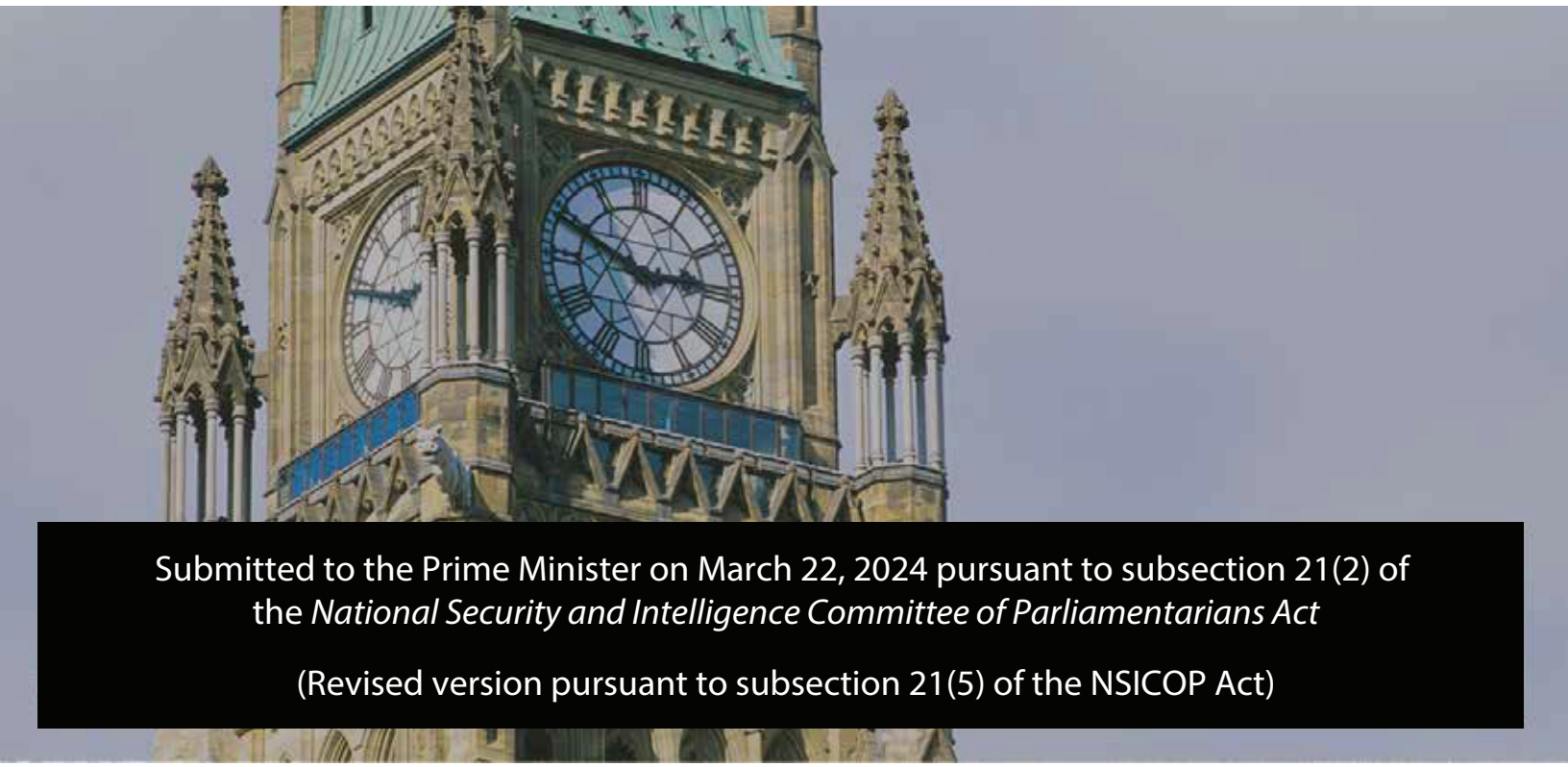
National Security and Intelligence Committee of Parliamentarians

Special Report on Foreign Interference in Canada's Democratic Processes and Institutions



Submitted to the Prime Minister on March 22, 2024 pursuant to subsection 21(2) of the *National Security and Intelligence Committee of Parliamentarians Act*

(Revised version pursuant to subsection 21(5) of the NSICOP Act)

Canada

Ottawa, ON.

The National Security and Intelligence Committee of Parliamentarians

Special Report on Foreign Interference in Canada's Democratic Processes and Institutions (Revised version pursuant to subsection 21(5) of the NSICOP Act)

CP104-6/2024E-PDF
978-0-660-71872-9

CP104-6/2024E
978-0-660-71874-3

Special Report on Foreign Interference in Canada's Democratic Processes and Institutions

The National Security and Intelligence Committee of Parliamentarians

The Honourable David McGuinty, P.C., M.P. Chair

Submitted to the Prime Minister on March 22, 2024
Revised version tabled in Parliament in June 2024

Note

This report is composed of an introduction, four chapters, a conclusion, the Committee's findings and recommendations, and four annexes. The four chapters are almost exclusively based upon classified documentation, mostly summary assessments intended for senior officials or ministers and classified briefings, but also specific reporting from various security and intelligence organizations. This is especially true of Chapter 2 and parts of Chapter 3, where the Committee summarizes trends or specific instances and issues of foreign interference. Readers should note that the Committee has fully or partly redacted references to much of this source material to avoid injury to Canada's national security, national defence or international relations.

Moreover, readers should consider that examples given in the text may refer to any order of government unless otherwise noted in this document.

Revisions

Consistent with subsection 21(2) of the *National Security and Intelligence Committee of Parliamentarians Act* (NSICOP Act), the Committee may submit a special report to the Prime Minister and the ministers concerned on any matter related to its mandate. Consistent with subsection 21(5) of the NSICOP Act, the Prime Minister may, after consulting the Chair of the Committee, direct the Committee to submit to him or her a revised version of the report that does not contain information the Prime Minister believes the disclosure of which would be injurious to national security, national defence or international relations or is information that is protected by solicitor-client privilege.

This document is a revised version of the Special Report provided to the Prime Minister on March 22, 2024. At the time, the document was classified as "Top Secret//Special Intelligence//[Codewords and handling caveats]//Cabinet Confidence//Solicitor-Client Privilege//Canadian Eyes Only." Revisions were made to remove information the disclosure of which the Prime Minister believed would be injurious to national security, national defence or international relations or which constitutes solicitor-client privilege. Where information could simply be removed without affecting the readability of the document, the Committee noted the removal with three asterisks (***) in the text of this document. Where information could not simply be removed without affecting the readability of the document, the Committee revised the document to summarize the information that was removed. Those sections are marked with three asterisks at the beginning and the end of the summary, and the summary is enclosed by square brackets (see example below).

EXAMPLE: [*** Revised sections are marked with three asterisks at the beginning and the end of the sentence, and the summary is enclosed by square brackets. ***]

The National Security and Intelligence Committee of Parliamentarians

(Membership from the 44th Parliament)

The Honourable David J. McGuinty, P.C., M.P. (Chair)

Mr. Stéphane Bergeron, M.P.

Mr. Don Davies, M.P.

The Honourable Patricia Duncan, Senator

Ms. Iqra Khalid, M.P. (ceased being a member on September 17, 2023)

The Honourable Marty Klyne, Senator

The Honourable Frances Lankin, P.C., C.M., Senator

Ms. Patricia Lattanzio, M.P.

Mr. James Maloney, M.P. (ceased being a member on September 17, 2023)

Mr. Rob Morrison, M.P.

Mr. Alex Ruff, M.S.C., C.D., M.P.

Table of Contents

Introduction

1. Beginning in the fall of 2022, media reports allegedly based on leaked intelligence brought the question of foreign interference squarely into the public discourse. They raised questions about what the Prime Minister knew and when, and whether the Government ignored intelligence for partisan advantage. The reports also prompted questions about what the government had done more broadly to respond to interference by the People's Republic of China and other countries in the federal elections of 2019 and 2021, including whether larger systemic negligence was at play. Some parliamentarians and commentators called for a public inquiry.

2. On November 1, 2022, the House of Commons Standing Committee on Procedure and House Affairs initiated a study of foreign interference. The Standing Committee called on Ministers and senior officials to explain how the government has responded to foreign interference activities. It also heard from subject matter experts, interested organizations and community groups about the threat from states conducting interference activities.[1] The House of Commons Standing Committee on Access to Information, Privacy and Ethics launched a similar study on December 7, 2022. Neither standing committee had access to classified information.[2]

3. On March 6, 2023, the Prime Minister requested or announced a number of independent reviews. The Prime Minister asked the National Security and Intelligence Review Agency (NSIRA) to conduct a review of the flow of information from national security agencies to decision-makers during the 43rd and 44th general elections.[3] NSIRA's review focused on the production and dissemination of intelligence on foreign interference, including how it was communicated across the government.[4] (NSIRA submitted its review to the Prime Minister on March 5, 2024.)[5] The Prime Minister also appointed an Independent Special Rapporteur to determine, among other things, whether the government should call a public inquiry into allegations of foreign interference.[6] (The Special Rapporteur concluded that a public inquiry should not be pursued;[7] however, the government ultimately established a public inquiry on

[1] On May 16, 2023, the Standing Committee on Procedure and House Affairs also launched a study on the Question of Privilege Related to the Intimidation Campaign Against the Member for Wellington – Halton Hills and Other Members.
[2] The Committee notes that in October 2020 the Special Committee on the Canada – People's Republic of China Relationship commenced a study of the national security dimensions of the Canada – China relationship, including foreign interference, and published a report in May 2023.
[3] Prime Minister, "Taking further action on foreign interference and strengthening confidence in our democracy," March 6, 2023.
[4] National Security and Intelligence Review Agency (NSIRA), "Terms of Reference for the NSIRA Review of the Government of Canada's production and dissemination of intelligence on foreign interference in the 43rd and 44th Canadian federal elections," May 23, 2023.
[5] NSIRA, Letter to the Chair of NSICOP, March 5, 2024.
[6] Prime Minister, "Taking further action on foreign interference and strengthening confidence in our democracy," March 6, 2023; Prime Minister, "Prime Minister announces mandate of Independent Special Rapporteur," March 21, 2023.
[7] David Johnston, *First Report – The Right Honourable David Johnston, Independent Special Rapporteur*, May 23, 2023.

September 7, 2023.)[8] Finally, the Prime Minister requested that the National Security and Intelligence Committee of Parliamentarians (the Committee) "complete a review to assess the state of foreign interference in federal election processes" with respect to "foreign interference attempts that occurred in the 43rd and 44th federal general elections, including potential effects on Canada's democracy and institutions."[9]

4. In response to the Prime Minister's request, the Committee decided to conduct a broader review, expanding its scope beyond the federal election process to Canada's federal democratic processes and institutions (defined at paragraph 7, below).[10] It did so for two reasons. First, the Committee had already completed a review of foreign interference in 2019 and was well aware of how states try to manipulate Canadian politics and society in support of their own national interests. As such, the Committee understood that elections, while critical, are part of a broader continuum of effort aimed at interfering with Canadian democratic processes and institutions. Second, the Committee wanted to focus its efforts where it has greatest value: access to highly classified information that cannot be discussed in public. The Committee relied in large part on classified materials, briefings and appearances to inform its understanding of the state of foreign interference in Canada's democratic processes and institutions and the government's response.

Scope

5. This report builds on the Committee's 2019 review, which was a broader examination of foreign interference in Canada. It included a detailed review of the main threat actors, their motivations, and foreign interference tactics and targets, and an examination of the government's response to the threat, including cooperation and deconfliction, resourcing and prioritization, and legislative frameworks. The 2019 review did not specifically examine foreign interference activities directed at the 43rd federal election given the government's nascent efforts in this area at the time.

6. This review seeks to avoid duplicating the Committee's previous work. It is clear to the Committee that foreign actors continue to carry out interference activities in Canada. The key threat actors, including their motivations, tactics and techniques, largely remain the same, although this review describes what has evolved and what intelligence agencies reported in the time period in question. Moreover, the mandates and legislative authorities of the departments and agencies responsible for responding to foreign interference are also largely unchanged; this review will discuss where there are exceptions.

7. As a result, this review narrowly focuses on the specific threat to Canada's democratic processes and institutions as a subset of the larger foreign interference challenge (see Annex B,

[8] Privy Council Office (PCO), "Government of Canada launches public inquiry into foreign interference," September 7, 2023; and PCO, Terms of Reference: Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, September 12, 2023.
[9] Prime Minister, "Taking further action on foreign interference and strengthening confidence in our democracy," March 6, 2023. The 43rd federal general election took place on October 21, 2019. The 44th federal general election took place on September 20, 2021.
[10] The Committee conducted its review consistent with paragraph 8(1)(a) of the NSICOP Act.

Committee Terms of Reference). The Committee defines democratic processes and institutions as those processes, actors and stakeholders with an integral role in influencing or determining how Canada governs itself. In this respect, key actors and stakeholders include:

- voters;
- political parties, candidates and their staff;
- Parliamentarians and their staff;
- public servants;
- the media;
- lobbyists; and
- community groups.

Key processes include:

- the election itself;[11]
- nomination processes, including leadership races;
- parliamentary business, including parliamentary motions and the legislative process;
- campaigns; and
- fundraising.

8. This review examined information from September 1, 2018 to March 15, 2024, and included the following organizations:

- Canadian Security Intelligence Service (CSIS);
- Communications Security Establishment (CSE);
- Department of Justice (DoJ);
- Elections Canada;
- Global Affairs Canada (GAC);
- The Office of the Commissioner of Canada Elections;
- Privy Council Office (PCO);
- Public Prosecution Service of Canada (PPSC);
- Public Safety Canada (PS); and
- Royal Canadian Mounted Police (RCMP).

9. This review does not examine the impact of foreign interference on democratic principles writ large.[12] This concept was covered in the Committee's previous report, which concluded that the consequences of foreign interference in democratic processes and institutions were clear: it undermines the democratic rights and fundamental freedoms of Canadians; the fairness and openness of Canada's public institutions; the ability of Canadians to make informed decisions

[11] Defined as the processes involved when Canadians vote for their member of Parliament: registering voters, casting ballots, counting ballots and disseminating results.
[12] Democratic principles include freedom of conscience and religion, freedom of thought and expression, freedom of the press, freedom of association, democratic rights, mobility rights, security of the person, and the rule of law.

and participate in civic discourse; the integrity and credibility of Canada's parliamentary process; and public trust in the policy decisions made by the government.[13] The Committee deliberated at length about this distinction, but ultimately decided that given its previous work and the ongoing efforts by other parliamentary committees to study foreign interference, its value lay in a more focused review of democratic processes and institutions drawing on highly classified materials.

Methodology

10. In support of the review, the Committee requested material from CSIS, CSE, the RCMP, PS, GAC and PCO, examining approximately 4000 documents totalling over 33,000 pages. It also relied on secretarial briefings and departmental responses to written questions. Senior officials appeared before the Committee, sometimes more than once, from CSIS, CSE, the RCMP, PS, GAC and PCO. Given their important roles in addressing aspects of foreign interference, senior officials from the Public Prosecution Service of Canada, Elections Canada and the Office of the Commissioner for Canada Elections also briefed the Committee. In the final stage of its review, the Committee held appearances with the Minister of Justice; the Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs; the Minister of Foreign Affairs; and the Prime Minister. The Committee extends its gratitude to Ministers and officials for their time, candour and expertise.

11. In considering information received for this review and conclusions from its previous review of foreign interference, the Committee noted the intelligence community's consistent assessment that threat actors continue to consider Canada a permissive environment, viewing interference activities as a low-risk, high reward way to pursue strategic interests.[14] This assessment has informed the Committee's analysis of review appearances and materials, raising several key questions:

- Has the government's response to this threat contributed toward the perception by foreign states that Canada's democratic processes and institutions are an easy target?
- If effective threat mitigation seeks to counter a hostile actor's intent, capability and opportunity to act, how and where are Canada's democratic processes and institutions most vulnerable?

The Committee used this analytical lens to develop its assessment, findings and recommendations, which are intended to provide the government clarity on where gaps persist and where action must be taken.

[13] National Security and Intelligence Committee of Parliamentarians (NSICOP), *Annual Report 2019*, 2020.
[14] Canadian Security Intelligence Service (CSIS), *** 2022; and CSIS, Email response to question from NSICOP Secretariat, December 11, 2023.

Chapter 1: Understanding foreign interference and its challenges

12. The term "foreign interference" is not codified in Canadian law, but is generally understood to mirror the CSIS Act definition of foreign influenced activities "within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person."[15] Since the Committee's last review, the definition of foreign interference has evolved as the threat has gained prominence in the security and intelligence community. In its 2021 report on threats to Canada's democratic process, CSIS stated:

> Broadly speaking, foreign interference includes attempts to covertly influence, intimidate, manipulate, interfere, corrupt or discredit individuals, organizations and governments to further the interests of a foreign country. These activities, carried out by both state and non-state actors, are directed at Canadian entities both inside and outside of Canada, and directly threaten national security.
>
> Foreign interference involves foreign states, or persons/entities operating on their behalf, attempting to covertly influence decisions, events or outcomes to better suit their strategic interests. In many cases, clandestine influence operations are meant to deceptively influence Government of Canada policies, officials or democratic processes in support of foreign political agendas.[16]

13. In the context of democratic processes and institutions, foreign interference can be a single act or a series of activities or behaviours over a period of time, throughout which a foreign state conceals its efforts to influence decision-making.[17] States engage in foreign interference in pursuit of a number of objectives, ranging on a spectrum from strategic to tactical. Strategic objectives include building or maintaining a positive or uncritical view of the state and its activities in Canada, and creating a disincentive to criticize a state's domestic policies or practices. Tactical objectives serve the strategic goal, such as impeding, blocking or altering Parliamentary studies, motions or law-making that the state perceives as detrimental to its interests, or instructing individuals to undermine or support the efforts or aspirations of ethnocultural groups within Canada.

14. As will be described in Chapter 3, foreign interference activities in Canada in the period under review were conducted predominantly through person-to-person interaction, which the Committee referred to in its previous report as "traditional" foreign interference.[18] Foreign actors seek to cultivate long-term relationships with Canadians who they believe may be useful in

[15] CSIS Act, section 2.
[16] CSIS, *Foreign Interference: Threats to Canada's Democratic Process*, July 2021.
[17] CSIS, *** 2022.
[18] As opposed to cyber-driven foreign interference methods such as hack-and-leak operations and disinformation campaigns. NSICOP, *Annual Report 2019*, 2020.

advancing their interests, with a view to having the Canadian act in favour of the foreign actor and against Canada's interests.

15. In this respect, foreign interference should be understood as a long-term effort, akin to espionage, using inducements or threats. Both dynamics enable the manipulation of targets when required, for example, through requests for inappropriate or special favours. Inducement typically involves two steps. First, a foreign actor offers the influential Canadian money or other favours. This may include direct payments, cash, in-kind campaign contributions, investment in their region, all-expenses-paid trips to the foreign country, or promises of an employment opportunity or a paid position requiring little to no work after leaving public office. This is intended to build a sense of debt or reciprocity. Second, once the Canadian accepts the foreign government's money or another favour, the foreign actor uses it as a "bargaining chip" to gain leverage over their target.[19]

16. The process may go on for years, and may develop at a slow enough pace that allows some Canadian targets to avoid, at least for a while, having to confront head-on that they are engaged in or assisting foreign interference. Some influential Canadians may self-censor on issues considered by a foreign country to be contentious, while others may internalize foreign messages and align themselves with the positions of these countries. Others may take action in the interest of the foreign state regardless of Canada's position, and may even act in ways detrimental to Canada's interests.[20]

17. Foreign actors also employ coercive techniques to discourage efforts to counter the foreign state's interest. These include denying visas, ordering the withdrawal of community support through votes or funds, or threatening the livelihood or benefits of family members living in the foreign state.

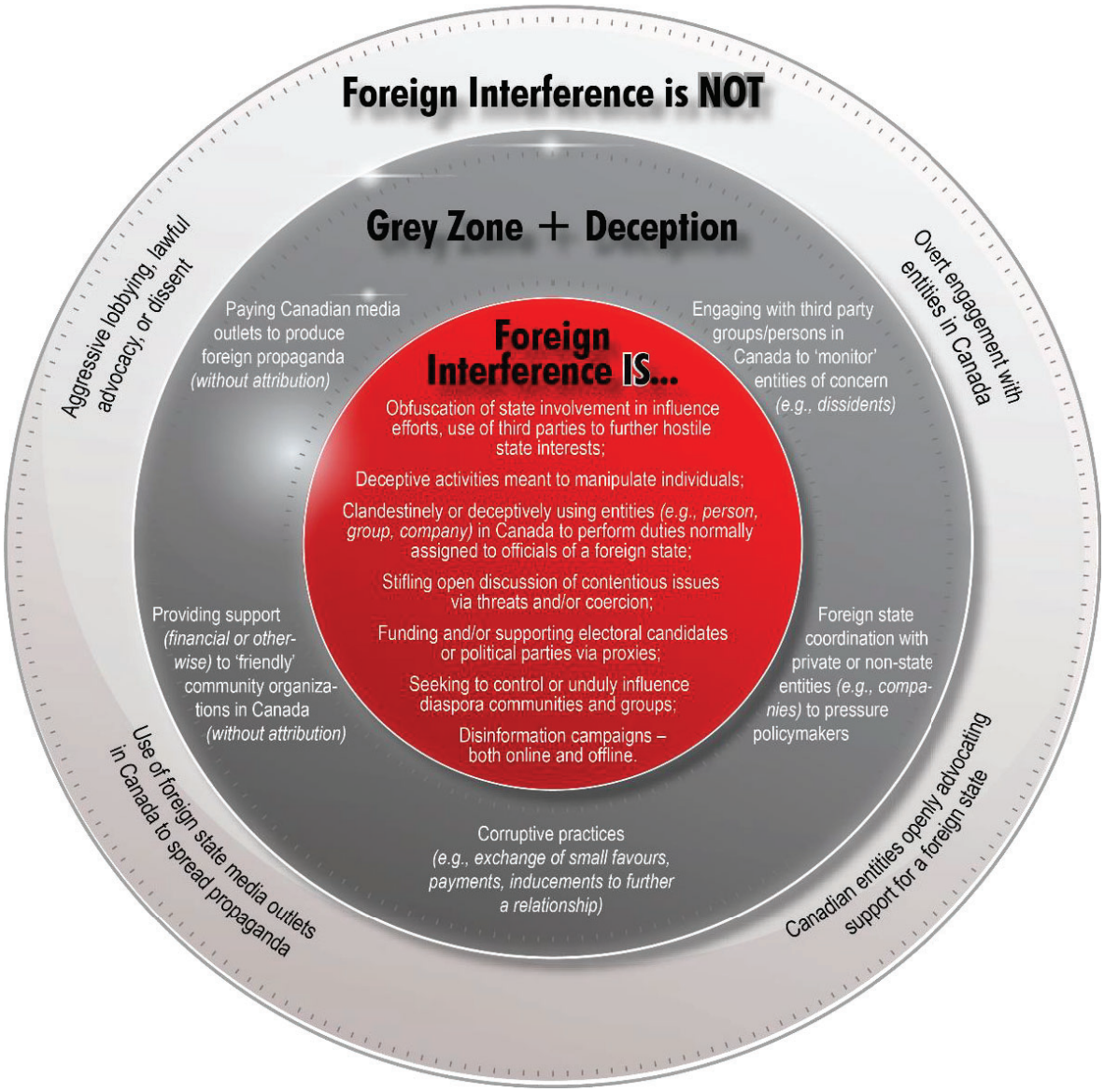
18. Foreign interference activities are distinct from acceptable diplomatic advocacy and lobbying. The latter activities are known to the host state and occur through recognized channels to achieve specific policy outcomes or objectives. It is normal for foreign diplomats in Canada, for example, to reach out to elected officials across the political spectrum, to pressure policymakers, to use local media to promote their national interests or to engage with and support domestic organizations. Canadian diplomats do the same abroad, advocating for Canadian strategic interests, seeking out influential state actors, and supporting initiatives that a host country may not fully welcome, such as pro-democracy projects. Whether employed in Canada or in another country, these activities are overt, declared to the host state, and consistent with the *Vienna Convention on Diplomatic Relations*. Foreign interference activities are not.

[19] Alliance Canada Hong Kong, *In Plain Sight: Beijing's unrestricted network of foreign influence in Canada*, May 2021.
[20] CSIS, *** 2022.

19. The Committee heard repeatedly from officials that identifying the line between foreign influence and foreign interference is not a straightforward exercise. Sophisticated foreign actors use a mix of both overt and covert activities. For this reason, significant amounts of foreign interference fall into a legal and normative "grey zone" (see Figure 1 below).[21] For example, it is not illegal for a foreign state to coordinate with a private or non-state entity to pressure policymakers. This activity becomes interference when the foreign state seeks to hide its involvement, direction or funding. Similarly, it is not illegal to pay Canadian media to produce coverage that portrays a foreign state in a positive light or to amplify the official policy of a foreign state. When that state conceals its involvement, however, this activity is no longer within the bounds of acceptable diplomacy and lobbying: it is foreign interference.

[21] CSIS, *** 2021.

Figure 1: Foreign Interference



20. Another challenge is determining whether an activity is state-directed given efforts by the state to conceal its work. For this reason, it can be difficult to identify whether an individual is a target of foreign interference (e.g., unaware that a foreign state is acting on their behalf to support their candidacy), an unwilling accomplice (e.g., due to threats of sanctions), or a witting participant (e.g., knowingly taking direction from a foreign diplomatic mission).[22] Hostile states are aware of this grey zone and take advantage of it.[23]

[22] CSIS, *** 2022.
[23] CSIS Director, NSICOP appearance, May 9, 2023.

21. For example, a common tactic used to advance foreign interference is the use of proxies. A proxy is a Canadian or a person residing in Canada with a formalized relationship with the foreign state who wittingly and knowingly conducts activities on behalf of the foreign state's interests. This tactic distances the threat activity from the foreign actor, giving the latter plausible deniability for their actions. A similar tactic uses co-optees. CSIS considers a co-optee as an individual who does not have a formal relationship with the foreign state, but is, to varying degrees of awareness, used by the state to further its interests.[24]

22. Foreign interference activities ebb and flow according to foreign states' strategic considerations. Historically, the shape and scope of foreign interference in Canada have been determined by factors such as a state actor's ability and willingness to deploy resources for foreign interference activities; whether a state actor believes its actions will be met with meaningful consequences; and, whether a state's homeland-related conflict has extended into Canada.[25] Foreign interference can also increase or decrease around major events: most notably for the purposes of this review, intensifying during election periods, which represent unique windows of opportunity for foreign actors to exert influence on all orders of government.[26] CSIS notes,

> …for some foreign states, the decisions and policy stances of the federal, provincial, and municipal governments may negatively affect their core interests. As the world has become ever smaller and more competitive, foreign states seek to leverage all elements of state power to advance their national interests and position themselves in a rapidly evolving geopolitical environment.[27]

[24] CSIS, Written response to NSICOP Secretariat, November 20, 2023.
[25] CSIS, *** 2018.
[26] CSIS, *** 2022.
[27] CSIS, *Foreign Interference: Threats to Canada's Democratic Process*, July 2021.

Chapter 2: The threat of foreign interference in Canada's democratic processes and institutions

23. This chapter describes the primary threat actors and outlines the four main tactics that these states have used since 2018, specifically:

- covertly influencing the opinions and positions of voters, ethnocultural communities and parliamentarians;
- leveraging relationships with influential Canadians;
- exploiting vulnerabilities in political party governance and administration; and
- deploying a variety of cyber tools to attain specific objectives.

Throughout this chapter, the Committee includes examples and case studies to illustrate the threat.

24. Foreign interference activities in Canada's democratic processes and institutions in the period under review were conducted predominantly through person-to-person interaction.[28] Foreign states also used mainstream and social media, and other digital means, to conduct interference activities. Interference activities in democratic processes and institutions were conducted by foreign diplomats, intelligence officers, state proxies and co-optees, and targeted all orders of government, civil society groups, ethnocultural communities, community organizations, businesspersons and journalists.

Key threat actors

25. In its 2019 review of the Government Response to Foreign Interference, the Committee noted that the most significant perpetrators of foreign interference in Canada were the People's Republic of China (PRC) and the Russian Federation, with the PRC representing the greatest foreign interference threat. The Committee also noted that other states, including India, ***, Pakistan and Iran engaged in foreign interference activities. The Committee found that these activities posed a significant risk to national security, principally by undermining Canada's fundamental institutions and eroding the rights and freedoms of people in Canada.[29]

26. Between September 1, 2018 and November 7, 2023, foreign interference targeting democratic institutions and processes remained largely consistent with the broader trends the Committee identified in its previous review. Most notably, the PRC remained the largest foreign interference threat to Canada, including to its democratic institutions and processes.[30] The PRC's foreign interference efforts continue to be sophisticated, persistent and multi-

[28] NSICOP, *Annual Report 2019*, 2020.
[29] NSICOP, *Annual Report 2019*, 2020.
[30] CSIS, *** 2018; CSIS, *** 2021; PCO, *** 2022; CSIS, *** 2022; and CSIS, *** 2022.

dimensional, targeting all orders of Canadian government and various facets of society and relying upon a number of methods.[31]

27. However, contrary to its assessment in 2019, which noted that Russia was the second most significant foreign interference threat, the Committee observed that Russia did not engage in foreign interference activities within the more narrow context of Canadian democratic institutions and processes. In this period of review, Canada was a lower-level priority for Russia, which focused its efforts instead on other strategic priorities and its adversarial competition with the United States.[32] In short, while Russia maintained the capability to engage in foreign interference generally against Canada, it lacked the intent to do so.[33]

28. Instead, India emerged as the second-most significant foreign interference threat to Canada's democratic institutions and processes. While India's foreign interference efforts have slowly increased ***,[34] it became clear during the period of this review that its efforts had extended beyond countering what it perceived as pro-Khalistani efforts in Canada to include interfering in Canadian democratic processes and institutions, including through the targeting of Canadian politicians, ethnic media and Indo-Canadian ethnocultural communities.[35] The Committee notes that Pakistan also targeted democratic institutions and processes in the early phase of the period under review, ***.[36]

29. A number of states conducted activities that undermined the democratic rights and freedoms of Canadians during the time under review. In addition to the foreign states mentioned above, *** and Iran continued to monitor and repress respective ethnocultural communities in Canada (see textbox on transnational repression below).[37] However, the Committee did not observe any intelligence reporting about these three states engaging in foreign interference activities targeting Canadian democratic processes and institutions.[38]

[31] CSIS, *** 2021.
[32] CSIS, *** 2020.
[33] SITE, *Security and Intelligence Threats to Elections Task Force, After Action Report (2019 Federal Election),* July 2020; and SITE, "Key Observations from GE44: Review of Principal Threat Actors and Elections Security," "Update to the Panel," after action report for the 2021 election, Deck, November 5, 2021.
[34] CSIS, *** 2021.
[35] CSIS, *** 2021.
[36] CSIS, *** 2023.
[37] CSIS Director, NSICOP appearance, June 26, 2023.
[38] CSIS, *** 2020; CSIS Director, NSICOP appearance, June 26, 2023.

Transnational repression

Transnational repression refers to the exertion of control of an ethnocultural community by a foreign state through monitoring, coercion, harassment, intimidation or violence. States deploy a wide range of tradecraft to carry out repression, including human intelligence collection, online monitoring, cyber attacks, coercion by proxy, controlling mobility by selectively providing consular services (such as visas), harassment and threats of violence, threats and harm to family members, forced repatriation and, in some cases, physical violence.[39]

These states target ethnocultural communities primarily to maintain their grip on power and control global narratives about their own domestic regimes. Central to this tactic is the targeting of overseas dissidents, exiled communities and critics, including journalists and human rights activists. The message that state-sponsored repression aims to send to ethnocultural communities is clear: regime opposition will not be tolerated anywhere in the world and Western democracies cannot offer protection from the regime or guarantee fundamental rights.[40]

During the period under review, the primary perpetrators of repression against ethnocultural communities in Canada were the PRC, India, ***, Iran, *** and ***.[41] Observed transnational repression focused on fundamental rights and freedoms (e.g., freedom of expression), but did not directly target democratic institutions and processes.

One means by which the PRC has engaged in transnational repression received attention by the media in late 2022. In September 2022, a report published by the non-governmental organization (NGO) Safeguard Defenders alleged that the PRC had established a series of "Overseas Police Stations" in countries around the world, including Canada. ("Overseas Police Station" is derived from the term "Police-Overseas Chinese Liaison Stations," which itself is a direct translation from the Chinese term used by the PRC.[42]) Subsequent investigation *** confirmed these reports.[43]

As of March 2023, there were at least seven stations in Canada: three in Toronto, two in Vancouver and two in Montreal.[44] The stations were housed in various locations, including a residence and a convenience store, and reportedly provided PRC-related administrative services, such as renewing PRC driver's licences.[45] According to PCO, Canadian community

[39] CSIS Director, NSICOP appearance, June 26, 2023; and CSIS, *** 2022.
[40] CSIS Director, NSICOP appearance, June 26, 2023.
[41] CSIS Director, NSICOP appearance, June 26, 2023.
[42] Safeguard Defenders, *110 Overseas: Chinese Transnational Policing Gone Wild,* September 2022. As described in the following paragraphs, these PRC 'police stations' have no equivalent to Canadian police functions.
[43] CSIS, CSIS Security Alert: 'Police Stations' in Canada a Part of Ongoing PRC Interference," December 5, 2022.
[44] House of Commons' Special Committee on the Canada – People's Republic of China Relationship, *The Chinese Communist Party's Overseas Police Service Stations*, Interim Report, November 2023.
[45] CSIS, *** 2022; PCO, *** 2022; and PCO, "People's Republic of China (PRC) Overseas Police Stations," Memorandum for the Prime Minister, undated (written on or after November 4, 2022).

leaders ran the stations under the broad direction of PRC-based Ministry of Public Safety police officers.[46]

The PRC established these stations without Canada's permission and in contravention of the *Foreign Missions and International Organizations Act.* CSIS assessed that a key purpose of these stations was "to collect intelligence and monitor former PRC residents living in Canada as part of the PRC's broader transnational anticorruption, repression, and repatriation campaign."[47] PCO similarly assessed that the stations represented the "institutionalization and intensification of [the PRC's] pre-existing extraterritorial law enforcement efforts," which it assessed were likely to continue, albeit with more emphasis on covert tactics.[48]

The United States (U.S.) has taken steps to respond to these Overseas Police Stations. In April 2023, the Federal Bureau of Investigation charged two Chinese-Americans, both U.S. citizens, with conspiring to act as PRC agents by establishing one of these stations in New York, under an offence that does not exist in Canada because Canada does not have a foreign agent registry.[49]

[*** Two paragraphs were deleted to remove injurious or privileged information. The paragraphs described CSE's response, including to provide intelligence to CSIS and the RCMP, and GAC's use of diplomatic tools with respect to the PRC. ***][50] [51]

In late October 2022, the RCMP announced that it was investigating.[52] In March 2023 the RCMP informed the House of Commons Standing Committee on Procedure and House Affairs (PROC) that uniformed RCMP officers had attended four stations, which reportedly ceased their operations afterwards.[53] In April 2023, the Minister of Public Safety informed PROC that the RCMP had "taken decisive action to shut down the so-called police stations,"[54] and in June 2023 the National Security and Intelligence Advisor (NSIA) informed PROC that the RCMP's investigations were ongoing.[55] As of November 2023, no charges had been laid.[56]

[46] PCO, *CHINA: Overseas Police Stations Expanding 'Law Enforcement without Borders'*, November 7, 2022.
[47] CSIS, "CSIS Security Alert: 'Police Stations' in Canada a Part of Ongoing PRC Interference," December 5, 2022.
[48] PCO, *CHINA: Overseas Police Stations Expanding 'Law Enforcement without Borders,'* November 7, 2022.
[49] U.S. Attorney's Office, "Two Individuals Arrested for Operating Undeclared Police Station of the Chinese Government in Chinatown in Manhattan," April 17, 2023.
[50] CSE, NSICOP appearance, May 18, 2023.
[51] PCO, "People's Republic of China (PRC) Overseas Police Stations," Memorandum for the Prime Minister, undated (written on or after November 4, 2022).
[52] RCMP, "Reports of criminal activity in relation to foreign 'police' stations in Canada," media statement, October 27, 2022.
[53] RCMP Deputy Commissioner, PROC Evidence, March 2, 2023.
[54] Hon. Marco Mendicino, Minister of Public Safety, PROC Evidence, April 27, 2023.
[55] NSIA, PROC Evidence, June 1, 2023.
[56] House of Commons' Special Committee on the Canada – People's Republic of China Relationship, *The Chinese Communist Party's Overseas Police Service Stations*, Interim Report, November 2023.

The House of Commons' Special Committee on the Canada – People's Republic of China Relationship has also studied this issue and in November 2023 released an interim report.[57]

[57] House of Commons' Special Committee on the Canada – People's Republic of China Relationship, *The Chinese Communist Party's Overseas Police Service Stations*, Interim Report, November 2023.

Key tactics

Covertly influencing the opinions and positions of voters, ethnocultural communities and parliamentarians

30. Foreign states relied on a range of tactics to covertly influence opinions and positions. They sought to manipulate public opinion through traditional and social media, including through disinformation campaigns; sought to covertly exploit ethnocultural communities, most notably to influence their voting preference; and targeted and attempted to intimidate parliamentarians. The Committee describes each of these methods below, focusing on federal democratic processes and institutions while also providing several examples from other orders of government.

Exploiting traditional and social media

31. During the period under review, the intelligence community observed states manipulating traditional media to disseminate propaganda in what otherwise appeared to be independent news publications.[58] Foreign states also spread disinformation to promote their agendas and consequently challenge Canadian interests,[59] which posed the greatest cyber threat activity to voters during the time under review.[60] These tactics attempt to influence public discourse and policymakers' choices, compromise the reputations of politicians, delegitimize democracy or exacerbate existing frictions in society.[61]

Disinformation refers to false or misleading information that is spread deliberately, as opposed to **misinformation**, which is spread unwittingly. It is a term often employed as shorthand for the broader challenge of information manipulation. In addition to false information, disinformation includes:

- The omission of facts;
- Inauthentic amplification of narratives;
- Doctored audio/visual content;
- Trolling; and
- Efforts to censor or coerce self-censorship of information.

All aim to distort the public's perception of reality.

Source: Global Affairs Canada, "Rapid Response Mechanism Canada," October 2023.

32. According to the intelligence community, the PRC was the most capable actor in this context, interfering with Canadian media content via direct engagement with Canadian media executives and journalists.[62] [*** Six sentences were deleted to remove injurious or privileged information. The sentences described examples of the PRC paying to publish media articles

[58] PCO, *China's Foreign Interference Activities*, Special Report, January 2022.
[59] CSE, *Cyber Threats to Canada's Democratic Process*, July 2021.
[60] CSE, *Cyber Threats to Canada's Democratic Process*, July 2021.
[61] CSE, *Cyber Threats to Canada's Democratic Process*, July 2021.
[62] CSIS, *** 2019; and CSIS, *** 2021.

without attribution, sponsoring media travel to the PRC, pressuring journalists to withdraw articles and creating false accounts on social media to spread disinformation. ***][63] [64] [65]

33. Online influence and information operations were some of the more difficult tactics for Canadian intelligence agencies to link to the PRC, or indeed any foreign state.[66] Intelligence agencies refer to this as the attribution problem.[67] For example, during the 2021 federal election, the government's Security and Intelligence Threats to Elections Task Force (SITE), an intelligence coordination mechanism created in 2018 to support implementation of the Critical Elections Incident Public Protocol (both SITE and the Protocol are described in Chapter 3), observed online and media activities aimed at discouraging Canadians, particularly of Chinese heritage, from supporting the Conservative Party of Canada.[68] The Conservative Party flagged related concerns to SITE about these developments.[69] While SITE was unable to find clear evidence that linked this activity to specific direction from the PRC government,[70] it did observe indicators of a coordinated campaign.[71] Specifically, different Chinese-language media outlets in Canada adopted the language of a PRC state media article, without specifically attributing it. Most of these media outlets were linked to the PRC via partnership agreements with the China News Service, the Chinese Communist Party's primary media entity servicing Chinese ethnocultural communities, which reports directly to the United Front Work Department, the Chinese Communist Party's central coordinating body for foreign interference activities (see textbox below).[72] Moreover, Chinese social media, notably WeChat, is heavily censored by the PRC. CSIS assesses that messages which appear and remain on WeChat have at least tacit support from the government.[73]

34. The SITE Task Force briefed the Panel for the Critical Elections Incident Public Protocol on these developments. The Protocol sets out the process by which Canadians would be notified of a threat to the integrity of a general election.[74] The Task Force advised the Panel that it could not definitively determine a link to the PRC nor measure the impact of such foreign

[63] CSIS, "Briefing to the Prime Minister on Foreign Interference: Director's Notes," February 9, 2021.
[64] CSIS, *** 2022.
[65] CSIS, *** 2021.
[66] According to CSE, ***online influence operations*** (such as hack-and-leak) are usually part of broader *online foreign influence activities* (OFIA), which are a common tool for adversaries to further their strategic interests, including national security, economic prosperity and ideological goals. Online influence campaigns try to impact civil discourse, influence policy makers choices, exacerbate friction in democratic societies and damage the reputation of public figures, such as politicians. OFIA often exploit misinformation and disinformation. An ***online information operation*** utilizes and affects various types and flows of online information to create a desired impact, which can include cyber compromise of systems. Information operations are considered to be *a type of* influence operation. CSE, Email response to questions from NSICOP Secretariat, February 19, 2024.
[67] SITE, "SITE TF Briefing to Secret Cleared Federal Political Parties: Canada's Foreign Interference Threat Landscape," July 2021.
[68] SITE, "Key Observations from GE44: Review of Principal Threat Actors and Elections Security," "Update to the Panel," after action report for the 2021 election, Deck, November 5, 2021.
[69] Mr. Fred DeLorey, Evidence to PROC, April 25, 2023.
[70] SITE, "Key Observations from GE44: Review of Principal Threat Actors and Elections Security," "Update to the Panel," after action report for the 2021 election, Deck, November 5, 2021.
[71] SITE, *Threats to the Canadian Federal Election 2021*, January 21, 2022.
[72] CSIS, *** 2022.
[73] CSIS, ***.
[74] Government of Canada, "Cabinet Directive on the Critical Election Incident Public Protocol," August 2021.

interference attempts on the election, and noted the difficulty in definitively concluding whether foreign interference took place, given that third parties can proactively further PRC interests with little-to-no tasking.[75] The five deputy ministers on the Panel determined that the threshold for a public announcement was not met as the incident did not threaten Canada's ability to have a free and fair election.[76]

35. More recently, the government identified an information operation targeting the Member of Parliament for Wellington-Halton Hills, Michael Chong. While monitoring digital platforms for the June 2023 federal by-elections, GAC's Rapid Response Mechanism (RRM), established in 2018 as part of a G7 initiative to counter threats to democracy, observed that the operation involved a coordinated network on WeChat, which shared and amplified a large volume of false or misleading narratives about Mr. Chong's identity, background, political stances and family heritage. GAC publicly stated that "…while China's role in the information operation is highly probable, unequivocal proof that China ordered and directed the operation is not possible to determine due to the covert nature of how social media networks are leveraged in this type of information campaign."[77]

36. During the period under review, India also demonstrated the intent and capability to engage in this type of foreign interference through media manipulation.[78] [*** Three sentences were deleted to remove injurious or privileged information. The sentences described an example of efforts to discredit a political party leader using materials drafted by Indian intelligence organizations. ***][79]

Exploiting ethnocultural communities

37. In the period under review, foreign states sought to exploit cultural and linguistic ties with ethnocultural communities and groups in Canada to interfere in Canada's democratic processes and institutions. The PRC was the most prolific actor, supported by its United Front Work Department (see following text box).[80] According to CSIS, members of Chinese ethnocultural communities are primary targets for influence work, relating to the Chinese Communist Party's efforts to control overseas Chinese diaspora populations and co-opt Canadian civil society for its own benefit. [*** One sentence was deleted to remove injurious or privileged information. The sentence described an example. ***][81]

---

[75] SITE, *Threats to the Canadian Federal Election 2021*, December 17, 2021.
[76] Morris Rosenberg, "Report on the Assessment of the 2021 Critical Election Incident Public Protocol," February 20, 2023; and threshold for informing the public as defined by the Government of Canada, "Cabinet Directive on the Critical Election Incident Public Protocol," August 2021.
[77] GAC, "Rapid Response Mechanism Canada detects information operation targeting member of Parliament," August 9, 2023.
[78] CSIS, ***.
[79] ***.
[80] CSIS, "Briefing to the Prime Minister on Foreign Interference," Director's Notes, February 9, 2021; CSIS, *** 2021; CSIS, *** 2021; and U.S. – China Economic and Security Review Commission, "China Overseas United Front Work, Background and Implications for the United States," August 24, 2018.
[81] CSIS, *** 2023.

The United Front Work Department

The United Front Work Department (UFWD), a department of the Central Committee of the Chinese Communist Party (CCP), is the organization primarily responsible for strengthening the PRC's influence and interests abroad.[82] The individual responsible for the United Front Work Department is the fourth highest ranking member of the PRC's seven-person Politburo.[83]

United front work refers to the PRC government's strategy of influencing, through both overt and covert methods, overseas Chinese communities, foreign governments, and other actors to take actions and positions supportive of Beijing's preferred global narrative. While the PRC employs a large network to carry out united front work, the UFWD is responsible for its conception, implementation and oversight.

The CCP is assessed to have spent over USD $2.6 billion on united front work in 2019 – more than it spent on the Ministry of Foreign Affairs. Twenty-three percent of the budget (approximately $600 million) was allocated to influencing foreigners and overseas Chinese, in particular.[84]

United front work has been successful in co-opting or subverting political opponents of the CCP and incentivizing public displays of support for the Party. The UFWD has produced propaganda, suppressed critical narratives, and engaged academics, media, businesses and politicians to influence them to adopt pro-China positions or avoid adopting what the PRC considers anti-China positions.[85]

The United Front Work Department works with the PRC's intelligence agencies.[86] [*** One sentence was deleted to remove injurious or privileged information. The sentence described UFWD methods.***][87]

There is no Western equivalent to united front work.[88] [*** Two sentences were deleted to remove injurious or privileged information. The sentences described CSIS analysis that indicated the PRC is aware of the increased scrutiny of united front work in Western countries

[82] CSIS Director, NSICOP appearance, June 26, 2023; and PCO, *China's Foreign Interference Activities*, Special Report, January 2022.
[83] Alex Joske, *The Party Speaks for You: Foreign interference and the Chinese Communist Party's United Front System*, Australian Strategic Policy Institute, 2020.
[84] Ryan Fedasiuk, "Putting Money in the Party's Mouth: How China Mobilizes Funding for United Front Work," The Jamestown Foundation, Volume 20, Issue 16, September 16, 2020.
[85] CSIS, *** 2021.
[86] Alex Joske, *The Party Speaks for You: Foreign interference and the Chinese Communist Party's United Front System*, Australian Strategic Policy Institute, 2020; and PCO, *China's Foreign Interference Activities*, Special Report, January 2022.
[87] Alex Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World*, Hardie Grant Books, 2022.
[88] CSIS, *** 2023.

and the importance of acting lawfully. The pretence of acting lawfully explains the CCP's opposition to legislation that would make united front work more difficult. ***][89]

38. [*** This paragraph was revised to remove injurious or privileged information. ***] The UFWD operates through a large network that includes front organizations which do not declare their affiliation to the Chinese Communist Party (CCP) and have an additional overt and legal function. These front organizations tasked state-owned enterprises, Chinese-registered private companies, Chinese student organizations, foreign cultural organizations, foreign media, members of Chinese ethnocultural communities, and prominent businesspersons and political figures to engage in democratic institutions and processes in a way that supports the goals of the CCP.[90] During the period under review, a security and intelligence organization took measures to counter these efforts.[91]

39. [*** This paragraph was revised to remove injurious or privileged information. ***] According to CSIS, the PRC views community associations in particular as an important means through which PRC-linked officials can approach the Canadian government and elected officials. CSIS assesses that the UFWD has established community organizations to facilitate influence operations against specific members of Parliament and infiltrated existing community associations to reorient them towards supporting CCP policies and narratives.[92]

40. Not all entities targeted by the UFWD were aware that they were being used or that what they were doing was problematic.[93] Indeed, CSIS emphasized *** that only a small number of people within community associations are witting co-optees or proxies.[94] These organizations often have close relationships with the PRC Embassy and consulates and may rely on financial support for their activities, may benefit from reciprocal favours, including financial and economic incentives or other honours and awards to cooperate with PRC authorities, or may simply support the PRC because of a sense of national pride.[95]

41. That said, there are clear examples of witting and co-opted community organizations engaging in foreign interference in democratic institutions and processes. [*** Six sentences were deleted to remove injurious or privileged information. The sentences described an example of the PRC creating an organization to conduct foreign interference, its work in a specific federal riding, and an unsuccessful effort by a security and intelligence organization to counter these activities. ***][96]

[89] CSIS, *** 2023.
[90] PCO, *China's Foreign Interference Activities*, Special Report, January 2022.
[91] *** 2023.
[92] CSIS, *** 2023.
[93] PCO, *China's Foreign Interference Activities*, Special Report, January 2022.
[94] CSIS, *** 2023.
[95] RCMP, *United Front Work in Canada* *** 2020.
[96] *** 2019.

42. Community organizations and events can be valuable sources of fundraising and help build community support for candidates for political office. [*** Three sentences were deleted to remove injurious or privileged information. The sentences described examples of how the PRC used community organizations to support or undermine candidates in specific electoral districts and at different levels of government. ***][97] [98]

43. Community organizations can also be used in a practice known as "astro-turfing," by which a foreign state can conceal its involvement and instead have it appear that influential Canadians or grass-roots organizations are expressing their own opinions on the issues.[99] For example, CSIS stated, "[b]y co-opting major community associations and leaders, the [Chinese Communist Party] is able to give the impression that the overseas Chinese community, much like the citizens of the PRC, speak with one voice – a voice that supports CCP policies."[100] [*** One sentence was deleted to remove injurious or privileged information. The sentence described an example of PRC efforts to interfere with Parliament's 2021 motion to declare the PRC's treatment of its Uyghur population as a genocide and to express concern about the deterioration of Canada-PRC relations. ***][101]

Targeting parliamentarians for coercion or suppression

44. CSIS and CSE have produced a body of intelligence that demonstrates that foreign actors have targeted federal parliamentarians to collect information to support potential future efforts to coerce them. Foreign actors have also intimidated or pressured parliamentarians who they perceived as having taken political positions counter to theirs.[102]

45. [*** This paragraph was revised to remove injurious or privileged information. ***] The PRC in particular employs this strategy. According to CSIS, the PRC is committed to a wide-scale influence campaign against Canadian federal actors, which is coordinated and executed by PRC officials (see Case Study #1).[103] The PRC's goal is to cultivate and increase the impact of pro-PRC voices in Canada and to marginalize individuals viewed as anti-PRC. CSIS assesses that the PRC categorizes its targets into groups based on their perceived level of support for the PRC.[104] [105] [106]

[97] CSIS, *** 2022.
[98] CSIS, *** 2022.
[99] "Astro-turfing" is a covert tactic that seeks to create "a misleading impression of representing monolithic grassroots communities." Alliance Canada Hong Kong, *Murky Waters: Beijing's Influence in Canadian Democratic and Electoral Processes*, May 2023.
[100] CSIS, *** 2023.
[101] CSIS, *** 2021.
[102] CSIS, *** 2021; and CSIS, *** 2021.
[103] CSIS, *** 2023.
[104] CSIS, *** 2023.
[105] CSIS, *** 2023.
[106] CSIS, *** 2023.

Case Study #1: * Intelligence reporting on the PRC and its distribution within the government ***

[*** Three paragraphs were deleted to remove injurious or privileged information. The paragraphs noted reported efforts by the PRC to tailor its targeted influence operations against federal parliamentarians, centered around supporting pro-PRC legislators and punishing their anti-PRC colleagues, including for their position on what the PRC considers the 'Five Poisons.' The paragraphs also described the limited distribution of this information within government, including, but not limited to, the National Security and Intelligence Advisor (NSIA), the Director of CSIS, the Minister of Foreign Affairs, the Minister of National Defence, and the Chief of Staff to the Prime Minister. The paragraphs also noted a potential risk to some Canadian parliamentarians, notably in the context of their travel to the PRC. ***][107] [108]

[*** This paragraphs was revised to remove injurious or privileged information. ***] In June 2021, CSIS drafted a paper drawing on a range of intelligence reporting to provide a more comprehensive and reliable picture of PRC interference. While the paper circulated unofficially, including to at least one senior GAC official, CSIS did not formally issue the paper until February 13, 2023, because of pandemic-related challenges and delays in obtaining approvals for dissemination.[109] The NSIA subsequently requested that the paper be withdrawn, indicating that the distribution list was too large.[110]

On February 24, 2023, the NSIA held a meeting with the Clerk of the Privy Council and Deputy Ministers from CSIS, CSE, Public Safety and GAC. According to PCO, the NSIA asked CSIS what actions could be taken about the intelligence contained in the report.[111] According to CSIS, Deputy Ministers agreed that the Prime Minister should read the report and requested that CSIS draft a condensed version for the Prime Minister. The Director of CSIS approved the new version on March 9, 2023.[112]

The Prime Minister was not provided the report. In a later response to Committee questions, PCO stated that it was the NSIA's view that "the activity indicated in the report did not qualify as foreign interference, but was rather part of regular diplomatic practice."[113] Indeed, the Director of CSIS only became aware that PCO had not provided the report to the Prime Minister in October 2023.[114] As of February 2024, this report had not been given to the Prime Minister.[115]

[107] CSIS, *** 2023.
[108] *** 2024.
[109] CSIS, Written response to NSICOP Secretariat questions, October 2023; and CSIS, Factual Review of NSICOP Report, January 19, 2024.
[110] CSIS, Written response to NSICOP Secretariat questions, October 2023; and PCO, Written response to NSICOP Secretariat questions, October 2023.
[111] PCO, Written response to NSICOP Secretariat questions, October 2023.
[112] CSIS, Written response to NSICOP Secretariat questions, October 2023.
[113] PCO, Written response to NSICOP Secretariat questions, October 2023.
[114] CSIS, Written response to NSICOP Secretariat questions, October 2023.
[115] PCO, Letter to the Executive Director of the NSICOP Secretariat, March 2024.

46. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described PRC efforts to collect information, including compromising information, on numerous federal actors, including from all political parties and both houses of Parliament. ***][116] [117] [118] [119]

47. [*** This paragraph was revised to remove injurious or privileged information. ***] According to some intelligence reporting, the PRC collected detailed information to produce profiles on some Chinese-Canadian members of Parliament in order to exert influence on them through various people and groups, in Canada and abroad.[120]

48. [*** This paragraph was revised to remove injurious or privileged information. ***] Federal actors of Chinese descent are a particular target of the PRC, due to the expectation that these individuals are or should be more sympathetic to the Chinese Communist Party's (CCP) goals and perspectives.[121] According to CSIS, the PRC could punish Chinese-Canadian legislators who had behaved in ways deemed unacceptable by PRC officials to deter such behaviour in others. Conversely, the PRC could reward Chinese-Canadian legislators for behaviour deemed appropriate by PRC officials by providing benefits both in Canada and the PRC, directly or indirectly (e.g., via family members). In short, the use of rewards and punishments is a routine part of the CCP's coercive approach to manage dissent and influence, within the PRC and abroad.[122]

49. One of the key examples of this practice was the PRC's targeting of Conservative Party of Canada Member of Parliament Michael Chong. In February 2021, Mr. Chong sponsored a vote in the House of Commons to identify the PRC's treatment of its Uyghur population as genocide.[123] [*** One sentence was deleted to remove injurious or privileged information. The sentence described efforts by the PRC to collect information on Mr. Chong and his family. ***][124] According to CSIS, at no time did the intelligence reporting indicate a threat to life, physical harm, or detention of Mr. Chong or his family members.[125] The PRC's objective was to make an example of Mr. Chong in order to deter other parliamentarians from taking "anti-China" positions.[126]

50. Mr. Chong was provided with increasingly detailed information on the PRC's efforts over time. In June 2021, CSIS briefed Mr. Chong on foreign interference threat activities,[127] but could

[116] CSIS, *** 2023.
[117] CSIS, *** 2023.
[118] CSIS, *** 2023.
[119] CSIS, *** 2023.
[120] *** 2023.
[121] CSIS, *** 2023.
[122] CSIS, *** 2023.
[123] CSIS, *** 2021.
[124] CSIS, Memorandum to the Minister re Threat Reduction Measure: PRC Targeting Specific Members of Parliament, signed by the Minister of Public Safety on May 18, 2023.
[125] CSIS, Memorandum to the Minister re Threat Reduction Measure: PRC Targeting Specific Members of Parliament, signed by the Minister of Public Safety on May 18, 2023.
[126] CSIS, *** 2021.
[127] Michael Chong, PROC Evidence, May 16, 2023.

not in its briefing provide classified information owing to the restrictions of s. 19 (1) of the CSIS Act, which limits the sharing of classified information to the federal government. In other words, CSIS was unable to share intelligence with Mr. Chong about the research by the PRC ***. Mr. Chong first became aware of the reported threats to his family on May 1, 2023, in the media.[128] On May 2, at the direction of the Prime Minister, the Director of CSIS provided Mr. Chong with a classified briefing by way of a Threat Reduction Measure under "exigent circumstances."[129] On May 16, 2023, the Minister of Public Safety issued the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians*, which directed CSIS to inform parliamentarians of such threats without delay.[130]

51. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described PRC efforts to collect and use compromising material on federal politicians to intimidate or silence them. ***][131] [132] [133] [134]

Leveraging relationships with influential Canadians

52. This section explores four means by which threat actors employ "traditional" foreign interference through human-to-human relationships. This primarily involves establishing reciprocal relationships with influential Canadians, using clandestine networks, employing proxies, and covertly buying influence with candidates and elected officials. In the period under review, threat actors used all of these levers, often at the same time.

Establishing reciprocal relationships

53. In the period under review, CSIS and CSE produced a body of intelligence that showed that foreign actors used deceptive or clandestine methods to cultivate relationships with Canadians who they believed would be useful in advancing their interests – particularly members of Parliament and senators – with a view to having the Canadian act in favour of the foreign actor and against Canada's interests. In this respect, their efforts extended beyond normal diplomatic activities.

54. In some cases, parliamentarians were unaware they were the target of foreign interference. [*** Two sentences were deleted to remove injurious or privileged information. The sentences described an example of India's financial support to some candidates from two

[128] Michael Chong, PROC Evidence, May 16, 2023.
[129] CSIS, Memorandum to the Minister re Threat Reduction Measure: PRC Targeting Specific Members of Parliament, signed by the Minister of Public Safety on May 18, 2023.
[130] Minister of Public Safety, *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians*, May 16, 2023.
[131] ***.
[132] ***.
[133] ***.
[134] ***.

political parties, and CSIS's assessment that the candidates were unaware of the source of the funds. ***][135] [136]

55. Some elected officials, however, began wittingly assisting foreign state actors soon after their election. [*** Three sentences were deleted to remove injurious or privileged information. The sentences described examples of members of Parliament who worked to influence their colleagues on India's behalf and proactively provided confidential information to Indian officials. ***][137] [138] [139]

56. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described a textbook example of foreign interference that saw a foreign state support a witting politician. CSIS provided specific intelligence to the secret-cleared representatives of the party shortly before the election and to the Prime Minister shortly after. The Prime Minister discussed this incident with the Committee and the steps he took in response to intelligence reporting. ***][140] [141] [142] [143]

57. [*** This paragraph was revised to remove injurious or privileged information. ***] In this context, CSIS assessed that the PRC believes that its relationship with some members of Parliament rests on a *quid pro quo* that any member's engagement with the PRC will result in the PRC mobilizing its network in the member's favour. The PRC would show support for lawmakers in ridings with large numbers of ethnic Chinese voters and who maintain close relationships with the Chinese ethnocultural community, including through Chinese leaders and business people.[144] [145]

[135] ***.
[136] CSIS, Briefing to NSICOP Secretariat, August 2023.
[137] CSIS, ***.
[138] CSIS, *** report for the CSIS director, *** 2020.
[139] CSIS, *2022-2023 Annual s. 6(4) Report to the Minister on CSIS Operational Activities*, August 2023.
[140] CSIS, "PM Briefing: ***.
[141] In response to this intelligence, the Director of CSIS briefed the Panel for the Critical Elections Incident Public Protocol on *** and ***. CSIS, accompanied by PCO, informed Secret-cleared *** representatives on *** and CSIS briefed the Prime Minister on ***. CSIS, "PM Briefing: ***.
[142] CSIS, "PM Briefing: ***.
[143] Prime Minister, NSICOP appearance, November 7, 2023.
[144] CSIS, *** 2023.
[145] CSIS, *** 2023.

*Member of Parliament wittingly provided information *** to a foreign state*

[*** This paragraph was revised to remove injurious or privileged information. ***] The Committee notes a particularly concerning case of a then-member of Parliament maintaining a relationship with a foreign intelligence officer. According to CSIS, the member of Parliament sought to arrange a meeting in a foreign state with a senior intelligence official and also proactively provided the intelligence officer with information provided in confidence.[146] [147] [148]

Clandestine networks

58. [*** This paragraph was revised to remove injurious or privileged information. ***] In the period under review, foreign states developed clandestine networks surrounding candidates and elected officials to gain undisclosed influence and leverage over nomination processes, elections, parliamentary business and government decision-making. Run by foreign states' officials, these informal networks consisted of Canadian ethnocultural community leaders and prominent businesspersons, political staffers, candidates and elected officials. Foreign officials conveyed their candidate preferences to their networks, after which co-optees or proxies promoted the chosen slate to targeted groups of voters.[149]

59. For example, *** the PRC had established an informal foreign interference network in ***, understood in this context to describe complex, overlapping and extensive personal and professional connections.[150] The *** network worked in loose coordination with one another and with guidance from the consulate *** to covertly support or oppose candidates in the 2019 federal election. The *** network had some contact with at least 11 candidates and 13 campaign staffers, some of whom appeared to be wittingly working for the PRC.[151] [*** Two sentences were deleted to remove injurious or privileged information. The sentences described the network's efforts to keep federal political candidates away from events that the PRC considered to be "anti-China," such as a pro-Hong Kong rally; noted similar activities by another network in the riding of Don Valley North; and identified specific individuals involved. ***][152] [153]

60. Officials from the PRC also used clandestine networks to conduct foreign interference in Greater Vancouver. [*** Six sentences were deleted to remove injurious or privileged information. The sentences described the PRC's efforts to leverage its network to support a specific political candidate, noted the work of certain organizations and individuals within the

[146] CSIS, ***.
[147] CSIS, ***.
[148] CSIS, ***.
[149] CSIS, *** 2022.
[150] CSIS, *** 2020; and CSIS, Factual Review of NSICOP Report, January 19, 2024.
[151] Contrary to the media article ***, the *** network did not count eleven candidates in its membership (it had *** central members), but it did have contact with at least 11 candidates. Global News, "Canadian intelligence warned PM Trudeau that China covertly funded 2019 election candidates: Sources," November 7, 2022; CSIS, *** 2020.
[152] CSIS, *** 2020; and PCO, *China's Foreign Interference Activities*, Special Report, January 2022.
[153] CSIS, *** 2019.

network, and noted an effort by a security and intelligence organization to counter the work of one of the individuals. ***][154] [155]

61. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described how India also takes advantage of networks and developed and built a network of contacts through whom it conducts interference activities, including journalists, members of ethnocultural communities and some members of Parliament. ***][156]

62. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described how Pakistan has engaged in foreign interference in provincial and federal politics. The paragraph described how Pakistan interfered in candidate nominations, worked to support a preferred candidate's election, including to mobilize voters and to fundraise, and efforts by a security and intelligence organization to counter these activities. ***][157] [158] [159]

The use of proxies

63. As noted in Chapter 1, foreign states use Canadians as proxies who act at their behest, creating a separation between the threat activity and the foreign actor. As reported elsewhere in this chapter, the PRC also relies on a network of proxies, including prominent businesspeople and community leaders, in major urban centres like Greater Vancouver (see paragraph 60), Greater Toronto (see ***) and ***. The PRC proxy considered by the security and intelligence community to be the most egregious case of foreign interference *** (see Case Study #2).

64. For its part, India has an active proxy, who has proactively looked for ways to further India's interests by monitoring and attempting to influence politicians, ***.[160] [*** Two sentences were deleted to remove injurious or privileged information. The sentences described the importance India ascribes to the proxy, how Indian officials developed and built a network of contacts through whom India conducts interference activities, including journalists, members of ethnocultural communities and some members of Parliament. ***] (***)[161] [162]

65. Political staffers in particular are a sought-after proxy for foreign actors. Staffers can influence or exert some measure of control over a politician by influencing messaging and controlling the calendar of the elected official for whom they work to covertly support the interests of the foreign state.[163] They have also been used to monitor their employers and report back to foreign state actors.[164] [*** One sentence was deleted to remove injurious or privileged

[154] CSIS, *** 2021.
[155] CSIS, *** 2022; *** 2022.
[156] CSIS, *** 2019; and CSIS, *** report for the CSIS Director, *** 2020.
[157] CSIS, *** 2019; and SITE, *After Action Report* (2019 Federal Election), August 2020.
[158] ***.
[159] ***.
[160] CSIS, *** 2021.
[161] CSIS, *** 2020.
[162] CSIS, *** 2021.
[163] CSIS, *** 2022.
[164] CSIS, ***.

information. The sentence described an example of a political staffer passing confidential information to a contact of a foreign state about a politician's activities and donors. ***][165]

Case Study #2 : * A proxy's activities pose a threat to national security**

[*** Twelve paragraphs were deleted to remove injurious or privileged information. The case study described the activities of a PRC proxy. It noted CSIS's assessment that the proxy represented a threat to Canada in every sense of the CSIS Act's s. 2 definition of foreign influence in that their actions over time have been detrimental to the interest of Canada and are clandestine, deceptive and threatening. CSIS further assessed that one aspect of the proxy's behaviour was a **high-risk, high-harm threat** to some Canadians and permanent residents. CSIS has shared information on the proxy with the RCMP. ***][166] [167] [168] [169] [170] [171] [172] [173] [174] [175] [176] [177] [178] [179] [180] [181] [182] [183] [184] [185] [186] [187] [188]

Covertly buying influence with candidates and elected officials

66. In the period under review, intelligence reporting from CSIS and CSE showed that foreign states attempted to covertly buy influence with candidates and elected officials. [*** Five sentences were deleted to remove injurious or privileged information. The sentences described an example of the PRC using intermediaries to provide funds likely to support candidates in the 2019 federal election, including two transfers of funds approximating $250,000 through a

[165] CSIS, ***.
[166] CSIS, *** 2022.
[167] *** 2022.
[168] *** 2022.
[169] *** 2023.
[170] *** 2019.
[171] *** 2021.
[172] *** 2022. ***.
[173] *** 2023.
[174] *** 2021.
[175] *** 2022.
[176] *** 2023.
[177] *** 2023.
[178] CSIS, *** 2023, bold emphasis in original.
[179] *** 2021.
[180] *** 2019.
[181] *** 2021.
[182] *** 2023.
[183] *** 2021.
[184] *** 2023.
[185] *** 2022.
[186] *** 2022.
[187] *** 2022.
[188] NSICOP Secretariat meeting with CSIS officials, August 30, 2023.

prominent community leader, a political staffer and then an Ontario member of Provincial Parliament. CSIS could not confirm that the funds reached any candidate. ***][189] [190] [191] [192]

67. In another example, *** Canadians believed to be proxies for the PRC covertly encouraged individuals to donate money to the campaigns of candidates that the PRC favoured and promised to pay them back, which is an offence under the *Canada Elections Act*.[193] [*** Two sentences were deleted to remove injurious or privileged information. The sentences noted that the RCMP and the Office of the Commissioner for Canada Elections were apprised of this intelligence. ***][194] [195]

68. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described CSIS information that an Indian proxy claims to have repeatedly transferred funds from India to politicians at all levels of government in return for political favours, including raising issues in Parliament at the proxy's request. CSIS did not share this information with the RCMP or with the Commissioner of Canada Elections. ***][196] [197] [198]

Case Study #3: India * funneled funds to some federal candidates ***

[*** Four paragraphs were deleted to remove injurious or privileged information. This case study described an example of India likely reimbursing a proxy who had provided funds to candidates of two federal parties. It noted CSIS's assessment that none of the candidates were aware the funds were from India, and that meetings between newly elected members of Parliament who had received funding and Indian officials were to take place. ***][199] [200] [201] [202] [203] [204] [205] [206]

[189] *** 2019.
[190] *** 2019.
[191] *** CSIS, *** 2023.
[192] CSIS, Factual Review of NSICOP Report, January 19, 2024.
[193] CSIS, ***.
[194] According to CSIS, RCMP provided feedback to CSIS on this intelligence reporting. CSIS, Factual Review of NSICOP Report, January 19, 2024.
[195] CSIS, Factual Review of NSICOP Report, January 19, 2024.
[196] CSIS, *** 2022.
[197] *** CSIS, *** 2020.
[198] CSIS, ***.
[199] These activities were part of a wider campaign of foreign interference *** 2023.
[200] ***.
[201] ***.
[202] ***.
[203] CSIS, Briefing to NSICOP Secretariat, August 2023.
[204] *** 2023.
[205] NSICOP, *Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*, October 12, 2018.
[206] CSIS, Meeting with NSICOP Secretariat, August 2023.

Exploiting vulnerabilities in political party governance and administration

69. In the period under review, foreign actors covertly supported or opposed candidates by exploiting vulnerabilities in political party governance and administration. This included interfering with nomination processes or attempting to influence or control electoral district associations. CSIS considers the nomination process to be a particularly soft target for several reasons.[207] First, many ridings are considered 'safe seats,' so winning the nomination is akin to winning the subsequent election without having to interfere in the election itself. Second, nomination processes are not directly regulated or safeguarded by federal, provincial, or territorial legislation or enforcement bodies, such as the Commissioner of Canada Elections. As a result, the likelihood and consequences of the detection of such activities are low. Unlike Australia and the United Kingdom, Canada does not criminalize interfering in nominations, leadership races, or any other political party process.[208]

70. Third, nomination processes are governed by the different rules of each political party: breaking these rules is not illegal. Each political party has its own rules and requirements for participating in a nomination, such as a minimum age or residency requirement, or whether a membership fee is required to join the party and vote. For example, some parties allow non-citizens to register as party members and vote in a nomination, as long as they live in the riding. *** CSIS assesses that it is relatively easy to fraudulently add voters who live outside a riding to a nomination process's voter list with inaccurate addresses. It is also reportedly relatively easy to show an altered phone bill with the wrong address, or a fraudulent letter from a school, in order to vote in a nomination.[209]

71. *** PRC-linked proxies involved in provincial politics engaged in efforts to control the federal Electoral District Association in ***. In addition to trying to influence the riding's nomination processes (***), they also sought to control the riding's finances. *** Their actions demonstrate how threat actors work across multiple orders of government: the proxies here worked at the provincial and federal levels, and the riding association they targeted was federal.[210]

[207] CSIS, *** 2022.
[208] Parliament of the Commonwealth of Australia, *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*, section 92.2(1)(c)(i), and paragraph 866 of the law's Revised Explanatory Memorandum, 2018; and UK Parliament, *National Security Act 2023*, section 14, 2023.
[209] CSIS, *** 2023; and CSIS *** 2019.
[210] CSIS, *** 2022.

Case Study #4: PRC interference in the Liberal nomination contest in Don Valley North

According to CSIS, the PRC *** had a significant impact in getting Han Dong nominated as the Liberal Party of Canada's 2019 federal candidate in Don Valley North. [*** Three sentences were deleted to remove injurious or privileged information. The sentences described the PRC's objectives and the work of its proxy. ***][211]

The nomination vote occurred on September 12, 2019. Many of Mr. Dong's supporters arrived in buses *** supported by the PRC: between 175 and 200 international Chinese students arrived in several buses. The Consulate reportedly told the students that they must vote for Mr. Dong if they want to maintain their student visas.[212]

The Consulate knowingly broke the Liberal Party of Canada's rule that voters in a nomination process must live in the riding. [*** Three sentences were deleted to remove injurious or privileged information. The sentences noted that the students reportedly: lived outside of the riding; were provided with fraudulent residency paper work; and sought to physically intimidate voters and distribute pro-Dong materials, contrary to Party rules. ***][213] [214]

CSIS assessed that the PRC's foreign interference activities played a *** significant role in Mr. Dong's nomination, which he won *** by a small margin.[215] By successfully interfering in the nomination process of what can be considered a safe riding for the Liberal Party of Canada, the PRC was well-positioned to ensure its preferred candidate was elected to Parliament.[216] [*** Two sentences were deleted to remove injurious or privileged information. The sentences described a CSIS assessment on the degree to which an individual was implicated in these activities. ***][217]

On September 28, 2019, CSIS briefed the Liberal Party of Canada's Secret-cleared representatives on its assessment, who in turn briefed the PM alone the following day.[218] The Liberal Party of Canada allowed Mr. Dong to run in both the 2019 and 2021 federal elections. [*** Two sentences were deleted to remove injurious or privileged information. The sentences described the Prime Minister's discussion with the Committee about Mr. Dong and the steps he took in response to intelligence reporting. ***][219]

[211] CSIS, *** 2021.
[212] CSIS, *** 2022.
[213] CSIS Director, "Notes for DIR PM Brief: Don Valley North in the 2019 Election," February 8, 2020.
[214] CSIS, *** 2020.
[215] CSIS, *** 2019.
[216] Mr. Dong was elected to Parliament by a wide margin: 22,998 votes versus 16,307 for the runner-up. Elections Canada, Results of the 43rd General Election, 2019.
[217] CSIS, *** 2019.
[218] Jeremy Broadhurst, Evidence to PROC, April 25, 2023.
[219] Prime Minister, NSICOP appearance, November 7, 2023.

72. Foreign actors also targeted party leadership campaigns. [*** Three sentences were deleted to remove injurious or privileged information. The sentences described two specific instances where PRC officials allegedly interfered in the leadership races of the Conservative Party of Canada. ***][220] [221]

73. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described India's alleged interference in a Conservative Party of Canada leadership race. ***][222]

74. Foreign actors did not limit their activities to the federal level. [*** Two sentences were deleted to remove injurious or privileged information. The sentences described PRC offers of support to a provincial politician, and its subsequent signalling of that support to trusted contacts, who took specific measures to support the politician. ***][223]

Use of cyber tools to attain specific objectives

75. Threat actors deploy a variety of cyber tools to interfere in democratic processes and institutions. They do so for three main reasons: to undermine the integrity of an election, either directly by corrupting the digital infrastructure on which it depends or indirectly by sowing doubt in the minds of voters; to embarrass political parties and elected officials through the leak of information; and to manipulate voters through disinformation to exploit political fissures. (Online foreign influence posed the greatest cyber threat activity to voters during the time under review, as discussed earlier in paragraph 31).

Cyber attacks on electoral infrastructure

76. Cyber threat activity against electoral infrastructure is largely conducted by state-sponsored actors. These activities include targeting information technology systems that support the election process, owners and operators of elections systems, individuals accountable for elections (e.g., election officials), and vendors of election system hardware and software.[224] States and their proxies engage in this activity to undermine democratic institutions or sabotage election results. This may take the form of targeting electoral processes and infrastructure, altering content on websites and social media accounts of election management bodies, stealing information such as voter registration databases, or compromising the systems or communications underlying the election.[225]

77. Under CSE's Defensive Cyber Operations Ministerial Authorization, CSE planned a defensive cyber operation in anticipation of the 2019 federal election, and again for the 2021 election. In both 2019 and 2021, the threat that the operations would have countered ultimately

[220] CSIS, *** 2020.
[221] CSIS, *** 2022.
[222] CSIS, *** 2022.
[223] CSIS, *** 2022.
[224] SITE, *After Action Report* (2019 Federal Election), August 2020.
[225] CSE, *Cyber Threats to Canada's Democratic Process*, July 2021.

failed to materialize and CSE did not need to conduct the operations. CSE also advised the Committee that for both the 2019 and 2021 federal elections, there was no indication that any foreign cyber threat activity targeted electoral infrastructure.[226]

Cyber attacks on political parties and parliamentarians

78. Foreign states and their proxies also attempt to engage in cyber threat activity to breach the information systems of political parties, candidates and their staff.[227] They do this to disrupt engagement with the public for financial gain, to harm the political party or candidate, or for publicity; to steal sensitive or proprietary information; or to interfere with political party procedures undertaken online.[228] The Canadian intelligence community observed cyber threat activity during the 2019 and 2021 federal elections. However, there was no indication that any threat activity specifically targeted Canadian political parties or elected officials in relation to the federal election. Instead, this activity was likely part of broader, ongoing cyber espionage campaigns.[229]

79. That said, CSE detected state-directed cyber threat activity targeting democratic institutions and processes outside of the election period. For example, a PRC state-directed cyber group started targeting eight members of Parliament and one senator in early 2021. All targeted Parliamentarians were members of the Inter-Parliamentary Alliance on China, an international multi-party group of legislators focused on how democracies should collectively approach issues related to the PRC. The cyber group's reconnaissance activity against Canadian politicians was most likely carried out in an attempt to obtain information on their personal and work devices; however, this cyber activity was unsuccessful. This type of activity is consistent with that in 19 European countries, which have reported similar cyber activity against their legislatures since early 2020.[230]

[226] CSE, "Foreign Interference Review: NSICOP Committee Hearing", May 18, 2023.
[227] SITE, *After Action Report* (2019 Federal Election), August 2020.
[228] CSE, *Cyber Threats to Canada's Democratic Process*, July 2021.
[229] SITE, *After Action Report (2019 Federal Election)*, August 2020; SITE, *Key Observations from GE44*, November 5, 2021; and SITE, *Threats to the Canadian Federal Election 2021*, December 17, 2021.
[230] CSIS, ***, *** 2021.

Chapter 3: The government's response

80. This chapter outlines the government's response to the threat of foreign interference in democratic processes and institutions (see Annex C). In this context, the Committee considers the government's response to include two broad policy initiatives: first, initiatives to protect Canada's democratic processes and institutions *** adopted by the government between 2018 and 2023 and the implementation of those initiatives; and second, efforts to amend the legislative frameworks for investigating, prohibiting, preventing or countering this threat. This chapter also examines the government's efforts to brief parliamentarians on the threat of foreign interference, its operational response to threat of foreign interference using existing mandates and authorities, and interdepartmental governance of the file.

Policy initiatives

The Plan to Protect Democracy (*** 2018)

81. Canada's strategic response to foreign interference in democratic processes and institutions must be understood in the context that brought the issue to the fore. As noted earlier, Russia carried out an influence campaign aimed at the United States (U.S.) in the 2016 presidential election with the goal of undermining public faith in the U.S. democratic process and discrediting the candidacy of Hillary Clinton.[231] It did so by leveraging social media to provoke and amplify political and social discord in the U.S., including by purchasing political advertisements and staging local political rallies. This influence effort was complemented by targeted cyber hacks and the release of materials damaging to the Clinton campaign.[232] The U.S. intelligence community was aware of Russian efforts during the presidential campaign, but the central challenge for the U.S. government during those events was how to inform the American public of Russia's interference without appearing to unduly influence the course of the election. Russia would go on to employ similar "hack-and-leak" and disinformation campaigns in the United Kingdom in 2016, France in 2017, and Germany in 2017.[233]

82. These events shaped Canada's early efforts to counter foreign interference in its elections. In February 2017, the Prime Minister tasked the Minister of Democratic Institutions to work in collaboration with the Ministers of Public Safety and National Defence to lead the government's efforts to defend the Canadian electoral process from cyber threats.[234] The Minister of Democratic Institutions developed a four-pillar framework, intended to serve as the architecture for Canada's efforts to combat foreign electoral interference. The four pillars were:

[231] United States Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," January 6, 2017.
[232] United States Government, Mueller Report, 2019.
[233] PCO, "Case Studies for Panel - Summaries of AUS, FR, GER, IRE, UK, US," September 12, 2019.
[234] Prime Minister's Office, "Minister of Democratic Institutions Mandate Letter," February 1, 2017.

- Combating foreign interference through increased threat awareness and international coordination;
- Promoting institutional resilience by supporting key stakeholders (e.g., government institutions, political parties, media, etc.) to effectively plan for, respond to, and mitigate electoral interference;
- Building citizen resilience by promoting informed and critical thinking about democracy and democratic issues in the digital space; and
- Establishing rules for digital platforms to act with appropriate responsibility in an elections context.[235]

83. [*** This paragraph was revised to remove injurious or privileged information. ***] In 2018, the Government recognized that additional measures were required to bolster Canada's electorate and electoral infrastructure, and more comprehensively mitigate cyber and non-cyber threats.[236] In January 2019, the Government announced the Plan to Protect Canada's Democracy, which sought to address what the government assessed to be the key vulnerabilities at the time, including by:

- Formalizing government responses to foreign interference during an election campaign, and how Canadians would be informed;
- Increasing media literacy programming to help inform and inoculate Canadians against disinformation campaigns;
- Expanding outreach efforts to political parties and diaspora communities to help them protect themselves from foreign human interference and cyber operations;
- Better understanding the spread of disinformation on digital platforms and identifying key foreign perpetrators.[237]

84. The Plan established or formalized several mechanisms and initiatives, specifically:

- The Critical Election Incident Public Protocol, including the Panel and the Security and Intelligence Threats to Elections (SITE) Task Force;
- The Digital Citizen Initiative at Canadian Heritage;
- Increased public engagement by intelligence agencies on the threat of electoral interference;
- Direction for the RCMP to form a team dedicated to investigating foreign interference activities;
- The creation of the Protecting Democracy Unit at PCO; and
- Direction for CSIS, CSE and the RCMP to provide a classified threat briefing to key political party leaders.[238]

The Committee will describe these initiatives and their implementation below.

[235] PCO, "Protecting Canada's Democracy: Overview," February 18, 2020.
[236] *** 2018.
[237] Public Safety Canada, "HASA File Timeline," October 28, 2019; and *** 2018.
[238] PCO, "Protecting Canada's Democracy: Overview," February 18, 2020.

85. The Critical Election Incident Public Protocol (the Protocol): Announced by the government on January 30, 2019, the Protocol set out how the government would publicly inform Canadians during the writ period about incidents that threatened Canada's ability to have a free and fair election. In 2021, the government updated the Protocol after the 43rd general election to align the Protocol's application period with the caretaker convention,[239] which refers to the period between the dissolution of Parliament or when the Government loses a vote of no-confidence and the swearing-in of a new government or when an election result returning an incumbent government is clear.[240] Implementation of the Protocol is supported by two key mechanisms: the Panel and the Security and Intelligence Threats to Elections (SITE) Task Force.

86. The Panel: Five deputy heads (the Panel) administer the Protocol. Its members are the Clerk of the Privy Council, the National Security and Intelligence Advisor, and the deputy ministers of the Departments of Justice, Foreign Affairs and Public Safety.[241] The Panel is supported and informed by SITE.

87. SITE: Consisting of CSIS, GAC, the RCMP, and CSE, SITE is an operational task force that "aims to improve awareness, collection, coordination and action in countering Foreign Interference in Canada's federal election[s]."[242] SITE focuses its efforts on covert, clandestine, or criminal activities interfering with or influencing electoral processes in Canada.[243] SITE also offered briefings to Secret-cleared representatives of each political party represented in the House of Commons during the election period (discussed below).[244] In the period under review, SITE operated throughout the phases of the electoral process. In the pre-writ periods, SITE met frequently, including with Elections Canada (EC) and the Office of the Commissioner of Canada Elections, and provided threat briefings to the Panel, EC and the Office of the Commissioner, and to those Secret-cleared representatives of federal political parties.[245] During the writ period and on election day, SITE met daily and produced a daily situation report for the Panel, was on call 24/7, and provided threat briefings to political party representatives (see paragraph 96 below). After election day, SITE remained on call 24/7 for one week and then prepared an after action report.[246] Since the 2019 election, SITE has remained a standing task force.[247]

---

[239] Government of Canada, "Strengthening Canada's electoral system," December 7, 2023.
[240] PCO, "Guidelines on the conduct of Ministers, Ministers of State, exempt staff and public servants during an election," August 2021.
[241] PCO, "Security and Intelligence Threats to Elections Task Force – Partner Roles," August 11, 2021.
[242] National Security and Intelligence Advisor (NSIA), "Memorandum for the Prime Minister: Creation of the Security and Intelligence Threats to Elections Task Force (SITE)," submitted October 16, 2018, returned from the PM January 24, 2019, hand written file number 2018-NSIA-00181.
[243] PCO, "Security and Intelligence Threats to Elections Task Force – Partner Roles," August 11, 2021.
[244] In 2019, SITE briefed Secret-cleared members from the Conservative, Liberal, New Democratic and Green Parties. In 2021, only the Conservative, Liberal, New Democratic and Green Parties accepted the government's offer to receive Secret-level briefings. Morris Rosenberg, "Report on the Assessment of the 2021 Critical Election Incident Public Protocol," February 20, 2023; and CSE, Factual Review of NSICOP Report, January 19, 2024.
[245] Morris Rosenberg, "Report on the Assessment of the 2021 Critical Election Incident Public Protocol," February 20, 2023.
[246] SITE, "Summary of SITE TF Activities: Pre-, During and Post-Federal Election," July 2, 2021.
[247] Meeting monthly. Morris Rosenberg, "Report on the Assessment of the 2021 Critical Election Incident Public Protocol," February 20, 2023.

88. The Protocol requires preparation of an independent report after each election to assess the Protocol's implementation and effectiveness in addressing threats. Two reports have been released to date: the Judd Report released in May 2020 and the Rosenberg Report released in February 2023.[248] The Judd report concluded that the Protocol was implemented successfully and suggested recommendations for improvement to resolve challenges that had been encountered, which were addressed by *** the Government in 2021, as noted earlier.[249] (The Cabinet Directive on the Critical Election Incident Public Protocol requires that the independent report on the Protocol's implementation be shared with the Committee. The Committee supported the author's key recommendations and flagged several considerations in a letter to the Prime Minister in December 2020).[250] The Rosenberg report found that while there had been foreign interference efforts, they did not meet the Protocol's threshold for the Panel to advise the public. The Rosenberg report also stressed that "the government's plan and public communications should acknowledge that the problem of interference occurs both before the election is called and during the caretaker period."[251]

89. Digital Citizen Initiative: Based at Canadian Heritage, the initiative aims to build citizen resilience against online disinformation and build partnerships to support a healthy information ecosystem, by supporting projects to promote critical thinking and digital media literacy.[252] The government reports that the initiative has spent over $15 million on 96 projects by civil society and academic organizations "to build citizen resilience against disinformation."[253] For example, in 2019-2020, the government contributed $7 million to bolster civic, news and digital media literacy, ranging from awareness sessions and workshops to the development of learning materials. According to the Digital Citizen Initiative, these projects reached more than 12 million Canadians.[254]

90. G7 Rapid Response Mechanism (RRM): Announced at the June 2018 G7 Summit in Charlevoix, this Canada-led initiative works to strengthen coordination across G7 countries to respond to foreign interference by sharing information and identifying opportunities for coordinated responses in response to disinformation campaigns.[255] Housed within GAC, RRM Canada, which is the permanent secretariat to the RRM, also monitors the digital information

[248] See James Judd, "Report on the Assessment of the 2019 Critical Election Incident Public Protocol," May 2020; and Morris Rosenberg, "Report on the Assessment of the 2021 Critical Election Incident Public Protocol," February 20, 2023. There are classified and redacted versions of each report.
[249] James Judd, "Report on the Assessment of the 2019 Critical Election Incident Public Protocol," May 2020.
[250] NSICOP, *2020 Annual Report*, March 2021.
[251] Morris Rosenberg, "Report on the Assessment of the 2021 Critical Election Incident Public Protocol," February 20, 2023.
[252] The Digital Citizen Initiative's programming focused on countering misinformation and disinformation in the context of democratic processes and institutions appears to have largely occurred in 2019 and 2020. Since then, the initiative has also supported activities to help Canadians identify other forms of misinformation and disinformation, such as about COVID-19 and the Russian invasion of Ukraine. Canadian Heritage, "Digital Citizen Initiative – Online disinformation and other online harms and threats," March 20, 2023; and "Government of Canada reinforces support to organizations to help counter harmful disinformation," March 16, 2022.
[253] PCO, *Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions*, April 6, 2023.
[254] Canadian Heritage, "Digital Citizen Initiative – Online disinformation and other online harms and threats," March 20, 2023.
[255] PCO, "G7 Rapid Response Mechanism", January 30, 2019.

environment for foreign state-sponsored disinformation, including during general elections.[256] RRM Canada leads GAC's participation in SITE, and began evaluating the Canadian digital information ecosystem in the year prior to the 2019 Election. RRM Canada regularly informed SITE of online and media activities, including disinformation, aimed at discouraging Canadians from supporting certain political parties, and discrediting Canadian politicians and institutions. An example of RRM Canada's contribution is described in paragraph 35.

91. Increased Public Engagement by Intelligence Agencies: *** The Plan to Protect Canada's Democracy also provided the authority for Canada's intelligence agencies to increase engagement with Canadians on the threat of electoral interference. For CSIS, this meant the authorization to make sustained investments in its capacity to investigate, analyse and provide advice on foreign influenced activity targeting Canada's democratic institutions, and to raise awareness of threats to key stakeholders involved in the democratic process. Similarly, the Plan enabled CSE to provide technical advice, guidance and services to Canadian political parties and elections administrators, and enhance public engagement efforts on cyber threats to Canada's democratic processes.[257] In July 2021, CSIS publicly released its report, "Foreign Interference: Threats to Canada's Democratic Process," which lays out foreign state motivations and techniques, key targets in Canada and government efforts to address the threat.[258] For its part, CSE built on a 2017 report to publish a report in 2019 on cyber threats to Canada's democratic processes, detailing key targets and trends and an assessment of the Canadian context.[259] CSE released an updated version of this report in July 2021.

92. RCMP: Under the *** Plan to Protect Democracy, *** the Government directed the RCMP to form a temporary team dedicated to investigating foreign interference activities in order to investigate and disrupt any criminal acts that may be conducted as a part of interference, including hacking, intimidation, and the bribery of public officials.[260] Initially based in the Ottawa Integrated National Security Enforcement Team, its activities were "informally" transferred to the Foreign Actor Interference Team (FAIT) within the Federal Policing National Security Program at National Headquarters (NHQ) in 2020.[261] According to the RCMP, the "informal establishment of the FAIT at NHQ was a short-term solution to address the most immediate foreign interference-related needs identified at the time."[262] The team consists of seven police officers who provide oversight of the RCMP's foreign interference investigations across Canada, but who do not directly conduct these investigations.[263]

---

[256] Global Affairs Canada, "Rapid Response Mechanism Canada: Global Affairs Canada," August 9, 2023.
[257] *** 2018.
[258] CSIS, *Foreign Interference: Threats to Canada's Democratic Process*, July 2021.
[259] CSE, *Cyber Threats to Canada's Democratic Process: July 2021 Update*, July 2021; see also the 2017 and 2019 reports.
[260] *** 2018.
[261] RCMP, Factual Review of NSICOP Report, January 19, 2024; and RCMP, "RCMP Document Production FRI8 – FP FAIT and ETRU," RCMP document produced for NSICOP's review of the RCMP Federal Policing mandate, June 2022.
[262] RCMP, Factual Review of NSICOP Report, January 19, 2024.
[263] RCMP, "RCMP Document Production FRI8 – FP FAIT and ETRU," RCMP document produced for NSICOP's review of the RCMP Federal Policing mandate, June 2022.

93. PCO Protecting Democracy Unit: In 2018, the government established the Protecting Democracy Unit within the Privy Council Office to coordinate, develop and implement "government-wide measures designed to combat disinformation and to protect Canada's democratic institutions."[264] The Unit was established to act as the central hub to lead and to coordinate all work across the Government with regards to strengthening and protecting Canada's democratic institutions from emergent threats, working with other government departments and agencies, and other domestic and international stakeholders, as appropriate.[265] Funding for the unit was not provided until Budget 2022.[266]

94. Briefing political parties: *** The Government authorized CSIS, CSE and the RCMP to provide leaders from the political parties represented in the House of Commons with in-depth, classified threat briefings to encourage them to strengthen their internal security practices and behaviours and build their awareness of foreign-influenced activities in Canada. To facilitate these briefings, PCO sponsored security clearances for individuals from each of the political parties represented in the House of Commons.[267] Ultimately, these briefings were provided under SITE's remit to SECRET-cleared party representatives from July 2019 to September 2019 for the 43rd general election, and from July 2021 to September 2021 for the 44th general election.[268]

95. In February 2023, the Rosenberg report concluded that the "political party representatives were generally pleased with the information sharing with government."[269] However, in April and May 2023, Conservative Party of Canada and Liberal Party of Canada representatives testified at the House of Commons Standing Committee on Procedure and House Affairs that they received very little threat information from the government, and what they did receive was "vague" and lacked specificity. The Conservative Party of Canada also testified that SITE did not take seriously its concerns about foreign interference in 13 ridings in the 2021 election (noted in paragraph 33). Both parties' representatives testified that they thought that SITE would provide them with actionable threat information, such as about their own party's candidates or volunteers, so that they could keep an eye on issues or conduct their own investigations. Party representatives also testified that SITE members repeatedly cited legislative challenges as a reason the task force could not share more information, although they reportedly did not specify what those challenges were.[270] Party representatives also noted other challenges of working with SITE. On the one hand, party representatives testified that SITE members' knowledge of political parties and how campaigns are conducted was low. On the other hand, party representatives acknowledged that their intelligence literacy was low, but noted that SITE did little to explain intelligence concepts to them.[271] In its capacity as former Chair of SITE, CSE

[264] PCO, "Countering an Evolving Threat: Update of Recommendations to Counter Foreign Interference in Canada's Democratic Institutions," April 6, 2023.
[265] *** 2018.
[266] PCO, Factual Review of NSICOP Report, January 19, 2024.
[267] *** 2018.
[268] CSE, "Foreign Interference Review: NSICOP Committee Hearing," May 18, 2023.
[269] Morris Rosenberg, "Report on the Assessment of the 2021 Critical Election Incident Public Protocol," February 20, 2023.
[270] The PROC hearings of April 25 and May 18, 2023.
[271] The PROC hearings of April 25 and May 18, 2023.

advised the Committee that it "had no recollection of specific discussions with political parties where SITE discussed political parties and campaigns or conversations on the finer points of intelligence collection/concepts."[272]

Strategy to Counter Hostile Activities by State Actors (HASA)

96. [*** This paragraph was revised to remove injurious or privileged information. ***] The security and intelligence community recognized that work to counter foreign interference in democratic processes and institutions needed to extend beyond securing elections.[273] Indeed, in 2018 the Government acknowledged that the threat of foreign interference was multi-pronged so Canada requires a multi-faceted, nimble approach, acknowledging that traditional human interference activity, long-tracked by intelligence agencies, continues to be perpetrated in Canada.[274]

97. In March 2018, Public Safety first briefed Deputy Ministers on the threat of hostile activities by state actors (HASA), defined as "actions by hostile states or their proxies that are deceptive, coercive, corruptive, covert, threatening or illegal, yet fall below the threshold of armed conflict, and which undermine Canada's national interests."[275] In July 2018, Public Safety subsequently began efforts to develop a strategy ***, which was discussed and debated over the ensuing four years.[276] By the fall of 2019, departments and agencies had identified areas for reform across the security and intelligence community. [277]

98. [*** This paragraph was revised to remove injurious or privileged information. ***] It would take the Government over two and a half years to put in place a plan of reform. The plan included a classified, internal-to-government countering HASA strategy; the creation of a HASA coordinator; an unclassified, public-facing strategy; consultations on legislative amendments; and new resources and activities for the RCMP. These initiatives are described below.[278] [279] [280]

99. A classified internal-to-government *Countering HASA Strategy*: The Strategy prioritized defending the following five sectors: democratic processes and institutions, Canadian communities vulnerable to harassment and intimidation, economic prosperity and research security, international affairs and defence, and critical infrastructure. These sectors are underpinned by three pillars of action:

---

[272] CSE, Factual Review of NSICOP Report, January 19, 2024.
[273] Public Safety, "HASA File Timeline, October 28, 2019.
[274] *** 2018.
[275] *** 2022.
[276] *** 2018.
[277] The Deputy Minister National Security Committee met on HASA in September 2018, March 2019, June 2020, September 2020, and September 2021. The Assistant Deputy Minister National Security Policy Committee discussed HASA in March 2019, September 2019, December 2019, May 2020. HASA was also discussed by the Deputy Ministers and Clerk Committee in October 2019. Public Safety, "HASA File Timeline", October 28, 2019.
[278] *** 2022.
[279] *** 2022.
[280] *** 2018.

- DETECT: Understanding the threat environment and establishing a common operating picture as a prerequisite for an effective whole-of-government response;
- STRENGTHEN: Building resilience, reducing vulnerabilities and the perception of Canada being a permissive environment, making Canada a harder target;
- ACT: Deploying coordinated mechanisms to respond to HASA, based on evidence gathered through threat detection and in accordance with all applicable laws.[281]

100. The creation of a new National Counter Foreign Interference Coordinator: [*** This paragraph was revised to remove injurious or privileged information. ***] The Government endorsed the creation of a coordination role to implement the Strategy and to convene federal departments and agencies to address emerging HASA issues through the creation of a "Counter-HASA Coordinator," beginning in the 2023-24 fiscal year. The Coordinator's role would not alter the mandates of national security agencies and departments, nor would it grant Public Safety the authority to operationally direct others. Rather, its mandate would be limited to better leveraging PS's existing coordination role to ensure that HASA threats are jointly examined and addressed.[282] This coordination role is also distinct from PCO's Protecting Democracy Unit, which focuses almost exclusively on implementing the Plan to Protect Democracy, notably on countering disinformation.

101. The Prime Minister announced the creation of the renamed National Counter Foreign Interference Coordinator on March 6, 2023.[283] This brought Canada partially in line with Australia, which appointed a National Counter Foreign Interference Coordinator in 2018 to administer a national, whole-of-government strategy with objectives similar to the HASA Strategy.[284] (Australia also has a Counter-Foreign Interference Taskforce, which includes the Australian Security Intelligence Organisation and the Australian Federal Police, which is responsible for detecting, disrupting and investigating foreign interference activities.)[285] Since the Coordinator was named, his efforts have primarily focused on establishing governance mechanisms, including a new *ad hoc* Deputy Minister Committee on Foreign Interference for urgent decisions.[286]

---

[281] *** 2022.
[282] *** 2022.
[283] Prime Minister's Office, "Taking Further Action on Foreign Interference and Strengthening Confidence in Our Democracy", March 6, 2023. *** In the lead to up the announcement of the position, the Coordinator's first efforts were to establish his office, including financial and spending authorities.
[284] Australia's Coordinator is supported by the Counter Foreign Interference Coordination Centre (CFICC), housed within the Department of Home Affairs. The CFICC coordinates Australia's whole-of-government effort to respond to FI by administering Australia's Counter Foreign Interference Strategy, coordinating outreach and advice to vulnerable sectors and systems, and engaging with culturally diverse communities to strengthen them against foreign interference. In addition, the NCFIC is responsible for engaging with international partners, and developing approaches to deter and prevent foreign interference in Australia, including making the public more resilient and better informed. Australian Department of Home Affairs, "Countering Foreign Interference," June 5, 2023
[285] Australian Department of Home Affairs, "Countering Foreign Interference," June 5, 2023.
[286] Public Safety, NSICOP appearance, June 26, 2023; and PS, Factual Review of NSICOP Report, January 19, 2024.

102. An unclassified public-facing *Countering HASA Strategy*: [*** This paragraph was revised to remove injurious or privileged information. ***] The Government considered a whole-of-government strategic communications and engagement strategy, intended to help coordinate government communications with the public and key stakeholders (e.g., industry, ethnocultural communities, historically marginalized groups and other orders of government, etc.) regarding HASA threats. This approach was aligned with counter-disinformation efforts led by the Privy Council Office Democratic Institutions Secretariat.[287] Public Safety subsequently noted that while the principles underpinning the public strategy remain valid, it has been challenging to find the right timing for its release in light of the media reports of leaked intelligence and the ensuing public debate about foreign interference, and is now considering whether to substitute this strategy with an educational approach.[288]

103. Mandate to conduct consultations on proposed legislative amendments: *** In 2023, the Government launched consultations on a potential foreign influence transparency registry and potential amendments to the *Canadian Security Intelligence Service Act* (CSIS Act), the *Criminal Code*, and the *Security of Information Act* (SOIA).[289] The following section provides an update on these efforts.

104. *CSIS Act Amendments*: Enacted in 1984, the CSIS Act has not been comprehensively reviewed since its initial five-year review completed in 1990. *** Despite amendments like the introduction of threat reduction measures in 2015 and the dataset regime in 2019, significant deficiencies in CSIS's authorities remain, which have an impact on its ability to respond to foreign interference. Specific shortcomings include CSIS's ability to collect foreign intelligence and to share classified information (i.e., with elected officials or other orders of government).[290] On November 24, 2023, the government launched public consultations on legislative amendments to the CSIS Act, including whether to amend the Act to enable CSIS to disclose classified intelligence outside the federal government.[291]

105. *Criminal Code and SOIA Amendments*: [*** This paragraph was revised to remove injurious or privileged information. ***] These are two statutes that address a broad range of conduct related to HASA. The *Criminal Code* criminalizes, among other things, treason, sabotage, trading in influence and the unauthorized use of a computer, while SOIA focuses on information-related conduct harmful to, or likely to harm, Canada. The Government believed that these provisions could benefit from modernization, such as the *Criminal Code's* dated prohibition against treason, and the SOIA's provision regarding unauthorized disclosure of official information in section 4, which was struck down by the Ontario Superior Court of Justice in 2006.[292] In April 2023, the government committed "to explore if further amendments to existing provisions are needed and whether to create new offences … to facilitate prosecution of

[287] *** 2022.
[288] Public Safety NSICOP appearance, June 26, 2023.
[289] Public Safety, "Countering Hostile Activities by State Actors: Deck for DMNS", September 2021.
[290] *** 2022.
[291] Government of Canada, "Enhancing measures to counter foreign interference: Whether to amend the *Canadian Security Intelligence Service Act*," Public consultation paper, November 24, 2023.
[292] *** 2022.

foreign interference activities."[293] Public Safety also informed the Committee that the *Canada Evidence Act* would now be part of this consultation exercise.[294]

106. On November 24, 2023, the government launched public consultations on legislative amendments to the *Criminal Code*, the *Security of Information Act* and the *Canada Evidence Act*.[295] The consultations sought input on whether to define foreign interference in criminal law and create related offences to protect democratic processes at all orders of government and at all times, including outside an election period. Of relevance to foreign interference in democratic processes and institutions specifically, the consultations also sought views on whether to increase the maximum penalties (from two to five years imprisonment) for anyone convicted of preparing, conspiring, or attempting to commit an existing or new foreign interference offence. Additionally, the consultations sought input on whether to implement a single regime for safeguarding sensitive information in judicial reviews and statutory appeals, and reforms to how national security information is protected and used in criminal proceedings. The Committee understands this as an attempt to address the "intelligence and evidence" challenge. This challenge refers to the risk of the unauthorized disclosure of sensitive collection techniques, confidential sources or intelligence shared from allies in a criminal trial.

107. *Foreign Influence Transparency Registry*: As outlined in the previous chapter, some foreign governments or their proxies use individuals or entities to influence government policies or public discourse covertly or in a non-transparent manner. Three of Canada's closest allies have adopted foreign agents' registries, which prescribe the registration of persons acting as agents of foreign principals and requires public disclosure of one's status as a foreign agent, to respond to this activity: notably the U.S. (1938),[296] Australia (2018),[297] and the United Kingdom (U.K.) (2023).[298] Registries serve two purposes: they promote transparency (similar to lobbying registries) and they enable criminal investigations into foreign interference. Under U.S. law, a person who works for or on behalf of a foreign government but has not registered with the U.S. Attorney General is liable to criminal prosecution, and this has enabled the FBI to investigate and lay charges in relation to election interference and transnational repression.[299] This is also the case in Australia (since 2018) and the U.K. (legislation creating a registry received royal assent in 2023).

---

[293] PCO, *Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions*, April 6, 2023.
[294] Public Safety, NSICOP appearance, June 26, 2023.
[295] Government of Canada, "Addressing foreign interference: Whether to Amend the *Security of Information Act* and Modernize certain *Criminal Code* offences, and to Introduce a review mechanism in the *Canada Evidence Act* to manage sensitive information," Public consultation paper, November 24, 2023. These consultations concluded after the completion of this review.
[296] United States Congress, *Foreign Agents Registration Act*, 1938.
[297] The Parliament of the Commonwealth of Australia, *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*, section 92.2(1)(c)(i), and paragraph 866 of the law's Revised Explanatory Memorandum, 2018.
[298] UK Parliament, *National Security Act 2023*, section 14, 2023.
[299] A recent example: United States Department of Justice, United States v. Ionov and others, press release and indictment, April 18, 2023.

108. On March 6, 2023, the Prime Minister announced the launch of public consultations on the potential scope and configuration of a Foreign Influence Transparency Registry, intended to "ensure transparency and accountability from people who advocate on behalf of a foreign government."[300] Public Safety held these consultations between March 10, 2023 and May 9, 2023.[301] In November 2023, both the Prime Minister and the Minister of Public Safety advised the Committee that they expected to introduce legislation imminently.[302]

Intelligence priorities

109. Cabinet approves national intelligence priorities every two years through the Intelligence Priorities Memorandum to Cabinet, the primary mechanism available to the Prime Minister, Cabinet, and senior security and intelligence officials for control, accountability, and oversight of Canada's intelligence collection and assessment priorities.[303] Once approved by Cabinet, the Ministers of Public Safety, Foreign Affairs and National Defence issue Ministerial Directives to the relevant organizations in their portfolios to guide intelligence collection and assessment over the ensuing two years.[304] Officials then use the intelligence priorities to inform the creation of intelligence requirements outlining specific issues or entities of interest to intelligence consumers.[305]

110. In the period under review, Cabinet set intelligence priorities for the years 2017-2019, 2019-2021 and 2021-2023. During this period, foreign interference in democratic processes and institutions featured regularly and prominently in Canada's intelligence requirements:

- 2017-2019: The government sought intelligence on how foreign states and their non-state proxies are using espionage, interference or sabotage to undermine the effective functioning and integrity of Canada's democratic institutions, governance and associated processes.[306] More specifically, officials sought intelligence on covert or malign efforts to influence or compromise Canadian (federal, provincial/territorial, municipal) politicians, elections, governance, policy, political institutions or infrastructure (including the media).[307] Officials cited specific concerns relating to social media platforms; agents of influence (journalists, academics, businesspersons, government officials); interference

[300] Prime Minister's Office, "Taking Further Action on Foreign Interference and Strengthening Confidence in Our Democracy", March 6, 2023.
[301] Public Safety, "Government of Canada launches public consultations on a Foreign Influence Transparency Registry in Canada", March 10, 2023.
[302] Minister of Public Safety, NSICOP appearance, October 31, 2023; and Prime Minister, NSICOP appearance, November 7, 2023.
[303] NSICOP, *2018 Annual Report*, 2019.
[304] NSICOP, *2018 Annual Report*, 2019.
[305] PCO, "Canadian Intelligence Requirements Pursuant to the 2021-2023 Canadian Intelligence Priorities and Outcomes" September 29, 2022.
[306] PCO, Standing Intelligence Requirement Chart on Espionage, Foreign Interference and Sabotage Coverage Review," April 2019.
[307] PCO, Standing Intelligence Requirement Chart on Espionage, Foreign Interference and Sabotage Coverage Review," April 2019.

or malign pressure on Canadian media or public policy figures; and any other covert, deceptive or malign use of Canadian proxies.[308]

- 2019-2021 and 2021-2023: Cabinet approved intelligence priorities for 2019-2021 and 2021-2023 that specifically included foreign interference, which in turn informed intelligence requirements related to the plans, intentions, and capabilities of hostile state actors (or their proxies) to conduct interference activities against Canadian strategic interests.[309] Clients specifically sought intelligence on:

    - Influence of Canadian officials, and threats to Canadian elections, democracy and civil society;
    - Intimidation and influence of diaspora and dissidents in Canada; and
    - Misinformation and disinformation campaigns, and cyber-enabled interference.[310]

PCO updates Cabinet annually on how each organization of the security and intelligence community has supported the intelligence priorities using the National Intelligence Expenditure Review (NIER). The NIER informs Cabinet Ministers of variances in annual expenditures over time.[311] Between 2019-2020 and 2021-2022, organizations increased their expenditures on intelligence collection and assessment for espionage, foreign interference and sabotage, the priority which includes foreign interference in democratic processes and institutions, by approximately $***, bringing it closer to expenditures for terrorism and extremism, the community's top priority.[312] Although the NIER methodology changed for the next year, this trend stayed steady in fiscal year 2021-2022.[313]

Legislative changes

111. Elections Modernization Act: The government enacted legislative changes through the *Elections Modernization Act*, which received royal assent in December 2018. The Act made amendments to the *Canada Elections Act*, which governs elections to the House of Commons and protects the rights of Canadian citizens to participate in Canada's democratic processes. The *Elections Modernization Act* added three offences: undue influence of electors to vote or refrain from voting by a foreigner; intimidation of voters to vote for or refrain from voting for a particular candidate or party; and prohibitions on the use of foreign contributions for partisan activities, advertising, elections advertising and election surveys. The Act also gave the

[308] PCO, Standing Intelligence Requirement Chart on Espionage, Foreign Interference and Sabotage Coverage Review," April 2019.
[309] PCO, "Canadian Intelligence Requirements Pursuant to the 2021-2023 Canadian Intelligence Priorities and Outcomes," September 29, 2022.
[310] PCO, "Canadian Intelligence Requirements Pursuant to the 2021-2023 Canadian Intelligence Priorities and Outcomes," September 29, 2022.
[311] PCO, "Canadian National Intelligence Expenditure Review For the 2020-2021 Fiscal Year," March 2022.
[312] PCO, "Canadian National Intelligence Expenditure Review For the 2020-2021 Fiscal Year," March 2022. In FY 2019-2020, the expenditures for espionage, foreign interference and sabotage and terrorism and extremism were approximately *** and ***, respectively, a difference of approximately ***; by FY 2021-2022, the expenditures were approximately *** and ***, respectively, a difference of approximately *** with the foreign interference-related category now higher. The dollar figures here include Internal Services.
[313] PCO, "Canadian National Intelligence Expenditure Review For the 2020-2021 Fiscal Year," June 2023.

Commissioner of Canada Elections the power to seek a court order to compel testimony to address serious instances of alleged non-compliance with the *Canada Elections Act*.[314]

112. Communications Security Establishment Act: The government enacted further legislative change with the passage of the *National Security Act*, which received royal assent in June 2019. The act made a number of changes, notably the creation of the *Communications Security Establishment Act*, which provided CSE the authorities to conduct defensive and active cyber operations to protect Canadians and Canadian interests and critical infrastructure, including electoral infrastructure. These authorities permitted CSE to respond operationally to foreign interference threats (*** examined further in paragraph 116 below).

Operational responses

113. The following section outlines how departments and agencies used their existing authorities to investigate, disrupt and deter foreign interference in Canada's democratic processes and institutions in the period under review. This section does not provide an exhaustive account of all operational activity; rather, it illustrates the various lines of effort that contributed toward the government's overall operational response to the threat. These include disruption operations; efforts by law enforcement bodies; and diplomatic activities.

Disruption operations

114. While the primary role of CSIS and CSE is to collect and report intelligence to the government, both organizations have the authority to disrupt or counter threats to Canada's national security. The following section outlines how those tools were used to respond to foreign interference in democratic processes and institutions.

115. CSE Active and Defensive Cyber Operations: Under the CSE Act, CSE may conduct defensive cyber operations to protect federal systems and non-federal systems designated of importance to the Government of Canada, including critical infrastructure, as well as active cyber operations to protect and pursue Canadian international affairs, defence and security interests. Under these authorities, CSE uses a variety of techniques, such as ***.[315] As noted in Chapter 2, under the period of review the Minister of Defence authorized two Defensive Cyber Operations to allow CSE to conduct activities that could disrupt malicious cyber operations targeting Canada's democratic processes and institutions, including the development of defensive measures to protect Elections Canada's infrastructure.[316] [*** Two sentences were deleted to remove injurious or privileged information. The sentences described how CSE selected its targets, and described a Ministerial Authorization for a CSE Active Cyber Operation to counter foreign interference. ***][317] [318]

[314] *Elections Modernization Act*, assented to December 13, 2018.
[315] CSE, *** 2022.
[316] CSE, NSICOP appearance, May 2023.
[317] CSE, *** ACO_DCO MA Quarterly Update Summary, undated.
[318] CSE, NSICOP Appearance, May 2023.

116. CSIS Threat Reduction Measures (TRMs): Under the CSIS Act, CSIS may take measures to reduce a threat to the security of Canada if the measures are reasonable and proportional to the severity of the threat, among other requirements.[319] Between September 2018 and September 2023, CSIS conducted seven TRMs responding to foreign interference in Canada's democratic institutions and processes by the PRC, Russia, India, and Pakistan (see Table 1 below).[320] The TRMs sought to either disrupt foreign interference networks in Canada,[321] diminish the influence of a threat actor,[322] or brief individuals who were the victims of foreign interference.[323]

Table 1: CSIS Threat Reduction Measures against foreign interference in democratic institutions and processes, September 1, 2018 to September 30, 2023

	Year	Country	Primary objective
1	***[324]	***	Disrupt foreign interference networks
2	***[325]	***	Diminish the influence of a threat actor
3	***[326]	***	Diminish the influence of a threat actor
4	***[327]	***	Disrupt foreign interference networks
5	***[328]	***	Diminish the influence of a threat actor
6	***[329]	***	Diminish the influence of a threat actor
7	***[330]	***	Brief individuals who were the victims of foreign interference

117. *** TRMs were developed in anticipation of the federal elections in 2019 and 2021. [*** Six sentences were deleted to remove injurious or privileged information. The sentences described Threat Reduction Measures taken to address the foreign interference activities of specific countries and the success of those measures. ***][331] [332] [333]

[319] *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23, ss. 12.1 and 12.2. CSIS must have reasonable grounds to believe the threat constitutes a threat to the security of Canada.
[320] To put this number in context, in a typical year CSIS conducts between 16 and 19 TRMs, and conducted a total of 77 TRMs between 2018 and 2022: 17 TRMs in 2018, 19 in 2019, 8 in 2020, 17 in 2021, and 12 in 2022. NSIRA, *2022 Annual Report*, September 2023.
[321] CSIS, ***; CSIS, ***; CSIS, ***; CSIS, ***.
[322] CSIS, ***.
[323] CSIS, "FW Questions stemming from DIRs 2023 05 09 appearance before NSICOP," email from CSIS to NSICOP Secretariat about CSIS's briefing of Mr. Chong (on May 2, 2023), May 31, 2023; CSIS, "Delivered Form of Words – Briefing to Erin O'TOOLE," May 26, 2023; and CSIS, "Delivered Form of Words – Briefing to MP Jenny KWAN," May 26, 2023.
[324] *** CSIS, Factual Review of NSICOP Report, January 19, 2024. ***.
[325] CSIS, ***.
[326] CSIS, ***.
[327] CSIS, ***.
[328] CSIS, ***.
[329] CSIS, ***.
[330] CSIS, "Memorandum to the Minister: Threat Reduction Measure: PRC Targeting Specific Members of Parliament," signed by the Minister of Public Safety on May 18, 2023.
[331] CSIS, ***.
[332] CSIS, ***.
[333] CSIS, ***.

118. On May 18, 2023, CSIS carried out a TRM under exigent circumstances to brief Member of Parliament Michael Chong (see paragraph 50). Later that month, CSIS used its TRM authority to provide threat briefings to two other members of Parliament, and one former member of Parliament in September 2023.[334] This TRM was notable in that CSIS described in its briefing to the Minister that the *** overall operational, reputational, legal and foreign policy risk for this TRM was high ***.[335] CSIS also noted that it had limited ability to prevent later disclosure of the classified information by the members of Parliament, and underlined the legal, policy and procedural implications of disclosing classified information to individuals who did not hold the requisite security clearance and were not bound by the *Security of Information Act*.[336]

Efforts by law enforcement

119. Canada has two federal organizations responsible for investigating criminal offences related to foreign interference in democratic processes and institutions: the Office of the Commissioner for Canada Elections and the RCMP. Section 14 (d) of the NSICOP Act limits the Committee's access to information relating directly to an ongoing investigation carried out by a law enforcement agency that may lead to a prosecution. For this reason, the Committee was unable to discern a clear picture of the investigations that may have been underway in the time period under review. However, it was able to learn the following information.

120. Office of the Commissioner for Canada Elections: The Office of the Commissioner of Canada Elections (OCCE) is mandated to ensure compliance with and enforcement of the *Canada Elections Act*.[337] While the Act does not define "foreign interference," it does prohibit the involvement of foreigners in specific ways, such as prohibiting foreigners from making political contributions.[338] The OCCE is a relatively small organization and its 20 investigators work almost entirely based on complaints received.[339] The maximum penalties for those committed of an offence under the Act are five years imprisonment, a fine of $50,000 for an individual and $100,000 for an entity, or a prohibition from sitting or being elected to Parliament for seven years.[340] The Commissioner of Canada Elections advised the Committee that her office was reviewing 174 foreign interference-related complaints it received about the 2019 and 2021 elections, almost all of which (148 or 85%) were received in 2023 after the leaks of classified information.[341] As of June 16, 2023, the OCCE had received 158 foreign interference-related

[334] CSIS, "Memorandum to the Minister: Threat Reduction Measure: PRC Targeting Specific Members of Parliament," signed by the Minister of Public Safety on May 18, 2023; and CSIS, Factual Review of NSICOP Report, January 19, 2024.
[335] CSIS, "Memorandum to the Minister: Threat Reduction Measure: PRC Targeting Specific Members of Parliament," signed by the Minister of Public Safety on May 18, 2023.
[336] CSIS, "Memorandum to the Minister: Threat Reduction Measure: PRC Targeting Specific Members of Parliament," signed by the Minister of Public Safety on May 18, 2023.
[337] *Elections Canada Act* (2000, c. 9), s. 509.2.
[338] Elections Canada, "Appearance of the Chief Electoral Officer before the National Security and Intelligence Committee of Parliamentarians," Deck, June 16, 2023.
[339] Commissioner of Canada Elections, Evidence to PROC, November 1, 2022.
[340] Office of the Commissioner of Canada Elections, "Annex 1 to the Presentation of the Commissioner of Canada Elections to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," June 2023.
[341] In November 2022, the Commissioner told PROC that the OCCE had received 10 foreign interference-related complaints concerning the 2019 election, and 13 concerning the 2021 election. Commissioner of Canada Elections, Evidence to PROC, November 1, 2022.

complaints concerning the 2019 election (out of a total of 8,000 complaints for that election),[342] and 16 concerning the 2021 election.[343] The Commissioner noted that the key external challenges faced by the OCCE included the intelligence-to-evidence dilemma, technological limitations (e.g., encryption), information sharing within the federal government and the difficulty in obtaining evidence located in other countries.[344]

121. RCMP: In 2020, the RCMP established a Foreign Actor Interference Team to coordinate and oversee its foreign interference investigations (paragraph 93). The unit was established using resources from other national security priorities and the RCMP advised the Committee that it will be unsustainable without new resources.[345] Despite the creation of this unit, the RCMP was unable to tell the Committee exactly how many foreign interference investigations it had undertaken in the review period – it could only calculate the number of "occurrences," defined as a record of a call for service or self-generated work (according to the RCMP, an investigation involves one or more occurrences, but "not all occurrences are investigations"). Between 2018 and 2022, the RCMP had six occurrences linked to foreign interference in democratic institutions and processes, all of which required the RCMP to determine whether suspicious events or allegations of foreign interference were potential offences under existing criminal law, such as breach of trust or intimidation.[346]

122. The RCMP conducted no investigations into foreign interference-related activities in the context of the 2019 and 2021 federal elections.[347] The SITE Task Force's post-election reports for the 2019 and 2021 elections noted that there was no information shared with SITE that could have led to a criminal investigation.[348] Additionally, the RCMP stated that CSIS likely did not provide it with any leads linked to foreign interference in democratic institutions and processes between 2018 and 2023 (the RCMP does not track CSIS leads by threat type, e.g., foreign interference, espionage).[349]

123. The RCMP has been taking other steps to respond to foreign interference. In 2020, the RCMP added foreign interference to the duties of an "all source" intelligence unit to brief senior RCMP officials for their situational awareness, but not for investigation. In 2021, the RCMP

[342] Commissioner of Canada Elections, Evidence to PROC, March 2, 2023.
[343] Commissioner of Canada Elections, NSICOP appearance, June 16, 2023. The OCCE subsequently advised NSICOP that it had submitted updated statistics to the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions on December 22, 2023, using a different methodology, which explains the difference in numbers. OCCE, Factual Review of NSICOP Report, January 19, 2024.
[344] Commissioner of Canada Elections, NSICOP appearance, June 16, 2023.
[345] RCMP, Factual Review of NSICOP Report, January 19, 2024.
[346] RCMP operational data provided to NSICOP on October 27, 2023.
[347] RCMP, "Foreign Interference in Canada's Federal Democratic Processes: RCMP Appearance to the National Security and Intelligence Committee of Parliamentarians," Deck, May 12, 2023.
[348] RCMP, "Foreign Interference in Canada's Federal Democratic Processes: RCMP Appearance to the National Security and Intelligence Committee of Parliamentarians," Deck, May 12, 2023; SITE, *Security and Intelligence Threats to Elections Task Force, After Action Report (2019 Federal Election),* July 2020 (TS//SI//CEO); and CSE, Factual Review of NSICOP Report, January 19, 2024.
[349] RCMP, "SASU SP2," spreadsheet received by NSICOP on September 22, 2023. This RCMP table shows that between September 1, 2018 and July 31, 2023, CSIS provided the RCMP with 219 disclosures of information related to national security, eight of which were related to foreign interference (none between 2018 and 2020, one in 2021, two in 2022, and five in 2023) but none of the eight were linked to democratic institutions and processes.

drafted a Foreign Actor Interference Strategy intended for the public; as of January 2024, the document remained unpublished.[350]

Diplomatic efforts

124. GAC contributed to several government initiatives aimed at protecting the 2019 and 2021 federal elections. As noted earlier, GAC's Rapid Response Mechanism Coordination Unit participated in the SITE Task Force and the Deputy Minister of Foreign Affairs sat on the Critical Election Incident Public Protocol Panel.[351] In advance of the 2019 and 2021 federal elections, GAC also sent a formal notice to all foreign diplomatic missions in Canada to remind heads of mission of their obligation to ensure "diplomatic and consular representatives do not conduct activities, which may either be perceived as inducing electors to vote for a particular candidate, or prohibiting them from voting for a particular candidate in any way during an election period. Furthermore, accredited foreign representatives should not – directly or indirectly – make any financial contribution to a candidate, political party or political event."[352]

125. Outside of the context of the federal elections and, as noted in the Committee's previous report, GAC's responsibility for managing Canada's bilateral and multilateral relationships renders it a key decision-maker in determining how to respond to a state's attempts at interfering in domestic affairs. GAC has a number of diplomatic tools at its disposal to induce behavioural change in other states. These include bilateral measures, such as cancelling important visits, denying admissibility to diplomatic officials, closing diplomatic missions, closing cultural centres, public attribution of hostile activities by foreign actors, sanctions and declaring a foreign diplomat *persona non grata*. GAC also employs multilateral approaches, such as sharing best practices and lessons-learned with likeminded partners on how to counter foreign interference, developing diplomatic responses with like-minded states or raising a country's behaviour for consideration by international organizations.[353] When considering possible measures, GAC calibrates the government's response against broader foreign policy interests.[354] A recent example of GAC's use of one of its tools is provided in Case Study #5, below.

[350] RCMP, "RCMP Foreign Interference (FI) Strategy Draft – For Internal Consultation Only," October 4, 2021.
[351] GAC, "Countering Foreign Inference: Components of an Effective Response by GAC," November 2023.
[352] GAC, "Important Notice about Federal Elections from the Office of Protocol of Canada: August 20 2021 | Avis important a propos des elections federales de la part du Bureau du protocole du Canada: le 20 août 2021," August 2021.
[353] GAC, "Countering Foreign Inference: Components of an Effective Response by GAC," November 2023.
[354] NSICOP, *Annual Report 2019*, 2020.

Case Study #5: The expulsion of Zhao Wei

On May 8, 2023, the Minister of Foreign Affairs announced that Canada had declared Zhao Wei, a Toronto-based PRC diplomat, *persona non grata*.[355] He was given five days to leave Canada.

This action followed a May 1, 2023 media report of a leaked July 2021 CSIS assessment which described the PRC's foreign interference activities in Canada as a "critical national security threat."[356] The article discussed a number of examples, including that the PRC's Ministry of State Security (MSS) took specific actions to target members of Parliament, notably to obtain information on relatives who may be located in the PRC "for further sanctions." It quoted the CSIS assessment as saying that these efforts were "almost certainly meant to make an example of this member of Parliament and deter others from taking an anti-PRC position." According to the Globe and Mail source, the target was Michael Chong and the PRC diplomat involved was Mr. Zhao.

[*** This paragraph was revised to remove injurious or privileged information. ***] Within the review period, CSIS had provided GAC and other government organizations intelligence reporting on officials conducting foreign interference activities. In addition to a July 2021 assessment, CSIS provided GAC several specific reports between 2019 and 2022, some of which specifically mentioned Mr. Zhao.[357]

The July 2021 report was an assessment product, and *** more than half of the reports had limited distribution, meaning that only named recipients, such as the Deputy Minister or specific officials, would have been able to read them.[358] One of these reports, *** was on the *** PRC seeking information ***. In none of these instances did GAC officials seek further information on these reports ***.[359]

During the same period (2019 – 2023), CSIS and GAC officials formally exchanged information on *** several occasions about specific *** actors, including Mr. Zhao, conducting foreign interference activities in Canada. ***

- In *** 2019, *** CSIS provided a document, at GAC's request, which *** summarized threat activities. In this document, CSIS *** identified Mr. Zhao as a *** candidate for expulsion.[360] GAC sought no further information from CSIS.

[355] GAC, "Canada declares Zhao Wei persona non grata," Statement, May 2023.
[356] The Globe and Mail, "China views Canada as a 'high priority' for interference: CSIS report," May 2023.
[357] CSIS, *** undated.
[358] It is important to note that these reports generally focused on *specific* instances of foreign interference. CSIS noted to the Committee that its assessment products are meant to provide *general* context about foreign interference in order to enable the reader to better understand more specific reports.
[359] NSICOP Secretariat meeting with CSIS officials, August 30, 2023.
[360] CSIS, "PRC Espionage and Foreign Influence Footprint: ***," *** 2019.

- On *** 2022, CSIS briefed GAC officials on a Threat Reduction Measure it was considering ***. [*** One sentence was deleted to remove injurious or privileged information. The sentence described links between the subject of the Measure and the PRC. ***] GAC officials noted that their Minister had expressed an interest in countering PRC foreign interference and they had been looking for potential steps to take in response. Officials discussed the possibility of declaring *** *persona non grata*, and CSIS committed to provide more information.[361] Nothing came of this initiative.

- In February 2023, four months after the first leaks to the media of intelligence on PRC interference activities in Canada, CSIS briefed an interdepartmental Counter Foreign Interference Working Group on actions by allied states against Russian and PRC officials engaged in foreign interference. The briefing concluded with a discussion of *** what CSIS described as "egregious" foreign interference activities: ***.[362] CSIS noted that GAC considered the expulsion option as being too extreme (a "nuclear option").[363]

- On *** 2023, CSIS received an urgent request from GAC ***.[364] CSIS provided GAC a list *** the following day. This list was intended to be illustrative and not exhaustive ***.[365] On April 1, GAC advised CSIS that it was considering options with respect to the PRC and that information *** would be welcome.[366]

[*** This paragraph was revised to remove injurious or privileged information. ***] On May 1, the day of the Globe and Mail story on Mr. Zhao, GAC sent an urgent request to CSIS. GAC asked CSIS to provide analysis and asked specific questions. CSIS responded the following day by providing previously released intelligence reports and recommending the review of another.[367] [368]

[*** This paragraph was deleted to remove injurious or privileged information. The paragraph described GAC's evolving view of Mr. Zhao and its ultimate assessment that he was likely involved in foreign interference activities in Canada. ***][369]

GAC stated that the decision to expel Mr. Zhao was made in response to his foreign interference activities. GAC stated that once Mr. Zhao's name was associated publicly with Mr. Chong, Canada was going to force Mr. Zhao to leave Canada. [*** One sentence was deleted to remove injurious or privileged information. The sentence described diplomatic

[361] CSIS email, *** GAC Briefing Summary," *** 2022.
[362] CSIS presentation, "*** Action_v.2," February 2023.
[363] NSICOP Secretariat meeting with CSIS officials, August 30, 2023.
[364] CSIS email to GAC, "GAC Request ***," ***, 2023.
[365] CSIS email to GAC, "GAC Request ***," ***, 2023.
[366] NSICOP Secretariat meeting with CSIS officials, August 30, 2023.
[367] CSIS email to GAC, "Urgent – Request from DM call this afternoon," *** 2023; *** ***, "Follow up question from factual accuracy check," January 26, 2024.
[368] ***, "[Update & new question] Follow-up question from factual accuracy check," January 26, 2024.
[369] GAC, "PRC/Canada: PRC Consul Zhao Wei and allegation in Canadian media," *** 2023; and GAC, "PRC/Canada: An updated assessment on Zhao Wei," *** 2023.

engagement with the PRC. ***][370] *** Canada declared Mr. Zhao *persona non grata* on May 8, 2023.[371]

Briefing parliamentarians

126. In its 2018 report on the Prime Minister's visit to India, the Committee recommended that "Members of the House of Commons and Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada." [372] The Committee repeated this recommendation in its 2019 report on foreign interference. [373] In December 2019, the Clerk of the Privy Council sought the Prime Minister's authorization to implement the Committee's recommendations by having CSIS brief parliamentarians in the early weeks of the 43rd Parliament.[374] The Prime Minister's Office never replied formally to the recommendation. In December 2020, the NSIA returned to the Prime Minister to seek authorization for CSIS to brief parliamentarians, including unclassified briefings to all members of Parliament and Senators, and classified briefings to opposition party leaders. [375] The package for the Prime Minister included draft instruction letters to the Ministers of Public Safety and Defence to coordinate the briefings, as well as draft letters to the opposition leaders offering classified briefings. The Prime Minister's Office did not reply. In February 2022, the NSIA revived the initiative in another memorandum to the Prime Minister, following December 2021 media articles about the Conservative Party of Canada's concerns with 13 ridings in the most recent federal election (*** this memorandum was ultimately not provided to the Prime Minister).[376] The memorandum noted a similar proposal had been submitted in December 2020, but did not go forward as a result of the 2021 election and proposed the same steps as the 2020 proposal.[377] When asked by the Committee why he had not proceeded with this initiative, the Prime Minister responded that he thought that the Parliamentary Protective Service already briefs new parliamentarians about foreign interference.[378]

127. That said, CSIS conducted briefings for select parliamentarians on an *ad hoc* basis. In 2021 the Minister of Public Safety instructed CSIS to brief parliamentarians who CSIS believed

[370] NSICOP Secretariat meeting with GAC officials, August 28, 2023.
[371] GAC, "Foreign Interference by PRC ***," Memorandum for Action, undated.
[372] "Members of the House of Commons and Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada." NSICOP, *Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*, 2018.
[373] NSICOP, *Annual Report 2019*, 2020.
[374] Clerk of the Privy Council, "Briefings to Parliamentarians on Foreign Interference and Extremism in Canada," Memorandum for the Prime Minister, December 16, 2019.
[375] NSIA, "National Security Briefings to Parliamentarians," "Decision Sought/Signature Required" Memorandum for the Prime Minister, December 22, 2020 (S); and NSICOP, *Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*, 2018.
[376] NSIA, "National Security Briefings to Parliamentarians," "Decision Sought/Signature Required" Memorandum for the Prime Minister, undated and unsigned.
[377] NSIA, "National Security Briefings to Parliamentarians," "Decision Sought/Signature Required" Memorandum for the Prime Minister, undated and unsigned.
[378] Prime Minister, NSICOP appearance, November 7, 2023.

had been the target of espionage, intimidation or foreign interference.[379] In the summer of 2021, CSIS provided a series of classified and unclassified briefings to 25 members of Parliament from the Conservative Party of Canada, New Democratic Party and Liberal Party of Canada.[380] The unclassified briefings were about the PRC's foreign interference activities against parliamentarians. CSIS conducted these briefings using open source information, while the classified briefings, which CSIS conducted under the authority of a Threat Reduction Measure, specifically mentioned *** foreign interference activities against parliamentarians (see paragraph 118).[381]

128. The briefings covered three topics: CSIS's mandate, the definition of foreign interference, and how members of Parliament and their staff can protect themselves from specific tactics. The information about tactics was general in the unclassified briefings and specific in the classified ones. CSIS provided members of Parliament with two infographics and contact information for who to contact at CSIS and the RCMP to report an act of foreign interference in the upcoming election.[382] CSIS conducted all of the summer 2021 briefings before the issuance of the writs on August 15, 2021.[383] CSIS did not provide briefings during the writ period in order to adhere to the caretaker convention.[384] Since the 2021 election, CSIS increased the number of briefings provided to parliamentarians. In 2022, CSIS briefed 49 MPs and five Senators.[385]

129. On April 6, 2023, the government responded to NSICOP's recommendations on briefings for parliamentarians. It noted:

- The Parliamentary Protective Service provides security briefings to incoming members of Parliament.[386]
- The Security and Intelligence Threats to Election Task Force (SITE) offers briefings to political party representatives during the writ period.
- The Privy Council Office Security Operations Division briefs all incoming Ministers and Parliamentary Secretaries on the spectrum of threats, including foreign interference. CSIS also provides briefings to Parliamentarians upon request.

[379] Hon. Bill Blair, Evidence to PROC, June 1, 2023.
[380] Seventeen members of Parliament received unclassified briefings and ten received classified briefings (two members of Parliament received both). CSIS, *CSIS Engagement with Elected Officials on Foreign Interference: An Initiative of National Significance*, CSIS Analytical Brief *** November 3, 2021.
[381] CSIS, *** 2021; and CSIS, *CSIS Engagement with Elected Officials on Foreign Interference: An Initiative of National Significance*, CSIS Analytical Brief ***, November 3, 2021.
[382] CSIS, *CSIS Engagement with Elected Officials on Foreign Interference: An Initiative of National Significance*, CSIS Analytical Brief ***, November 3, 2021.
[383] CSIS, *CSIS Engagement with Elected Officials on Foreign Interference: An Initiative of National Significance*, CSIS Analytical Brief ***, November 3, 2021.
[384] CSIS's response to RFI #6, September 18, 2023.
[385] CSIS, *CSIS Public Report 2022*, March 2023; and CSIS, "Briefing to the NSIA and Clerk of the Privy Council on Foreign Interference Threats to Canada's Democratic Institutions, Monday, September 12, 2022, 12:30 – 1:30 PM," Tab 3 "IMU Stats: CSIS defensive briefings since May 2021," September 12, 2022.
[386] The Committee notes the Parliamentary Protective Service provides physical security within the Parliamentary precinct.

- Briefings for members of Parliament and the Senate will be provided upon their swearing-in and on a regular basis.[387]

As of February 2024, this approach appears to be unchanged, with no specific briefing program for all parliamentarians on the threat of foreign interference, per the Committee's recommendations in 2018 and 2020.[388]

Interdepartmental governance

130. During the review period, the government created two deputy ministerial committees and one Cabinet committee – the National Security Council – to improve its assessment of intelligence and response to national security threats, including foreign interference.

131. The Deputy Minister Intelligence Committee (DMIC): In 2020, the NSIA created and chaired DMIC, whose mandate was to flag important strategic intelligence assessments to deputy ministers and ensure a coordinated response.[389] Its core membership includes PCO, CSE, CSIS, GAC, Public Safety, the RCMP, the Canada Border Services Agency (CBSA), and the Canadian Armed Forces and Department of National Defence (CAF/DND).[390] The governance structure was designed for getting policy decisions to Cabinet instead of driving the work of the national security community, and the intelligence discussed often lacked the level of detail needed to understand a threat issue.[391] The Committee is only aware of one DMIC meeting in which members discussed intelligence on foreign interference against democratic institutions and processes.[392] DMIC ceased meeting in June 2021, but reconvened in March 2023.[393]

132. The Deputy Ministers' Committee on Intelligence Response (DMCIR): In summer 2023, the NSIA created DMCIR.[394] DMCIR is mandated to review more operational and tactical intelligence reporting that requires a timely response.[395] It also identifies intelligence that should be briefed to Ministers, Cabinet or the Prime Minister and any intelligence already identified for briefing via other means.[396] Membership includes CSE, CSIS, GAC, Public Safety, RCMP and PCO.[397] According to its Terms of Reference, DMCIR began by focusing only on foreign interference issues, but may broaden its scope to include other appropriate issues.[398] PCO

[387] PCO, *Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions*, April 6, 2023.
[388] PCO, Factual Review of NSICOP Report, January 19, 2024.
[389] Vincent Rigby, PROC Evidence, June 8, 2023. Mr. Rigby was the NSIA from January 2020 to June 2021.
[390] PCO, DMIC Terms of Reference, February 2023.
[391] Public Safety, "Governance in Canada's National Security Community," Deck, June 29, 2021.
[392] PCO, "DMIC Agenda," January 2021. This was the only DMIC agenda that PCO provided NSICOP.
[393] PCO, Factual Review of NSICOP Report, January 19, 2024.
[394] Rob Stewart (Deputy Minister of Public Safety during the 2021 election), PROC Evidence, October 19, 2023.
[395] PCO, Factual Review of NSICOP Report, January 19, 2024.
[396] PCO, "Deputy Ministers' Committee on Intelligence Response (DMCIR) Terms of Reference," June 2023; and PCO, Factual Review of NSICOP Report, January 19, 2024.
[397] PCO, "Deputy Ministers' Committee on Intelligence Response (DMCIR) Terms of Reference," June 2023.
[398] PCO, "Deputy Ministers' Committee on Intelligence Response (DMCIR) Terms of Reference," June 2023.

advised the Committee that DMCIR meets weekly, with formal tracking of discussions including the production of meeting minutes.[399]

133. The National Security Council: On September 27, 2023, the Prime Minister announced the creation of the National Security Council, a new committee of Cabinet.[400] The Council first met in October 2023,[401] and is mandated to serve "as a forum for strategic decision-making and for sharing analysis of intelligence in its strategic context."[402] Chaired by the Prime Minister, who stated that he wished to convene it on a regular basis,[403] the members of the Council are the following:

1) Deputy Prime Minister and the Minister of Finance
2) Minister of Defence
3) Minister of Emergency Preparedness
4) Minister of Foreign Affairs
5) Minister of Innovation, Science and Industry
6) Minister of Justice and the Attorney General
7) Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs.[404]

Parliamentary ethics officers

134. In its review of the Prime Minister's official visit to India in 2018, the Committee recommended that "Ministers exercise discretion with whom they meet or associate, and clearly distinguish between official and private media messaging, and be reminded that, consistent with the *Conflict of Interest Act*, public office holders must always place the public interest before private interests."[405] Two independent and non-partisan officers of Parliament support compliance with the Act. The Conflict of Interest and Ethics Commissioner provides members of the House of Commons and federal public office holders with direction and advice about ethics and conflicts of interest with a view to avoid conflicts of interest before they occur. The Senate Ethics Officer plays the same role for Senators. Both officers of Parliament also investigate potential breaches of the *Conflict of Interest Act* and the conflict of interest codes of each chamber.[406]

135. Currently, foreign interference is not defined in the *Conflict of Interest Act* or in the conflict of interest code of either chamber. This being the case, the Conflict of Interest and Ethics

[399] PCO, Factual Review of NSICOP Report, January 19, 2024.
[400] Prime Minister, "Prime Minister announces changes to Cabinet committees," September 27, 2023.
[401] Hon. Dominic LeBlanc, Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs, NSICOP appearance, October 31, 2023.
[402] Prime Minister, "Cabinet Committee Mandate and Membership," September 27, 2023.
[403] Prime Minister, NSICOP appearance, November 7, 2023.
[404] Prime Minister, "Cabinet Committee Mandate and Membership," September 27, 2023.
[405] NSICOP, *Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*, 2018, Recommendation #1.
[406] The *Conflict of Interest Code for Members of the House of Commons* and the *Ethics and Conflict of Interest Code for Senators*. The *Parliament of Canada Act* is the enabling legislation for both officers.

Commissioner and the Senate Ethics Officer are not currently expressly empowered to provide parliamentarians and federal public office holders with advice on how to avoid potential exposure to foreign interference and to investigate conflicts of interest linked or potentially linked to foreign interference as such.

Chapter 4: The Committee's assessment of the response to foreign interference in democratic processes and institutions

136. Foreign interference is not new. For over thirty years, CSIS has been reporting to successive governments on attempts by foreign actors to interfere in Canada's democratic processes and institutions. The Committee's 2019 report on foreign interference marked the first time the issue had been examined by a review body. The Committee was concerned by what it found: Canada was the target of pervasive and sustained foreign interference activities, which the Committee believed posed "a significant risk to the rights and freedoms of Canadians and to the country's sovereignty."[407] This remains the case today.

137. The Committee's previous review did not specifically examine the government's response to threats of foreign interference in the run-up to 43rd federal election, given the government's early efforts to address threats to the election process. These efforts would result in the Plan to Protect Democracy, under which the government established the Critical Elections Incident Public Protocol, amended the *Canada Elections Act*, and implemented mechanisms and initiatives to respond to misinformation and disinformation campaigns. The government later took steps to address the threat of foreign interference more broadly, specifically by establishing an internal, whole-of-government strategy to address this threat, including the creation of the role of Foreign Interference Coordinator and consultations for a foreign influence transparency registry act. The government also adapted its intelligence priorities to learn more about the threat of foreign interference, which brought new information to light about how foreign actors interfere in Canada's democratic processes and institutions. In short, the government has launched or implemented a number of strategic policy initiatives to address foreign interference since our 2019 report, including in areas which specifically address foreign interference targeting democratic processes and institutions.

138. Operational departments have also acted to different degrees. CSIS has conducted a number of Threat Reduction Measures to counter specific instances of foreign interference in democratic processes or institutions, collected and reported intelligence on states and individuals involved in foreign interference in Canada to government, and briefed a number of Parliamentarians on the threat. Under the Ministerial Authorization for Defensive Cyber Operations issued by the Minister of Defence, CSE planned two defensive cyber operations to protect election infrastructure during the two most recent federal elections, which proved to be unnecessary. Additionally, CSE conducted operations under a Ministerial Authorization for Active Cyber Operations to counter *** foreign interference, and collected intelligence on specific foreign actors. The RCMP created a small unit to coordinate investigations of foreign interference and initiated a number of investigations, although it cannot determine exactly how many, nor does it distinguish between those involving democratic processes and institutions and

[407] NSICOP, *2019 Annual Report*, 2020. The 2019 review covered the period 2015 – 2018. This review covers the period 2018 – 2023.

other investigations into foreign interference more generally. No charges have been laid in respect of foreign interference in democratic processes and institutions. For its part, GAC identified a number of online threats through its Rapid Response Mechanism, and expelled one mid-level diplomat for conducting foreign interference following significant media pressure.

139. Notwithstanding these efforts and the considerable intelligence reporting on specific foreign interference activities targeting Canada's democratic processes and institutions, the Committee notes that the intelligence community continues to assess that threat actors view Canada as a permissive environment to pursue their strategic interests.[408]

140. The Committee's assessment explores the persistent disconnect between the gravity of the threat and the measures taken to counter it, a gap which the Committee believes is the reason why threat actors continue to view Canada's democratic processes and institutions as easy targets for foreign interference. As noted in Chapter 1, effective threat mitigation seeks to counter a hostile actor's intent, capability and opportunity to act. While the government has limited ability to address intent and capability, it is accountable for addressing vulnerabilities that permit threat actors to interfere. The state of foreign interference in Canada's democratic processes and institutions cannot be understood without understanding how and why these vulnerabilities persist. The following assessment is divided into three themes: the threat posed to our democratic processes and institutions; the systemic challenges which contribute to Canada being a permissive environment for foreign actors to interfere; and the role that all Parliamentarians must play in reducing the threat. The Committee also shares its views on the leaks of sensitive material and the integrity of the 43rd and 44th federal elections.

The threat of foreign interference in democratic processes and institutions

141. Over the course of its review, the Committee heard from the Prime Minister, three Ministers, and 34 officials from eight departments and agencies, and reviewed over 4,000 documents, including over 1,000 intelligence products. On the basis of this information, the Committee believes there is ample intelligence to support the intelligence community's assertion that foreign interference in democratic processes and institutions constitutes a continuing, significant threat to Canada's national security.

142. The PRC is clearly the most prolific actor. In its efforts to protect and enhance the legitimacy and stability of the Chinese Communist Party domestically and abroad, the PRC employs a comprehensive approach to targeting and leveraging virtually all aspects of Canada's democratic processes and institutions to advance its strategic interests (see paragraph 7 for the Committee's definition of democratic processes and institutions). The Committee underlines the scale and sophistication of the PRC's efforts, which comprise a complex array of covert and overt mechanisms, using PRC and non-PRC entities, ranging from community groups to private enterprises, to accomplish foreign interference in Canada's democratic processes and

[408] CSIS, ***; and CSIS, Email response to question from NSICOP Secretariat, December 11, 2023.

institutions. While not as widespread as the PRC's efforts, India's activities are also of significant concern. India seeks to cultivate relationships with a variety of witting and unwitting individuals across Canadian society with the intent of inappropriately exerting India's influence across all orders of government, particularly to stifle or discredit criticism of the Government of India. The Committee was already aware of India's efforts to interfere in Canada's democratic processes and institutions through its review of the Prime Minister's official visit to India in 2018 and its 2019 foreign interference review. This review reinforced the Committee's understanding of India's activities.

143. In addition to interference against Canadian democratic processes and institutions by the PRC, India and to a limited extent Pakistan, other countries, notably Iran *** engaged in episodic foreign interference directed towards suppressing dissidents and critics in Canada. Known as "transnational repression," these activities represent one of the most egregious forms of foreign interference. The Prime Minister's announcement in Parliament on September 18, 2023 that Canada's intelligence community had been actively pursuing credible allegations of the Government of India's involvement the murder of Canadian citizen Hardeep Singh Nijjar in June 2023 is the latest example.[409] The Committee condemns this and all instances of transnational repression and considers them a threat to Canadian values, human rights and democratic freedoms. However, they are not the focus of this review.

144. In reflecting on the significant body of intelligence pointing to the PRC and India's targeting of democratic processes and institutions, the Committee observed that in almost all cases, the activities could not be construed as regular diplomatic lobbying. Rather, they clearly met the definition of foreign interference as described in Section 2 of the CSIS Act: contrary to Canada's national interest, and deceptive, clandestine or threatening. More worryingly from the Committee's perspective, these states could engage in such activities owing at least in part to challenges and gaps which the Committee had previously identified to the government in 2019. These challenges help to perpetuate a permissive environment for foreign actors to operate.

A permissive environment: How systemic challenges in responding to foreign interference provide opportunities for foreign actors

145. There are four significant unaddressed challenges which help to create an environment where foreign states may interfere in Canada's democratic processes and institutions. These are: differences in thresholds for response to foreign interference; an absence of robust tools to counter the threat; limitations in the dissemination, assessment and use of intelligence; and the lack of effective communication with federal parliamentarians. Each are discussed below.

[409] CBC, "Trudeau accuses India's government of involvement in killing of Canadian Sikh leader," September 2023.

Absence of a common threshold for action

146. The first challenge is the absence of an agreed threshold for action. In its 2019 report, the Committee observed that "[s]ecurity and intelligence organizations do not share a common understanding of the threat, including its gravity in Canada and its most common manifestations."[410] In many ways, this situation continues. While departments and agencies appear to have coalesced around a similar definition of what constitutes foreign interference, differences still persist in measuring the gravity of the threat, recognizing interference in practice and determining thresholds for action. This is particularly problematic in policy departments like PCO and GAC, organizations which make decisions, including on whether to brief ministers on intelligence and to recommend what actions to take in response.

147. Two examples from our review are particularly salient. The first is a decision not to brief the Prime Minister on important intelligence. In February 2023, the Clerk of the Privy Council, the National Security and Intelligence Advisor (NSIA) to the Prime Minister, and deputy heads from CSIS, CSE, GAC and PS met and agreed that a highly sensitive and comprehensive intelligence assessment on foreign interference should be briefed to the Prime Minister. However, the NSIA later concluded that the activities did not constitute foreign interference and did not share the assessment with the Prime Minister.

148. The second example is the decision to expel PRC diplomat Zhao Wei. Until leaks forced the government's hand, GAC had frequently dismissed CSIS reporting on foreign interference activities in democratic processes and institutions, including those conducted by Mr. Zhao. GAC believed that CSIS had misunderstood regular diplomatic behaviour and that the behaviour "did not reach the threshold." We note, however, that GAC has no threshold, codified or customary, to make such decisions, and the Vienna Convention on Diplomatic Relations is silent in this regard.

149. Both examples illustrate the lack of a consistent understanding of a threshold above which permissible diplomatic activities become foreign interference. They also illustrate the difficulty in moving from identifying a problem to addressing it. While the Committee recognizes that defining something as complicated as a threshold for action is difficult, and the absence of a *Criminal Code* offence or other statutory definitions no doubt compounds the problem, decisions as important as these should rest on firmer foundations.

Absence of robust tools

150. The Committee heard repeatedly over the course of its review that an outdated legal framework is hampering the government's response to foreign interference. There are a number of areas for reform. Perhaps the most important are changes to the *Criminal Code* and the *Security of Information Act*, for two reasons. First, amendments should provide clear and modern definitions of foreign interference, helping to clarify what activities do and do not qualify

[410] NSICOP, *2019 Annual Report*, 2020.

as threats. That should ensure departments develop standardized definitions of what constitutes thresholds for action. Second, changes to these statutes would provide more numerous and specific offences for the RCMP to investigate, and signal to current and would-be offenders the gravity of their behaviour. The same logic applies to the proposed legislation for a Foreign Influence Transparency Registry. Crafted carefully to avoid the stigmatization of ethnocultural communities and to protect Canadian rights and freedoms, the legislation should clarify what behaviours qualify as interference, and act both as a deterrent to agents of foreign states and to provide the RCMP with offences to investigate. Similar legislation in allied states has proven to be a useful tool for police to respond to foreign interference.

151. Changes to the CSIS Act are similarly overdue. The CSIS Act is showing its age, particularly with respect to countering foreign interference. Over the course of this review, the Committee noted that CSIS was using its authority to conduct Threat Reduction Measures (TRM) to brief some federal parliamentarians on foreign interference threats posed to them by foreign actors. In this, we believe that CSIS acted in good faith: section 19 (1) of the CSIS Act does not provide CSIS the authority to share classified information to individuals outside the government, but CSIS needed to respond to specific threats and it used a novel authority to do so. At the same time, the Committee believes this is far from ideal. The TRM authority exists to permit CSIS to take measures to reduce a threat where there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada. It was not intended to address CSIS's inability to share classified information outside the government.

152. The requirement for these changes was identified by government departments in 2018, and highlighted by this Committee in 2019. Policy work to develop the Hostile Activities by State Actors (HASA) strategy, which recommended these statutory changes, was well advanced by fall 2019. It took *** the Government two more years to endorse the strategy, in June 2022, another nine months to launch consultations on a foreign influence registry in March 2023, and another eight months to launch public consultations on amendments to the *Criminal Code*, the SOIA and the CSIS Act in November 2023. At the end of this review, the government assured the Committee that it intended to table legislation for the Foreign Influence Transparency Registry "imminently." While the Committee welcomes that commitment and looks forward to seeing the bill, the Committee believes that delays in launching public consultations and tabling legislation were unnecessary, and represent a lost opportunity to build upon the changes the government implemented in 2018 to address threats posed by foreign interference in Canada's democratic processes and institutions.

153. There are two other areas for statutory reform. The first is in the area of "intelligence and evidence." Intelligence agencies take great care in protecting their sensitive collection techniques, confidential sources and intelligence shared from allies. The disclosure of such information in a court could reduce the effectiveness of future operations, endanger sources and damage relations with foreign partners. Consequently, if CSIS or CSE decides to share intelligence with law enforcement, it does so knowing that it risks being disclosed in court if the police investigation leads to a criminal trial. The Committee noted numerous instances over the course of its review in which intelligence agencies did not share information with enforcement

bodies, including the RCMP and the Office of the Commissioner of Canada Elections, for this reason. The Committee believes this is a critical problem, where significant differences exist between operational organizations and the Department of Justice. The creation of new criminal offences for foreign interference activities will matter little if law enforcement bodies still cannot rely on information derived from intelligence collection. This is a foundational, complex issue which merits its own review. In the meantime, the government should review the legislative options which have been developed that could start to address the problem.

154. The second area for legislative reform is the regulation of political nomination processes. The Committee was disturbed to learn how easily foreign actors take advantage of loopholes and vulnerabilities in political party governance and administration to support preferred candidates or to gain access to other influential positions within the parties, most notably in the context of candidate nomination processes. This is a critical gap, because a number of ridings in Canada are considered "safe seats" for one party or another, so a successful nomination may amount to a candidate's election. Because the number of votes required to sway riding nominations is so small, they are a useful avenue for foreign states to engineer the election of their preferred candidate. While the *Canada Elections Act* imposes administrative penalties on fundraising by a foreign entity, Canada does not criminalize interfering in nominations or in any other political party process. The government should do so. It should also engage all political parties to determine whether party nomination processes should be included within the framework of the *Canada Elections Act*, subject to monitoring by Elections Canada and the Office of the Commissioner for Canada Elections.

155. In the meantime, federal political parties themselves have a role to play. Parties need to reduce or eliminate opportunities for foreign states to directly or indirectly interfere in a foundational part of our democratic system – the nomination process – by identifying and addressing vulnerabilities in their own systems and processes, including in areas such as age and residency requirements and fundraising. More generally, the government should work with all parties to establish the means to allow CSIS and other intelligence organizations to raise with party leaders specific instances of foreign interference occurring prior to, during and after an election, so that those instances may be addressed. The Committee further encourages the government to give the same consideration to other orders of government.

156. The Committee does not call for legislative reform lightly. As legislators, Committee members recognize the complexity and significance of statutory reform. However, it has become clear that the initiatives implemented by the government in 2018 – the Critical Election Incident Public Protocol, the Panel, SITE and the Rapid Response Mechanism – are insufficient on their own to address the threat. While the Committee recognizes that CSIS's Threat Reduction Measures and CSE's Active and Defensive Cyber Operations play important roles in addressing interference in democratic processes and institutions, their use is limited by circumstance (among other things) and their effects are hard to measure in terms of disruption or deterrence. Addressing these limitations requires, at least in part, specific legislative reforms. In short, the security and intelligence community needs more tools. The government should see that it has them and be properly resourced to use them.

The distribution, assessment and use of intelligence

157. It is clear that there are systemic problems in the distribution, assessment and use of intelligence to inform decision-making on foreign interference. In the time period under review, the government adapted its intelligence priorities to learn more about the threat of foreign interference, causing intelligence organizations to increase their collection and assessment. It is unclear whether this change made a material difference to the officials in departments responsible for policymaking and decision-making.

158. The Committee wishes to underscore that decision-makers from policy departments (Privy Council Office, Public Safety and Global Affairs Canada), not intelligence organizations (CSIS, CSE), are ultimately responsible for providing policy advice and recommendations on how to respond to intelligence about foreign interference. In that respect, the Committee is concerned that, while intelligence organizations have increased their reporting on foreign interference, policy departments lack the instinct to make responsive recommendations based on that reporting. On the one hand, the Committee observed strong, if slow, engagement by the three policy departments in the development of strategic policy proposals, like the Hostile Activities by State Actors Strategy. On the other, the Committee saw little evidence that these departments saw a role for themselves in responding to intelligence reporting by providing separate policy advice to their respective ministers (although the Committee notes that in March 2023 GAC commenced briefing the Minister of Foreign Affairs on intelligence reporting relevant to the security of Canada, whereas it had previously focused on international issues). In fact, the Committee found few cases where these departments made any recommendations to their respective ministers when provided intelligence on specific threats or summary assessments of threat actors, except in reaction to the media. At the same time, it does not appear that the Ministers responsible for those departments, who are ultimately accountable for protecting Canada against foreign interference, requested policy advice in response to intelligence reporting. If this context persists, it will not matter how much the intelligence community collects and assesses if its reports are simply read by officials and then ignored.

159. That said, the intelligence community could make it easier for their reports to have an impact. First, the dissemination of intelligence products across the government is uneven, with the most important items marked for a very limited number of senior-level officials, who often have little time to read and digest such information, and are not shared with the policy experts who would be responsible for advising on a proposed response. Additionally, systems for dissemination are inconsistent across the intelligence community: notably, CSE's electronic dissemination system permits clients (i.e., those that receive intelligence products) to track readership and search for items, while CSIS's distribution system lacks this function. This inconsistency creates challenges for clients in developing strategic policy advice. Clients must either develop their own summary of intelligence reporting over time, which is difficult because they are not intelligence professionals, or they must rely on intelligence agencies to provide summary products and assessments for use in decision-making, which is difficult because intelligence organizations are not expert on the mandates and authorities of their clients.

160. Second, intelligence agencies often remove information that would be salient for officials in the belief that the information is too sensitive or on the assumption that the sanitized information would still be compelling. Conversely, in some cases, senior officials have requested that intelligence agencies pull back published reports because *they* believed the information was too politically sensitive. Not only does this behaviour create a chilling effect on intelligence collection and assessment, depriving the government of the full context of its decisions, it also undermines a core public service value of providing "fearless advice" and risks politicizing the community's own intelligence reporting to suit the inclinations of the government of the day. This issue should be of concern for this and all future governments.

161. In short, intelligence must be both available and specific enough to be persuasive to decision-makers. As such, the Committee believes there is space for closer collaboration between intelligence producers and consumers in drafting intelligence assessments based on a shared understanding of the threat and a common threshold for action, where each side can bring to bear their expertise and understanding of their mandates. The Committee believes such collaboration would strengthen the work of two new governance bodies. The first is the Deputy Minister Committee on Intelligence Response, which the Committee understands as a forum for senior public servants to consider intelligence reporting from a government-wide perspective, weigh national security against other important considerations, including international relations, and develop recommendations to support decision making by relevant Ministers or Cabinet. The second and most important body is Cabinet itself. The Committee welcomes the creation of the National Security Council (NSC) and the Prime Minister's stated commitment to its success. The Committee hopes that the Council will not only drive necessary reforms in the security and intelligence community, especially as they pertain to foreign interference in democratic processes and institutions, but also provide an effective forum to discuss specific threats and take decisions to address them. More importantly, the Committee hopes that these bodies will strengthen the accountability of government in addressing foreign interference threats.

Engagement with Parliamentarians

162. The final tool which the Committee emphasizes is important to address foreign interference is engagement with Parliamentarians. In its 2018 report on the Prime Minister's official visit to India and its 2019 report on foreign interference, the Committee recommended that all members of the House of Commons and the Senate receive briefings regarding foreign interference upon being sworn in and regularly thereafter. It did so because Parliamentarians are often at the center of interference activities by foreign states. While the Committee recognizes that CSIS has provided briefings to some members of Parliament, a comprehensive briefing strategy covering all Parliamentarians was not implemented despite PCO seeking the Prime Minister's approval on two occasions. The Committee considers the Prime Minister's lack of action on this recommendation to be a serious omission. This initiative was comparatively simple to implement: PCO and CSIS were ready to act and could have done so quickly. That it was not represents an unfortunate and potentially consequential missed opportunity.

The role of Parliamentarians in addressing foreign interference

163. The Committee recognizes that the problem of foreign interference in democratic institutions and processes is not the government's alone to solve. Parliamentarians have a role to play as well. The Committee has seen considerable evidence that Parliamentarians across all parties and groups are potential *targets* for interference activities of foreign states and actors because of the roles they play in Parliament, in Cabinet and within the communities they represent. As such, Parliamentarians need to ensure ethical and lawful conduct in their engagement and activities with foreign officials. The Conflict of Interest and Ethics Commissioner and the Senate Ethics Officer could play a role, in this regard, if they were respectively empowered to provide Parliamentarians with direction and advice on how to avoid exposure to foreign interference, and to investigate allegations linked to foreign interference. More broadly, Parliamentarians should also consider what vulnerabilities persist in areas that they themselves control, such as their official business, including sponsored travel, party nominations or engagements with foreign officials. In doing so, it would become it harder for foreign states to target them and their parties.

164. Unfortunately, the Committee has also seen troubling intelligence that some Parliamentarians are, in the words of the intelligence services, "semi-witting or witting" *participants* in the efforts of foreign states to interfere in our politics. These examples include:

- Communicating frequently with foreign missions before or during a political campaign to obtain support from community groups or businesses which the diplomatic missions promise to quietly mobilize in a candidate's favour;
- Accepting knowingly or through willful blindness funds or benefits from foreign missions or their proxies which have been layered or otherwise disguised to conceal their source;
- Providing foreign diplomatic officials with privileged information on the work or opinions of fellow Parliamentarians, knowing that such information will be used by those officials to inappropriately pressure Parliamentarians to change their positions;
- Responding to the requests or direction of foreign officials to improperly influence Parliamentary colleagues or Parliamentary business to the advantage of a foreign state; and,
- Providing information learned in confidence from the government to a known intelligence officer of a foreign state.

These are particularly concerning examples of behaviour by a few Parliamentarians. Some may be illegal, but are unlikely to lead to criminal charges, owing to Canada's failure to address the long-standing issue of protecting classified information and methods in judicial processes. Regardless, all the behaviours are deeply unethical and, the Committee would submit, contrary to the oaths and affirmations Parliamentarians take to conduct themselves in the best interest of Canada. While some of the Committee's recommendations should help the government to address instances of foreign interference abetted by Parliamentarians, the Committee reminds its colleagues that their duty as Parliamentarians is to the people of Canada.

Committee comments

The Committee's comment on unauthorized disclosure of intelligence (the leaks)

165. The genesis of this review was media reporting based on unauthorized leaks of highly sensitive intelligence. It is not the Committee's mandate to investigate the leaks, nor comment on individual allegations reported in the media. That said, the Committee is deeply troubled by both the leaks and the media's decision to publish material derived from highly classified intelligence. There are justifiable reasons why the government cannot share information with the public, not least of which is to protect confidential sources and methods and the integrity of its relationships with allies. The leaks may well have *** undermined specific aspects of Canada's national security. They certainly have provided hostile threat actors with critical information about the government's capabilities, vulnerabilities and plans, doing significant damage to intelligence collection efforts and to Canada's reputation as a trusted foreign partner. The Committee rejects any notion that the individual or individuals responsible for the leaks acted as patriots or whistleblowers.

166. On the other hand, the Committee acknowledges an uncomfortable truth. Prior to the leaks, there was little sense of urgency between elected officials and senior decision-makers to address outstanding gaps to this important and well-documented threat to national security. Regrettably, the leaks were the principal catalyst for the government to start considering key legislative reforms and to take meaningful actions against particular states. But the ends do not justify the means and that is not how our system should work. Canada is a parliamentary democracy. The illegal actions of one or more individuals should not drive policy and legislative changes. The elected government, with the support of Parliament, must set the agenda. It is unfortunate that it took leaks to do so.

The Committee's comment on the Critical Elections Incident Public Protocol and the integrity of the 43rd and 44th federal elections

167. As the Canadian public has learned from the reports of the Critical Elections Incident Public Protocol and the Independent Special Rapporteur on Foreign Interference, the government was aware of foreign interference activities during the 43rd and 44th general elections. Often, these activities targeted specific political candidates and ridings. However, the reports agreed that the overall integrity of the respective elections was maintained. While the Committee did not focus exclusively on the 43rd and 44th elections, it did not observe any material in its review to suggest that the Protocol reports' or the Independent Special Rapporteur's conclusions were incorrect. Nonetheless, it notes two concerns.

168. First, the Committee cautions future Panels about relying too heavily on a clear link to a foreign state. In the case of the potential disinformation campaign about the Conservative Party's position on the PRC flagged by Kenny Chiu and the Honourable Erin O'Toole, the Committee is concerned that the Protocol set too high a bar by relying on definitive state attribution when the indicators of a coordinated campaign were evident. Direct state attribution

will always be challenging, if not impossible, given states' efforts to conceal disinformation campaigns through proxies and other means. It appears that the Rapid Response Mechanism is successfully addressing this dynamic in its June 2023 public announcement of an information campaign targeting Member of Parliament Michael Chong. Implementation of the Protocol should evolve in a similar manner.

169. Second, the Committee joins the authors of those reports in noting the difficulty in determining the effects of foreign interference in specific ridings. Foreign states and their proxies clearly intended and attempted to interfere in the elections, but to the extent that can be determined they were not successful in swaying the overall outcome of the election. This should not give Canadians great comfort. By expanding its review of foreign interference activities directed at democratic processes and institutions outside of the previous two elections, the Committee saw concerning intelligence of foreign states interfering in, for example, specific nomination processes and riding elections. The Committee was disturbed to learn that these foreign states often believed their efforts had an impact, which would likely encourage similar behaviour in the future.

170. In the Committee's view, foreign interference in even one riding is too many. The threat is persistent and pervasive. The government must ensure that foreign interference is not left unchecked, lest it become determinative both in future elections at the party nomination and riding levels and more broadly in Canada's democratic processes and institutions.

Conclusion

171. This report represents the third time the Committee has reviewed the government's response to threats of foreign interference. Its 2018 report introduced the Committee to the threat in the specific context of the Prime Minister's official visit to India. Its 2019 report was a more thorough examination of foreign interference activities from 2015 to 2018. Although the Committee opted not to study electoral interference in light of the government's early efforts to counter specific threats in this area, its recommendations to counter foreign interference were sufficiently broad to address interference across a wide spectrum, including democratic processes and institutions (see Annex D). Given the risks posed by foreign interference to Canada's national security, the Committee expected the government to act. It was slow to do so. Indeed, the Prime Minister has acknowledged publicly that the government needed to do a better job of following up on the Committee's recommendations.[411]

172. In the Committee's view, this delay contributed in part to the crisis in which the government found itself in late 2022 and early 2023. A number of unauthorized leaks of intelligence raised significant concerns about the state of foreign interference in Canada and in our democratic processes and institutions. The Prime Minister requested three separate reviews, one by the Independent Special Rapporteur on Foreign Interference, one by the National Security and Intelligence Review Agency, and one by this Committee. Specifically, he asked the Committee to "assess the state of foreign interference in federal election processes" with respect to "foreign interference attempts that occurred in the 43rd and 44th federal general elections, including potential effects on Canada's democracy and institutions."[412]

173. The Committee accepted the Prime Minister's request, expanding its scope in order to conduct a review that captured the broader issues of foreign interference in our democratic processes and institutions. This review revealed that the reforms implemented by the government in 2018 were insufficient to address foreign interference in democratic processes and institutions. While the government recognized this gap in 2018, it took four years to develop and approve its "Hostile Activities by State Actors" strategy. A key part of the strategy, consultations on legislative reforms, was then delayed by over a year. The length of this process did not, in the Committee's view, demonstrate a sense of urgency commensurate with the gravity of the threat.

174. The delay in these actions, many of which had been recommended by the Committee, undermined the government's operational responses to the threat. With no new tools, the security and intelligence community was forced to rely upon existing authorities and legislation. Gaps in these areas limited the ability of security and intelligence organizations to act, particularly with respect to sharing information with law enforcement bodies to enable investigations, lay charges or support prosecutions. Similarly, CSIS was largely unable to share

[411] CBC News, "Prime Minister admits he hasn't heeded intelligence watchdog's recommendations in the past," March 2023.
[412] Prime Minister, "Taking further action on foreign interference and strengthening confidence in our democracy," March 6, 2023.

salient information with key stakeholders outside of the federal government, notably with Parliamentarians and other orders of government. These gaps contribute to a situation in which there are few meaningful deterrents to foreign states and their Canada-based proxies to conduct interference activities.

175. The slow response to a known threat was a serious failure and one from which Canada may feel the consequences for years to come. The implications of this inaction include the undermining of the democratic rights and fundamental freedoms of Canadians, the integrity and credibility of Canada's parliamentary process, and public trust in the policy decisions made by the government. Canada is only now beginning to see the introduction of additional measures to address foreign interference activities.

176. The threat of foreign interference is pervasive and persistent. It is imperative that the government act now to address the vulnerabilities that make Canada's democratic processes and institutions an easy target. The government must ensure that legislation keeps pace with this evolving threat so that the security and intelligence community has the tools it needs to respond to the threat in a way that discourages future interference efforts. It must clearly define thresholds for response and clarify the roles and mandates of governance bodies to support a coherent and coordinated response to instances of foreign interference, and the accountabilities of Ministers. The government must also address deficiencies in how intelligence is distributed, assessed and used internally, and in doing so build a culture where officials and Ministers alike are seized with and accountable for identifying challenges and taking decisions to address them.

177. Bearing in mind its responsibility for ensuring Canada's national security, the federal government needs to act swiftly to remove the obstacles that prevent it from playing an effective leadership role throughout the country in countering foreign interference. These include outdated legislation governing the sharing of classified information, stalled initiatives to inform the Canadian public and other key stakeholders, and the absence of mechanisms to engage other orders of government. The Committee underscores that briefing Parliamentarians on the threat is imperative.

178. Finally, Parliamentarians have a role to play. They must recognize that as lawmakers, they may be targets of foreign interference because of the positions they occupy and the decisions they take. The Committee calls on Parliamentarians to carefully consider all ethical and legal ramifications of their engagement with foreign officials or their proxies, and act to reduce their own vulnerabilities. Foreign interference is not "politics as usual." Parliamentarians must be part of the solution.

Findings

179. The Committee makes the following findings:

F1 Foreign states conduct sophisticated and pervasive foreign interference specifically targeting Canada's democratic processes and institutions, occurring before, during and after elections and in all orders of government. These activities continue to pose a significant threat to national security, and to the overall integrity of Canada's democracy. The PRC and India are the most active perpetrators.

F2 The government was aware in 2018 that the reforms implemented under the Plan to Protect Democracy were insufficient to address foreign interference in democratic processes and institutions. It has yet to implement an effective response to foreign interference in democratic processes and institutions. This is despite a significant body of intelligence reporting, the completion of foundational policy work, public consultations and having been called to do so by this Committee.

F3 Significant differences persist in how Ministers, departments and agencies interpret the gravity and prevalence of the threat, including the threshold for response.

- The intelligence community increased its reporting to the government on the threat of foreign interference in Canada's democratic processes and institutions in response to Canada's intelligence priorities.
- Policy departments (Privy Council Office, Global Affairs Canada, and Public Safety) did not adequately consider intelligence reporting or assessments, or develop policy advice to address specific cases of foreign interference.
- Ministers accountable for national security did not request policy advice in response to intelligence reporting and the government was slow to put in place governance structures to consider intelligence and take decisions.

F4 The roles, mandates and accountabilities of the National Security Council and supporting governance committees are unclear.

F5 Canada's current legal framework does not enable the security and intelligence community or law enforcement to respond effectively to foreign interference activities. This impedes the federal government's ability to engage other orders of government and law enforcement with respect to sharing and use of classified intelligence, respectively.

F6 While departments and agencies conducted operations to disrupt or deter foreign interference, tangible results with respect to the level of actual threat reduction were difficult to measure.

F7	The government continues to lack an effective approach to engage with the Canadian public and other orders of government. While it has increased engagement with some Parliamentarians, political parties and electoral candidates, its efforts have been time-bound (i.e., election-focused), narrowly targeted, often reactive and the information provided too general. It has also repeatedly failed to implement a comprehensive approach to engaging federal Parliamentarians.
F8	The government's ability to address vulnerabilities in political party administration is limited.

Recommendations

180. The Committee makes the following recommendations:

R1 The government table legislation before the next federal election to address gaps in Canada's legal framework with respect to foreign interference, specifically to:

a) Create a foreign influence transparency registry;
b) Amend the *Criminal Code* and the *Security of Information Act* to define foreign interference and introduce relevant offences;
c) Modernize the *Canadian Security Intelligence Service Act*, including to facilitate wider sharing of classified information;
d) Address the intelligence and evidence challenge; and,
e) Reduce vulnerabilities in political nomination processes, including leadership conventions.

R2 The government engage political parties to determine whether party nomination processes and leadership conventions be included within the framework of the *Canada Elections Act*, and work with Parliament to determine whether the statute governing the Conflict of Interest and Ethics Commissioner and the Senate Ethics Officer be revised to include foreign interference.

R3 The government review and renew legislation, strategies and funding to ensure they keep pace with the evolution of foreign interference activities and other national security threats, and regularly include and respect legislative review provisions in national security legislation.

R4 The government ensure that the roles, mandates and accountabilities of the National Security Council and supporting governance committees are clear and publicly communicated to improve transparency and performance.

R5 The security and intelligence community develop consistent definitions and thresholds for action with respect to foreign interference, and organizations responsible for intelligence collection and those responsible for providing policy advice, respectively, regularly collaborate to provide the government timely and comprehensive assessments of threats and advice for action.

R6 The government immediately implement and report annually on the briefings for Parliamentarians on the threat of foreign interference.

Annexes

Annex A: List of witnesses

The Ministry

- The Right Honourable Justin P.J. Trudeau, P.C., M.P., Prime Minister of Canada
- The Honourable Mélanie Joly, P.C., M.P., Minister of Foreign Affairs
- The Honourable Dominic Leblanc, P.C., M.P., Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs
- The Honourable Arif Virani, P.C., M.P., Minister of Justice and Attorney General of Canada

Canadian Security Intelligence Service

- Director
- Deputy Chief, Foreign Interference
- Foreign Interference Coordinator
- Director General, ***
- Acting Director General, ***
- Deputy Chief, ***
- Senior Intelligence Analyst

Communications Security Establishment

- Deputy Chief, Authorities, Compliance and Transparency
- Director General, ***
- Director General, ***
- Director, ***
- Director, ***

Elections Canada

- Chief Electoral Officer of Canada
- Deputy Chief Electoral Officer, Security and Digital Transformation

Global Affairs Canada

- Deputy Minister of Foreign Affairs
- Assistant Deputy Minister, Indo-Pacific
- Chief Intelligence Officer, Director General Intelligence Bureau
- Director General, Office of Human Rights, Freedoms, and Inclusion

Justice Canada

- Deputy Minister of Justice and Deputy Attorney General
- Assistant Deputy Minister, Public Safety, Defence and Immigration
- Deputy Assistant Deputy Minister, Policy Sector

Office of the Commissioner of Canada Elections

- Commissioner of Canada Elections
- Senior Director, Enforcement

Privy Council Office

- Deputy Clerk
- Deputy Secretary to the Cabinet, Governance
- National Security and Intelligence Advisor to the Prime Minister
- Assistant Secretary to the Cabinet, Security and Intelligence
- Assistant Secretary to the Cabinet, Machinery of Government
- Executive Director, Task Force on Foreign Interference

Public Safety Canada

- Associate Deputy Minister
- National Counter-Foreign Interference Coordinator and Assistant Deputy Minister, National and Cyber Security Branch
- Director, Counter-Foreign Interference
- Director, National Security Operations

Royal Canadian Mounted Police

- Deputy Commissioner, Federal Policing
- Acting Assistant Commissioner, Federal Policing National Security
- Acting Director General, Federal Policing Intelligence and International Policing
- Senior Advisor, Federal Policing Strategic Management

Annex B: Terms of Reference

Review: Foreign interference in Canada's federal democratic processes

Overview

On March 6, 2023, the Prime Minister requested that the National Security and Intelligence Committee of Parliamentarians (NSICOP, or the Committee) "complete a review to assess the state of foreign interference in federal electoral processes" with respect to "foreign interference attempts that occurred in the 43rd and 44th federal general elections, including potential effects on Canada's democracy and institutions."

The Committee met on March 7, 2023 and considered the Prime Minister's request. It decided on a broader review under paragraph 8(1)(a) of the NSICOP Act of the state of foreign interference in Canada's federal democratic processes, from 2018 to the present, and may examine other periods, where relevant. The Committee will consider the latest independent assessment of the Critical Election Incident Public Protocol.

On March 8, 2023, the Committee announced its Review of Foreign interference in Canada's federal democratic processes, 2018 - present. The review will build on the Committee's 2019 review of the government's response to foreign interference, which focused on the period January 1, 2015 to August 31, 2018.

Definitions

The *Canadian Security Intelligence Service Act* describes "foreign influenced activities" as "activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person." The term "foreign influence" also appears in the *Security of Information Security Act*.

That said, the term "foreign interference" has become common in Canada and among its allies to better distinguish between acceptable diplomatic practices and hostile or unlawful practices. The Committee uses "foreign interference," but emphasizes that its definition is identical to that of "foreign influenced activities," as described in the *Canadian Security Intelligence Service Act*.

Democratic processes and institutions include the candidate nomination process, fundraising and donations, the campaign, and the election itself, and key actors such as voters, political parties, lobby groups, community organizations and the media.

Foreign interference in democratic processes and institutions can include using deceptive means to "cultivate relationships with elected officials and others perceived to possess influence in the political process; seek to influence the reporting of Canadian media outlets; seek, in some cases, to affect the outcome of elections; and coerce or induce diaspora communities to

advance foreign interests in Canada." It can also include the spread of false narratives through disinformation campaigns.

Objectives

This review has two primary objectives. The first is to examine the state of foreign interference in Canada's federal democratic processes and institutions.

The second objective is to examine the federal government's response to the threat of foreign interference in Canada's federal democratic processes and institutions, including:

- Strategies, policies, and approaches to protecting Canada's federal democratic processes and institutions from this threat;
- The implementation and resourcing of the operational response to the threat;
- Interdepartmental coordination of the policy and operational response to the threat;
- The legislative frameworks for investigating, prohibiting, preventing or countering this threat;
- The engagement by relevant organizations with ministers or their offices on related threats, issues, or challenges, or in the use of organizational authorities to investigate, disrupt, or collect information on such threats.

As with previous reviews, the Committee will arrive at findings and make recommendations. Officials and others will be called, as required.

The review may provide an update about the government responses of the other countries to foreign interference in national democratic processes and institutions.

Cooperation with NSIRA

Consistent with paragraph 9 of the NSICOP Act, the Committee will take all reasonable steps to cooperate with the National Security and Intelligence Review Agency to avoid unnecessary duplication of work in relation to the fulfilment of their respective mandates. This will include regular coordination meetings between Secretariats and may include shared document requests and information briefings.

Appearances

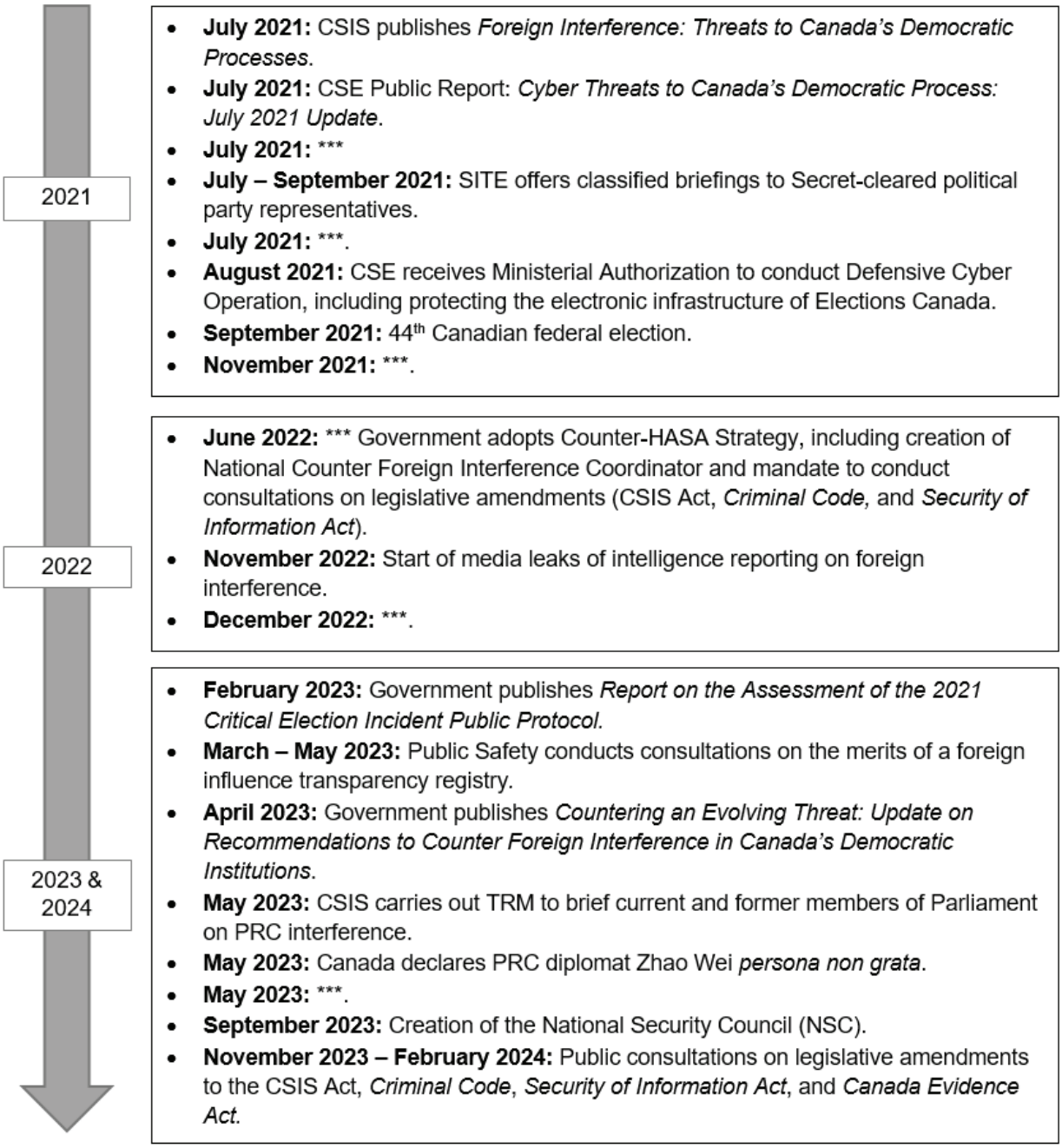
Consistent with paragraph 18 of the NSICOP Act, government officials will be invited to appear before the Committee in private. The Committee will publish a list of senior officials who appear.

Annex C: Timeline of the government's response to foreign interference in democratic processes and institutions, 2018 to 2024

- **May 2018:** NSICOP submits its classified report on the Prime Minister's Visit to India in February 2018 to the Prime Minister (see Annex D).
- **June 2018:** Canada announces G7 Rapid Response Mechanism at G7 Summit.
- **July 2018:** Public Safety begins developing a strategy to counter Hostile Activities by State Actors (HASA).
- ***** 2018:** *** Plan to Protect Canada's Democracy, including the Critical Election Incident Public Protocol and the Security and Intelligence Threats to Elections Task Force (SITE).
- **December 2018:** Prime Minister Tables NSICOP Special Report on the Prime Minister's Visit to India in February 2018.
- **December 2018:** *Elections Modernization Act* receives Royal Assent, amending the *Canada Elections Act*.

- **February 2019:** Release of CSE Public Report: *Cyber Threats to Canada's Democratic Process*.
- **July – September 2019:** SITE offers classified briefings to Secret-cleared political party representatives.
- **August 2019:** ***.
- **August 2019:** NSICOP submits its classified report on foreign interference to the Prime Minister (see Annex D).
- **August 2019:** CSE receives Ministerial Authorization to conduct Defensive Cyber Operation, including protecting the electronic infrastructure of Elections Canada.
- **October 2019:** 43rd Canadian federal election.

- **March 2020:** Prime Minister tables NSICOP Annual Report 2019 in Parliament, which includes the report on foreign interference.
- **May 2020:** *Report on the Assessment of the 2019 Critical Election Incident Public Protocol*.
- **October 2020:** ***.
- **December 2020:** ***.


2021
July 2021: CSIS publishes Foreign Interference: Threats to Canada's Democratic Processes.
July 2021: CSE Public Report: Cyber Threats to Canada's Democratic Process: July 2021 Update.
July 2021: ***
July – September 2021: SITE offers classified briefings to Secret-cleared political party representatives.
July 2021: ***.
August 2021: CSE receives Ministerial Authorization to conduct Defensive Cyber Operation, including protecting the electronic infrastructure of Elections Canada.
September 2021: 44th Canadian federal election.
November 2021: ***.
2022
June 2022: *** Government adopts Counter-HASA Strategy, including creation of National Counter Foreign Interference Coordinator and mandate to conduct consultations on legislative amendments (CSIS Act, Criminal Code, and Security of Information Act).
November 2022: Start of media leaks of intelligence reporting on foreign interference.
December 2022: ***.
2023 & 2024
February 2023: Government publishes Report on the Assessment of the 2021 Critical Election Incident Public Protocol.
March – May 2023: Public Safety conducts consultations on the merits of a foreign influence transparency registry.
April 2023: Government publishes Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions.
May 2023: CSIS carries out TRM to brief current and former members of Parliament on PRC interference.
May 2023: Canada declares PRC diplomat Zhao Wei persona non grata.
May 2023: ***.
September 2023: Creation of the National Security Council (NSC).
November 2023 – February 2024: Public consultations on legislative amendments to the CSIS Act, Criminal Code, Security of Information Act, and Canada Evidence Act.

Annex D: Foreign interference-related findings and recommendations from NSICOP's 2019 annual report

Findings:

F8. Some foreign states conduct sophisticated and pervasive foreign interference activities against Canada. Those activities pose a significant risk to national security, principally by undermining Canada's fundamental institutions and eroding the rights and freedoms of Canadians. (Paragraphs 136–175)

F9. CSIS has consistently conducted investigations and provided advice to government on foreign interference. (Paragraphs 195–201)

F10. Throughout the period under review, the interdepartmental coordination and collaboration on foreign interference was case-specific and ad hoc. Canada's ability to address foreign interference is limited by the absence of a holistic approach to consider relevant risks, appropriate tools and possible implications of responses to state behaviours. (Paragraphs 219–227 and 280–285)

F11. Foreign interference has received historically less attention in Canada than other national security threats. This is beginning to change with the government's nascent focus on "hostile state activities." Nonetheless, the security and intelligence community's approach to addressing the threat is still marked by a number of conditions:

- There are significant differences in how individual security and intelligence organizations interpret the gravity and prevalence of the threat, and prioritize their resources. (Paragraphs 276–279)
- In determining the measures the government may use to address instances of foreign interference, responses address specific activities and not patterns of behaviour. Furthermore, the government's approach gives greater weight to short-term interests (e.g., foreign policy) than longer-term considerations (e.g., risks to freedoms, rights and sovereignty). (Paragraphs 281–285)

F12. Government engagement on foreign interference has been limited.

- With the exception of CSIS outreach activities, the government's interactions with sub-national levels of government and civil society on foreign interference is minimal. (Paragraphs 256–267)
- Engagement is limited in part by the lack of security-cleared individuals at the sub-national level. (Paragraph 261)
- There is no public foreign interference strategy or public report similar to those developed for terrorism or cyber security. (Paragraphs 289–291)

F13. Canada is working increasingly with its closest allies and partners to address foreign interference. This is essential for Canada. (Paragraphs 268–274)

Recommendations:

R5. The Government of Canada develop a comprehensive strategy to counter foreign interference and build institutional and public resiliency. Drawing from the Committee's review and findings, such a strategy should:

a. identify the short- and long-term risks and harms to Canadian institutions and rights and freedoms posed by the threat of foreign interference;

b. examine and address the full range of institutional vulnerabilities targeted by hostile foreign states, including areas expressly omitted in the Committee's review;

c. assess the adequacy of existing legislation that deals with foreign interference, such as the *Security of Information Act* or the *Canadian Security Intelligence Service Act,* and make proposals for changes if required;

d. develop practical, whole-of-government operational and policy mechanisms to identify and respond to the activities of hostile states;

e. establish regular mechanisms to work with sub-national levels of government and law enforcement organizations, including to provide necessary security clearances;

f. include an approach for ministers and senior officials to engage with fundamental institutions and the public; and

g. guide cooperation with allies on foreign interference.

R6. The Government of Canada support this comprehensive strategy through sustained central leadership and coordination. As an example of a centralized coordinating entity to address foreign interference, the Committee refers to the appointment and mandate of the Australian National Counter Foreign Interference Coordinator.

The Committee reiterated a recommendation from its *Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*:

In the interest of national security, members of the House of Commons and Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada. In addition, Cabinet Ministers should be reminded of the expectations described in the Government's *Open and Accountable Government*, including that Ministers exercise discretion with whom they meet or associate, and clearly distinguish between official and private media messaging, and be reminded that, consistent with the *Conflict of Interest Act*, public office holders must always place the public interest before private interests.