single point of contact or hotline, it is important that the designated point of contact actively triage the report to the appropriate government actor and ensure there is follow-up with those using the hotline.

I also heard evidence that CSIS, the RCMP and CSE understand the importance of public trust for fulfilling their mandates and that they are working to improve their engagement with the public in a variety of ways (see Volume 4, Chapters 16 and 17). Despite these efforts, based on what diaspora community members told me, I conclude more work is needed to build trust in Canada's national security and intelligence institutions.

It is difficult to build trust with a community whose members feel they are over-policed, homogenized, victimized or misunderstood. Those responsible for outreach need to understand the community they seek to approach. This knowledge is best acquired through lived or shared experiences. Steps to reach out and build trust with affected communities have been taken. However, this work must continue and be appropriately resourced and reinforced at every level.

Recommendations 17 and 18

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

Once the government receives intelligence about foreign interference, the government decides what to do with it. In some cases, the nature of the intelligence may compel the government to take direct action. This will generally be the case when intelligence identifies a credible threat of serious harm (see Volume 3, Chapters 12 and 13 and Volume 4, Chapter 15).

However, CSIS does not have a specific policy on sharing threat-to-life information with police. CSIS witnesses said that, when it has information of a threat of physical harm or a threat to the life of an individual, CSIS immediately engages police authorities to ensure the individual is physically protected, while taking necessary steps to protect the source of the information.

I believe Public Safety should ensure a consistent and coordinated approach for CSIS and the RCMP to warn people within Canada about credible threats of serious harm potentially attributable, directly or indirectly, to foreign entities. In conjunction with the relevant agencies, Public Safety should consider and set an appropriate threshold for warning and develop a formal policy that reflects this threshold and sets timelines for providing warnings.

This policy should be made publicly available, including online. Doing so would provide important transparency around a process that the public may not understand well. The policy could require warning both those facing a credible threat of serious harm and those responsible for protecting them. Who has the responsibility for protecting the threatened individual will obviously vary depending on the circumstances. For parliamentarians, this would include the Sergeant-at-Arms, the Senate Director of Corporate Security, the Parliamentary Protective Service and the RCMP. In other cases, it might include the police of local jurisdiction and appropriate local security officials.

Recommendation 19

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

Parliamentarians make laws, challenge the government and can influence policy. For this reason, they are potential targets of foreign interference directed at one of Canada's principal democratic institutions.

Ministerial Directive on threats to parliamentarians

The recent *Ministerial Directive on Threats to the Security of Canada Directed at Parliament and Parliamentarians* (“**Ministerial Directive**”) and its related Governance Protocol are necessary and important means of enhancing the national security and intelligence community’s ability to protect democratic processes from foreign interference (see Volume 3, Chapter 12 and Volume 4, Chapter 15).

I note however that the Ministerial Directive and its Governance Protocol do not specify time limits for completing the process required to advise parliamentarians. The evidence has shown instances where the consultations and discussions have taken too long. This is a concern, particularly in cases where the risk to parliamentarians may be time sensitive. As currently drafted, the Governance Protocol would appear to require extensive – and potentially lengthy – consultations even when the imminence of a threat would require immediate action.

Recommendation 20

20. The *Ministerial Directive on Threats to the Security of Canada Directed at Parliament and Parliamentarians* and/or its Governance Protocol should be amended to ensure that, in cases of imminent threats, parliamentarians will be advised in a timely way.

Informing parliamentarians of cyber threats and disinformation campaigns

The APT 31 cyber campaign targeting some parliamentarians highlighted that the Ministerial Directive does not expressly cover threats identified by agencies other than CSIS (see Volume 4, Chapter 15). Some government witnesses said if the APT 31 incident happened today, it would most probably fall under the Ministerial Directive and be dealt with accordingly. However, this view was not unanimous.

Furthermore, there is no documented procedure about how to inform parliamentarians of cyber threats, who would be responsible for informing them or under what circumstances they would be informed.

A formal policy is needed to inform parliamentarians of cyber threats. Billions of cyber threats (generally unsuccessful) target Canada’s technological infrastructure annually. It would not be possible or useful to advise parliamentarians of every cyber threat. Instead, they should be advised only in appropriate circumstances, especially when they have been or are expressly targeted.

A similar policy could also be developed to inform parliamentarians or federal election candidates who have been targeted by disinformation campaigns potentially attributable to a foreign state. This could be done first in conjunction with RRM Canada. Later, the task could be assigned to the new

body that I recommended monitor the open source domestic online information environment.

Recommendations 21, 22 and 23

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.

Education and training regarding foreign interference

Education and training can reduce the vulnerability of parliamentarians to foreign interference. For example, training could cover how foreign interference can manifest itself and steps to take if it does, as well as provide greater clarity about permissible interactions with foreign states. The evidence demonstrates that the line between acceptable behaviour by a foreign state and foreign interference is sometimes not clear (see Volume 3, Chapter 10). I also heard that parliamentarians may not necessarily be aware where to draw that line (see Volume 4, Chapter 18).

The House of Commons administration has been working with the national security and intelligence community to provide unclassified briefings to members of Parliament (“MPs”) and their staff members. These briefings cover the foreign interference threat landscape and precautions that MPs and staff members can take. Such briefings should continue.

Senators may also be targets for foreign interference. However, it appears that the government has recently begun preparations to provide senators with similar briefings.

Sometimes, parliamentarians need to receive classified intelligence. This could be through a measure under the *Canadian Security Intelligence Service Act* or under the Ministerial Directive and Governance Protocol. Because of this, they must understand the inherent limits of intelligence, the intelligence collection process and the consequences of revealing classified information. Becoming more familiar with the nature of intelligence will make parliamentarians less vulnerable to foreign interference. It will also help them fulfill their accountability function in both the Senate and the House of Commons.

Recommendation 24

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.

The Foreign Influence Transparency and Accountability Registry

The recently enacted *Foreign Influence Transparency and Accountability Act* (“*FITAA*”) will establish a registry designed to promote transparency about activities conducted for foreign principals. Persons or entities entering arrangements with a foreign principal to undertake certain activities relating to political or governmental processes in Canada must provide information to a commissioner who, in turn, will create and maintain a public register.

The *FITAA* regime is somewhat analogous to that in the federal *Lobbying Act*. Both allow activities related to political or governmental processes but, because of the risk of improper influence, require transparency.

The Office of the Commissioner of Lobbying of Canada encourages parliamentarians contacted by lobbyists to check the Registry of Lobbyists, ask lobbyists if they are aware of the *Lobbying Act* and the *Lobbyists’ Code of Conduct* and take other steps to encourage compliance. In this way, parliamentarians have a role in compliance.

Parliamentarians also have a role in detecting, deterring and countering foreign interference. This is an important element of a whole-of-society approach. It is reasonable to expect parliamentarians to employ all available measures against foreign interference. Proactively consulting the Foreign Influence and Transparency Registry is one way to do this. At the very least they would learn of existing relationships between individuals they interact with and foreign states.

Recommendation 25

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

Political parties are among the central players in our democratic system. Parties recruit and support candidates, sign-up members, choose leaders and compete for votes based on their policy platforms. They are a primary point of connection between the public and the electoral process.

Political parties are often called public organizations because of the vital function they perform in elections. But they are private organizations. They are self-governing, have their own criteria for membership and establish their own guiding principles and values. In that sense, political parties are private entities serving a public interest.

All party representatives who testified at the Commission’s public hearings expressed some concern about foreign interference potentially targeting political parties (see Volume 3, Chapter 13).

It is in the public interest to help political parties protect themselves against foreign interference and to help them develop the tools and competencies they need to detect and combat foreign interference. Given the public role of political parties, it seems appropriate to devote public resources to this end.

Best practices guides

Political parties have a role to play in a whole-of-society response to foreign interference. To be able to detect, deter and counter foreign interference, however, they must first develop an awareness about foreign interference tactics and learn how to protect themselves. The government has provided some briefings to political parties, but I believe it would also be helpful for

parties to have a resource they can use to train their staff and consult when certain situations arise, for example, when someone travels abroad. At the same time, it is important to recognize that, while government can do more to give political parties tools, it is ultimately the responsibility of political parties to use them.

Recommendation 26

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.

Some political parties have had contact with CSE’s Canadian Centre for Cyber Security (“**CCCS**”) and found it helpful to varying degrees. At least two parties also consulted external cyber security experts. Each party’s ability to respond to cyber threats, including foreign interference, is determined by its resources. This leaves some parties less able than others to detect, deter and counter foreign cyber threats.

I understand the CCCS already provides advice and other cyber security services to political parties on request and provides a range of resources to the public on its website. While this is highly valuable, as a practical matter it may be useful for CCCS to more proactively provide parties with a compilation of regularly updated best practices. By actively reaching out to parties, rather than relying on parties to come to it, the CCCS may be more successful in its ultimate objective of equipping political parties with the tools they need to protect themselves.

Recommendation 27

27. The Canadian Center for Cyber Security should proactively provide parties with a regularly updated compilation of best practices.

Security clearances for political party leaders

Leaders of political parties have unique powers and responsibilities within Canada’s democratic system. They decide whether to approve or reject any candidate who seeks election in the party’s name and assign people to positions and functions within the party. Party leaders cannot expel an MP

from Parliament once the MP is elected but can oust them from the party caucus. Party leaders can also informally raise concerns with MPs, set out expectations and convey warnings about inappropriate conduct. Several witnesses pointed to these powers as potential tools to address foreign interference targeting parliamentarians (see Volume 4, Chapter 15).

I also heard that, until recently and to avoid appearances of partisanship, the Prime Minister was generally not given intelligence about a member of another party.

Ideally, any such intelligence should be given to the leader of the other party. In some cases, this has occurred because the leader had the necessary Top Secret security clearance to receive classified information.

It is preferable for political party leaders to have a Top Secret security clearance. A party leader without a clearance may not be able to receive the detailed information they need to understand and act against the foreign interference risk facing their party.

However, in our political system, it is not desirable, and maybe not even feasible, to require a leader to apply for and obtain a security clearance. Security clearances may be denied for all kinds of reasons, even some that may be unrelated to the individual applicant. Moreover, requiring a leader to obtain a security clearance would be an intrusion by the government into the freedom of political party members to choose their party leader. Imposing a mandatory security clearance requirement for party leaders would, in my view, severely interfere with basic rules of Canadian democracy as it could result in disqualification of the person chosen by a party's members to lead it.

It is nevertheless essential for each party to be able to receive and, more importantly, act upon classified information. For instance, if significant and credible concerns about a nomination contestant come to light early enough in the nomination process, the contestant should perhaps not be permitted to continue. If significant and credible concerns are identified with a sitting parliamentarian, it may be that steps should be taken to mitigate the risks. This could mean ensuring that the parliamentarian is not in a position to receive classified information or ensuring that they are not given a position of authority within caucus, such as House Leader, Whip or caucus chair. Decisions about these situations generally fall to the party leader. If a party leader does not have a Top Secret clearance, they might consider delegating some of their authority and prerogatives to a security-cleared representative.

Recommendation 28

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.

Dedicated points of contact

Overall, the evidence indicates that communications between national security and intelligence agencies and political parties represented in the House of Commons have been uneven and inconsistent (see Volume 4, Chapter 15). This may have been in part because party representatives dealing with the government changed over time and government agencies were not informed.

Also, while the government has provided classified and unclassified briefings to political party representatives through the SITE TF and the Privy Council Office, representatives generally said they did not find these particularly helpful. This may explain the poor attendance at the unclassified briefings during the 2023 and 2024 by-elections.

Government transparency and effective communication both build trust. They can also help to educate parties about situations that may create vulnerability to foreign interference. This knowledge can help to deter and counter foreign interference. It may also help to identify those who may be vulnerable to foreign interference. A consistent and continuing relationship between political parties and national security and intelligence agencies is a necessary part of the foundation for transparency and effective communication.

Recommendations 29 and 30

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.

Nomination and leadership contests

Efforts to co-opt the legislative process can begin even before elections, including during party nomination contests and leadership races. For example, the Commission found possible foreign interference with a nomination contest in the Don Valley North riding in 2019 (see Volume 2, Chapters 7 and 9).

Nomination contests can be thought of as the first step in an election. As I explained in Volume 3, Chapter 13, each political party sets, implements and enforces its own rules for nomination processes. With few exceptions, Elections Canada does not regulate these contests. The only role for Elections Canada in nominations is to oversee a limited set of political finance rules.

Although the evidence before me does not indicate that foreign interference in federal nominations has been widespread to date, nomination contests are nevertheless vulnerable to foreign interference. Interference could manifest

itself via votes at a nomination meeting, or through communications, donations (cash or in-kind) or intimidation (see Volume 2, Chapter 7 and Volume 3, Chapter 13).

Foreign states could also manipulate nomination contests through inauthentic membership purchases. They could buy bulk memberships and assign those memberships to people who will vote as the foreign state wants. Voters who are not Canadian citizens or permanent residents – foreign students from autocratic states, for example – may be susceptible to coercion by their home countries.

Interference is also a risk in party leadership contests. State actors likely see leadership contests as producing greater benefits for them than nomination contests. Political party leaders have considerable authority within their party and could become prime minister.

Political party representatives who testified expressed firm opposition to any form of governmental control of party processes. However, I share the Chief Electoral Officer's view, expressed in his recommendations to the Commission, that the right to vote in nomination and leadership contests should be limited to Canadian citizens and permanent residents. This would likely reduce the use of some foreign interference methods.

Most political parties already have such a membership rule. Enshrining it in law would ensure it is respected, especially if the Chief Electoral Officer or the Office of the Commissioner of Canada Elections, as the case may be, receives some authority to oversee compliance with the rule. It would also increase coherence between political party rules and Canadian electoral law, since only Canadian citizens may vote in federal elections, and only Canadian citizens and permanent residents may contribute to parties, candidates, electoral district associations and leadership and nomination contestants.

I have recently become aware, through media reporting, of the rules established by the Liberal Party of Canada to govern its current leadership race and have noted that voting is restricted to party members who are Canadian citizens, permanent residents or persons with status under the *Indian Act*.

Given that this question was not explored at all in the proceedings before me, I have neither included nor excluded persons having status under the *Indian Act* (and who are not Canadian citizens or permanent residents) from my recommendation on voting rights in nomination and leadership races. However, the fact that I do not mention these individuals should not be taken as a pronouncement one way or the other.

Political parties are private entities and, in our democracy, they have considerable autonomy over their decision-making processes. For this reason, I do not recommend imposing further rules about who should be entitled to vote. Nor do I recommend that the SITE TF monitor and assess nomination and leadership races, although the government may consider making the SITE TF available to monitor a leadership race upon request of a political party. But I strongly encourage all parties and their electoral district

associations to adopt more stringent rules about who is entitled to vote in nomination and leadership contests. These rules could include requiring party membership for a longer minimum period and requiring proof of residency in the riding.

If, while conducting its usual activities, the SITE TF obtains credible and reliable information regarding potential foreign interference in a political party nomination or leadership race, this should be reported to the relevant deputy minister committee, and the party should be alerted. As discussed in Recommendations 28 and 30, the party leader and/or security-cleared representatives should receive the information. The government may wish to consider other ways for the SITE TF to help political parties that choose to approach it.

I also agree with the Chief Electoral Officer that parties and electoral district associations should be required to file their nomination and leadership contest rules with Elections Canada, and file notices of contests before and after they occur. I further agree that all contestants should be required to file a financial return with Elections Canada, not just those who exceed a contribution or expenditure limit.

Section 282.4 of the *Canada Elections Act*, prohibiting undue influence by foreigners, should be amended to apply to nomination and leadership contests, and also should apply at all times (not just during an election period). This is because attempts to influence may happen at any time, and nomination and leadership contests do not necessarily occur during an election or pre-election period.

Finally, I endorse the Chief Electoral Officer's recommendation to expand the prohibitions that apply to elections (bribery and intimidation, for example) to cover nomination and leadership contests.

Recommendation 31

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 district associations 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.
-

Financing

An expert at the policy roundtables pointed out that, from 2004 until 2015, Canadian federal political parties were entitled to a “per-vote subsidy.” This was an annual payment of roughly \$1.75 per year for each vote received in the most recent election. This subsidy created stable funding for political parties. Its elimination may have made party financing more precarious.

In Canada, only Canadian citizens and permanent residents are eligible to give donations to political parties and candidates. Corporate and union donations are illegal. Moreover, there are limits on how much individuals can donate. These measures are intended to ensure that corporate, union and individual interests do not unduly influence Canadian politicians. However, this generates a financial challenge for parties, candidates and other political entities. It may also make them more vulnerable to foreign actors and illegal financing. I have not delved deeply enough into the matter to form an opinion as to what the system should be, but I believe it might be worthwhile for the government to consider the appropriate balance between private and public funding for political parties, since they serve a public interest.

Recommendation 32

32. The government should consider whether it would be appropriate to create a system of public funding for political parties.

Foreign embassies and consulates

Global Affairs Canada (GAC) has frequently engaged with representatives of countries known to engage in foreign interference. The evidence presented to the Commission during its public hearings suggests some foreign interference (and transnational repression) undertaken by foreign diplomatic personnel is carried out through consulates. This evidence implicated consulates in Toronto and Vancouver in particular.

Despite this, there was little evidence presented of direct pre-emptive engagement on foreign interference by GAC with consulates. This presents an opportunity for GAC to clearly communicate its expectations of appropriate diplomatic behaviour with possible sources of the problem. Foreign diplomats in embassies are no doubt aware of the activities of their consulates and may even be directing those activities. Still, consulate staff may feel compelled at least to reduce the scale of their actions once GAC tells them directly that such actions are inappropriate.

Recommendation 33

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

Following the arbitrary detention of two Canadians by the People’s Republic of China in 2018, Canada led like-minded countries in launching a *Declaration against Arbitrary Detention in State-to-State Relations* (“**Declaration**”). To date, 79 countries have endorsed the Declaration, although it remains non-binding. Signatories are largely democracies sharing a belief in the rules-based international order. The Declaration has the stated goal of ending the arbitrary detentions of foreign nationals, but a more realistic result would be to raise the diplomatic costs of engaging in these arbitrary detentions.

Canada has sought to use its own definition of foreign interference, both in Canada and in the governance of the activities of Canadian diplomats abroad. This definition is not recognized by many states. Canada is itself sometimes accused of foreign interference when it openly criticizes the domestic policy of foreign states. There is virtually no possibility of achieving an international treaty to define what constitutes foreign interference. However, as with arbitrary detention, a widely supported international declaration could give Canada strong diplomatic cover to oppose covert, malign and deceptive activities by foreign states, while adding legitimacy to Canadian diplomatic practice abroad.

Recommendation 34

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

The Commission’s mandate concerned only federal democratic institutions and processes. Still, the evidence is clear that foreign interference can potentially target all levels of government, including provincial, territorial, Indigenous and municipal. Moreover, foreign interference is a problem that impacts all of Canada and implicates many areas for which the provinces have constitutional responsibility, such as education. Foreign interference is a whole-of-country problem and so will require whole-of-country solutions that are grounded in inter-governmental collaboration.

The federal government is responsible for ensuring national security and has the resources to do so. It is essential that the federal government intensify its efforts to engage and collaborate with other levels of government to take a more effective stand against foreign interference.

Recommendation 35

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.

19.4 Enforcement

The second line of effort I envision for better protecting federal democratic institutions from foreign interference is enforcement. While Canada cannot just prosecute away the threat of foreign interference, the criminal law is nonetheless an important component of a whole-of-society response to the problem, and essential for maintaining public confidence in democratic processes.

In 2024, the government introduced new criminal and regulatory measures to discourage foreign states and their proxies or co-optees from engaging in foreign interference, and to punish those who do. This legislation serves an important deterrent and signaling function. However, enforcement is key. Failure to meaningfully enforce both new and existing laws could ultimately impair the government’s work to counter foreign interference.

The following section outlines my recommendations to increase Canada’s capacity to enforce domestic law prohibiting foreign interference.

The Royal Canadian Mounted Police

Training on foreign interference

In places where the RCMP serves as police of jurisdiction, RCMP officers serving in frontline or community policing roles are likely the first to engage with targets of foreign interference, including those affected by transnational repression. As a former RCMP Commissioner noted, frontline officers are best placed to “credibly access, engage, communicate with and inform the many affected communities across this country.” These officers need to understand the foreign interference threat so that they know when to call on the RCMP’s Integrated National Security Enforcement Teams to investigate (see Volume 3, Chapter 11).

Recommendation 36

36. All Royal Canadian Mounted Police officers working in affected communities should receive training about foreign interference, including transnational repression.

Resources and staffing

I heard from several witnesses and experts that the RCMP’s Federal Policing sector lacks resources to thoroughly investigate foreign interference offences.

In addition to the technical skills required to conduct foreign interference investigations, these crimes can often involve a transnational element. Transnational investigations can be especially complicated from an evidentiary point of view, and officers require additional resources.

Providing adequate resources to the RCMP and having it recruit, train and retain personnel with the necessary skills to investigate foreign interference should be a priority for the government. Failure to make this a priority could impair the government’s ability to protect Canadians and democratic processes from hostile state actors. Adequate resourcing means not just additional staff, but personnel with critical skill sets not typically acquired during an RCMP career. These skills can include forensic accounting, cyber security, language skills and cultural or geopolitical expertise.

Recommendations 37 and 38

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

Another obstacle to the successful investigation and prosecution of foreign interference offences lies in the intelligence-to-evidence challenge discussed in Volume 2, Chapter 5. National security intelligence is often used to further a criminal investigation and at times can be key to criminal charges. But some intelligence cannot be publicly disclosed for important national security reasons. This inability to disclose information creates obstacles to prosecution.

The RCMP and CSIS have taken procedural steps to address this challenge, but legislative improvements are also required. The government looked at several possible solutions during its public consultations on foreign interference. Two were included in the *Countering Foreign Interference Act*.

The prosecution of foreign interference offences will almost inevitably engage the intelligence-to-evidence issue in challenging ways. Adding new foreign interference offences to the *Criminal Code* and *Foreign Interference and Security of Information Act* is a positive step. Measures proposed in Bill C-65 would also have been positive, but the Bill died on the Order Paper on 6 January 2025. However, successful prosecutions will remain difficult unless the intelligence-to-evidence challenge is more effectively addressed.

Recommendation 39

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

The evidence indicates that our electoral system has been well-served by Elections Canada against foreign interference. Nevertheless, I heard from the Chief Electoral Officer and the Commissioner of Canada Elections about additional steps Canada could take to enforce and strengthen existing electoral law.

Since foreign interference in democratic institutions is not limited to election periods, the *Canada Elections Act* should be amended to prohibit certain activities during the pre-election period as well as the election period. I have already recommended that the provision about undue influence by foreigners apply at all times.

There is precedent for extending the *Canada Elections Act*'s regulation beyond the election period itself. The Act already regulates certain activities – for example, partisan activities, advertising and election surveys – during a defined pre-election period. I agree with the recommendations made by the Chief Electoral Officer that additional provisions of the Act should apply to the pre-election period as well.

Artificial intelligence has made it easier and cheaper to generate and spread misinformation and disinformation. Legal prohibitions will not prevent foreign states from engaging in misinformation and disinformation, but may increase its risk, potentially deterring individuals who might otherwise carry out misinformation and disinformation for a foreign state. Of course, to avoid violating the *Charter*, prohibitions limiting speech, especially political speech, must be narrowly tailored to their purpose. Still, I believe there is room to expand certain existing prohibitions under the *Canada Elections Act* to better protect against foreign interference without unduly limiting the rights of Canadians.

Recommendations 40 and 41

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

As he was invited to do, the Chief Electoral Officer made written submissions with recommendations to the Commission. Those recommendations included tightening some political financing rules, particularly those related to third parties. Some of these recommendations were reflected in Bill C-65, the *Electoral Participation Act*, but this Bill died on the Order Paper when Parliament was prorogued on 6 January 2025.

The *Canada Elections Act* limits the size of annual contributions to political parties, candidates, leadership and nomination contestants and electoral district (riding) associations. The Act also limits spending by political entities, including third parties, on certain activities before and during election campaigns.

Contributions from foreign entities, cash or in-kind, cannot be used for many election activities. Foreign cash contributions are easiest to link to a source, and their value is also easily determined. In-kind contributions, however, can be more difficult to detect and could help foreign entities infiltrate the electoral process more easily.

For most political entities, additional rules apply to promote transparency and ensure that foreign money does not enter Canada's electoral process. However, the rules respecting third parties are substantially different. I heard how these rules do not provide for adequate transparency and can make it difficult to detect illegal contributions (see Volume 3, Chapter 13).

I have carefully reviewed the Chief Electoral Officer's recommendations and their rationale and believe they should be implemented.

Recommendation 42

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

Canadian criminal law relies in part on penalties and fines to deter undesirable behaviour, including foreign interference. Administrative Monetary Penalties (“AMPs”) – while not criminal penalties – are another important tool for promoting compliance with the law. I heard from the Commissioner of Canada Elections of a concern that AMPs and fines in the *Canada Elections Act* are too low.

The maximum AMP for a violation by an individual is \$1,500 and \$5,000 for a corporation or entity. The Commissioner of Canada Elections has suggested raising maximum AMPs, particularly for foreign interference, and I agree. Current AMP levels may offer no deterrent effect since the amounts may simply be seen as a minor cost of doing business. The same is true for fines for offences related to foreign interference, which range from \$2,000 to \$50,000.

Recommendation 43

43. The government should increase maximum administrative monetary penalties as well as fines for violations of *Canada Elections Act* prohibitions applicable to foreign interference.

19.5 Civic resilience

I mentioned at the outset of this chapter that building resilience against foreign interference requires a whole-of-society approach. This is why the third line of effort envisioned by my recommendations is civic resilience. I view building civic resilience as fundamental to combating foreign interference.

Civic resilience is not a given in society. It requires a greater awareness of Canadian civics and understanding of our society, its democratic institutions and their processes, and the roles individuals play in those institutions and processes. That understanding must be cultivated from an early age and must be reinforced and supported daily. Governments at all levels, Canadians and civil society organizations must work together to build and maintain it. To build resilience against foreign interference misinformation and disinformation, efforts must focus on supporting a healthy information environment and on rebuilding and maintaining trust in our public institutions.

A whole-of-society response to foreign interference requires coordination and collaboration with stakeholders, both domestically and internationally. It may involve funding local intervention and support initiatives, financing, planning and coordinating research on how to identify and counter the threat and incorporating that research in the work of frontline responders.

I learned of interesting models in several countries to build civic resilience, especially against misinformation and disinformation. These countries include Finland, Taiwan, Sweden, Denmark and Norway. The Commission did not have the time it needed to examine these models, but the government might usefully consider them in its response to foreign interference, especially foreign interference involving misinformation or disinformation.

There are many tools for increasing civic resilience. These apparently successful models suggest that there is merit in creating a dedicated body to oversee implementation and coordination of the whole-of-society strategy I mentioned.

The evidence shows that foreign state actors are increasingly using the media to interfere in our democratic institutions and processes by spreading disinformation and amplifying division (see, among others, Volume 3, Chapter 10). Civic resilience is therefore essential to defeat it.

Navigating the information environment

Developing civic resilience to misinformation and disinformation requires building the knowledge and skills citizens need to navigate an increasingly complex information environment. At the same time, efforts to counter the spread of misinformation and disinformation must not unduly restrict freedom of expression.

In a healthy democracy, voters have access to a rich information environment where they can hear and voice different perspectives and assess evidence advancing diverse policies. Voters can then take this into account when choosing a candidate or party to support.

Today's information environment makes accessing and weighing evidence and perspectives much more challenging than in the past. Media that abides by a professional code of ethics committed to accuracy, independence, fairness, integrity and respect (i.e. professional media) is giving way to an increasing number of social media and other non-traditional media sources. The growing potential of artificial intelligence (“AI”) to create deepfakes and other materials also makes it more difficult for Canadians to assess whether what they see or hear is real, or what they read is true.

Misinformation and disinformation, both foreign and domestic, are immense threats to democracy that extend far beyond the mandate of this Commission and the scope of its work. Nonetheless, I have a number of recommendations aimed at helping Canadians to navigate the modern information environment.

These recommendations speak to supporting a healthy information environment, developing digital and media literacy, and protecting and promoting information integrity. This will help counter information manipulation.

Supporting professional media

Without strong professional media, Canadians have fewer reliable resources to assess what they are seeing online. It is thus critical that the government continues to support the development of a strong, healthy information environment.

A free press is one of the most important safeguards in a democracy (see Volume 3, Chapter 13). But as we heard from witnesses and experts, traditional journalism is struggling. Media organizations are facing financial challenges as citizens turn away from mainstream media, and towards social media or non-traditional platforms that may, for a variety of reasons, be more susceptible to misinformation and disinformation.

Witnesses from the Department of Canadian Heritage (“**Canadian Heritage**”) spoke about the importance of supporting Canadian media to ensure news is trustworthy and of good quality, and what the government was doing to accomplish this (see Volume 3, Chapters 11 and 13).

I share their concern about Canada’s professional media. Canada must have a press that is strong and free. It is crucial to have credible and reliable sources of information to counterbalance misinformation and disinformation. Professional, independent and appropriately resourced journalism is essential for protecting Canada’s democratic institutions. The measures already put in place by Canadian Heritage are helpful and its efforts to ensure the survival of a strong professional media should continue.

I heard from experts about how declining resources are particularly acute for Canada’s foreign language media. I also heard that foreign language media outlets can be attractive vehicles for foreign state efforts to interfere in Canada’s democratic processes. If media become financially dependent on foreign advertising and investment, they can become more vulnerable to foreign interference. Foreign states can use that dependence to gain control of the material published. It is therefore essential to reinforce the independence of foreign language media in Canada.

Recommendation 44

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.

Promoting access to professional media

However, supporting a free and independent press is not sufficient to ensure civic resilience. All Canadians must also be able to access that information and critically assess it.

Experts in foreign language media drew my attention to barriers some Canadians face in accessing professional Canadian journalistic sources because of language barriers. These barriers could increase vulnerability to foreign interference by cutting off an important source of information that could help individuals to critically assess foreign disinformation campaigns. The government should take steps to reduce these barriers to accessing professional media. AI translation tools may help here.

Recommendations 45 and 46

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

A particular source of concern around misinformation and disinformation is the rapidly developing sophistication of fake images and videos generated by AI. These materials are especially concerning when they target our democratic processes, for example by impersonating politicians. I learned that it can be very difficult, even for experts, to detect deepfakes.

Public awareness that AI can create highly sophisticated disinformation through means such as videos, pictures or robocalls can undermine public trust in genuine material and discourage citizens from taking an interest in public affairs.

This vulnerability is troubling, particularly because AI technology is developing quickly. Rapid change, however, should not prevent the government from working to respond to the dangers of AI. I have already recommended that the impersonation offence under the *Canada Elections Act* be expanded to capture the use of deepfakes. Still, prohibiting deepfakes addresses only a relatively narrow set of circumstances. There may be a need for greater

transparency measures and technological work to be done to better identify deepfakes in other contexts.

Recommendations 47 and 48

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.

I have also reviewed the recommendations made by the Chief Electoral Officer that are relevant to AI, advertising and digital and media literacy and the rationale behind these recommendations. I agree with implementing them.

Recommendation 49

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.
-

Efforts to improve a harmful information environment cannot just rely on healthy options and the regulation of unhealthy ones. Canadians must develop and maintain the ability to critically assess the information environment that shapes our understanding of the world.

Some Canadians are already very well versed on how social media platforms work, how they create echo-chambers, amplify controversial and divisive topics and positions, and how they can distort or corrupt the information environment. This is something all Canadians need to understand. Understanding that we can be vulnerable to social media enables us to better defend ourselves when hostile foreign actors attempt to exploit those vulnerabilities.

Building critical thinking skills requires education. Legislative power over education rests with provincial, territorial and Indigenous governments. For this reason, the federal government must continue to build partnerships to support the development of relevant education programs across the country. The Commission heard that Canadian Heritage has already begun this work (see Volume 4, Chapter 16). These efforts should continue and expand.

Recommendation 50

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

The evidence before me was unequivocal that the vast majority of misinformation and disinformation is spread online, through digital platforms and social media. In my view, it would be no exaggeration to say that online information manipulation poses the single greatest threat to our democracy today. It certainly creates our greatest vulnerability to foreign interference.

In 2023, Canada, along with the Netherlands, launched the *Global Declaration on Information Integrity Online* (“**Global Declaration**”), which establishes a set of high-level international commitments by participating states to protect and promote information integrity online, including government engagement with private industries. Thirty-six countries are now signatories.

In its statement of purpose, the Global Declaration notes that “[w]e are at a global inflection point where taking action to protect the digital information ecosystem is necessary to preserve safe and productive online environments and continue to enjoy the benefits the digital age provides.”¹ I agree.

The Global Declaration expresses the signatory states’ commitment to the core values of freedom of opinion and expression, and the right to information. It also invites online platforms to take steps in a number of key areas, from responsible use of emerging technologies to increased transparency and accountability of algorithms.

In my view, it would be appropriate to begin consultations with the public and private industry on steps Canada can take to implement the principles of the Global Declaration and uphold information integrity online.

Recommendation 51

51. The government should consult with the public, with private industry and with international partners on steps that may be taken to implement the principles of the *Global Declaration on Information Integrity Online*.

19.6 Call to Action on Transnational Repression

I save some of my last words to comment on transnational repression taking place on Canadian soil.

Transnational repression can touch our democratic institutions and processes, but it is much broader than that. It is repression by a foreign state, generally targeting political dissidents or members of diaspora communities living in Canada. It can take many forms, including silencing, coercing, harassing or even harming these people (see Volume 4, Chapter 17 and Volume 6).

Transnational repression is a very complex subject. The Commission did not have the mandate to investigate it in the comprehensive and thoughtful way it requires. However, I am very concerned by what I heard. A resilient civil society is inclusive. Everyone in Canada has the right to freely participate in the public activities central to our democratic processes and to remain safe. Transnational repression denies individuals these rights, and it seems to be on the rise as the world continues to change rapidly.

¹ *Global Declaration on Information Integrity Online*, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/declaration_information_integrity-integrite.aspx?lang=eng

I strongly urge the government to investigate and develop a comprehensive strategy to address transnational repression.

19.7 Evaluation and Assessment

Finally, I note the difficulty in predicting how effective the measures recommended in this chapter will be in practice. Social phenomena do not respond to strict scientific rules about how they will react to changing conditions. Expert advice and research, and in some cases publicly available information about international experiences, suggest that the Commission’s recommendations are sound. But foreign interference threats and threat actors are constantly adapting. There are no simple or certain solutions.

Consequently, the government should regularly assess its efforts to counter the threat and be prepared to adjust its approaches as required. Foreign interference will not cease to be a threat even if every recommendation made is adopted, but it will make Canada more resilient in the face of it.

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 threats, 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 district associations 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