Report on the assessment of the 2021 Critical Election Incident Public Protocol

Morris Rosenberg

Report on the Assessment of the 2021 Critical Election Incident Public Protocol.

For more information, contact:

Privy Council Office
85 Sparks Street, Room 1000
Ottawa ON Canada K1A 0A3
info@pco-bcp.gc.ca

Cette publication est également disponible en français : *Rapport sur l'évaluation du Protocole public en cas d'incident électoral majeur pour 2021.*
CP22-193/2023E-PDF
ISBN: 978-0-660-47651-3

TABLE OF CONTENTS

Introduction

Mandate

I have been retained by the Privy Council Office to prepare an independent report on the Critical Election Incident Public Protocol (the Protocol), its implementation and its effectiveness in addressing threats to the 44th General Election which took place on September 20, 2021.

The requirement for an independent report is found in section 9.0 of the Protocol:

"Following each general election, an independent report will be prepared, assessing the implementation of the Critical Election Incident Public Protocol and its effectiveness in addressing threats to the election. This report will be presented to the Prime Minister and to the National Security and Intelligence Committee of Parliamentarians. A public version will also be developed. These reports are intended to help inform whether adjustments to the Protocol should be made".

The Directive was put into place in 2019 in advance of Canada's 43rd General Election. Prior to its approval at Cabinet, the Protocol was shared with the four parties represented in the House of Commons. It is only one element of an integrated plan to strengthen Canada's electoral system against cyber and other threats. The Protocol is a mechanism for a panel of five senior public servants (the Panel) to communicate clearly, transparently, and impartially with Canadians during an election in the event of an incident or incidents that threaten the integrity of a federal election.

In announcing the Protocol, the then Minister of Democratic Institutions explained that it was designed to avoid the kind of gridlock that could prevent an effective response to threats to the integrity of the election. She also emphasized that the Protocol has a very narrow scope and a very high threshold for a public announcement. It would only apply during the writ period[1]. She added that "Our hope is that such a public announcement never happens, but it is essential that we inform Canadians now of a structure in place to keep them informed and engaged".[2]

Methodology

This review is based on a number of sources. Firstly, there were interviews with all the members of the 2021 election Panel, some members of the 2019 Panel, the Chief Electoral Officer (CEO) and the former Commissioner of Elections. There were also interviews with representatives of the national security agencies (NSAs) and other government officials. There was an opportunity to meet with representatives of major political parties, civil society and academic actors and social media platforms.

[1] See Annex A for Glossary of terms.

[2] See Democratic Institutions Website https://www.canada.ca/en/democratic-institutions/services/reports/report-assessment-critical-election-incident-public-protocol.html.

I had access to briefing material prepared for the Panel and to their meeting agendas. I was also able to review Canadian government documents as well as foreign government publications and publications from Canadian and foreign non-governmental organizations. There was also a review of Canadian and foreign media articles reporting on election interference, and measures adopted to combat it.

Structure of this report

Section 1 will describe the problems the Protocol is intended to address. First, it will describe the issue of election interference. It will then focus on the specific problem of foreign interference, which was the principal preoccupation of the government when the Protocol and other measures were put into place in 2019. It will go on to describe how concerns with election interference evolved to include concerns about the role played by domestic actors, without any necessary connection to foreign states or entities. Following this, the report will focus on a specific aspect of the problem*:* how to handle election interference after an election is called, when the government is supposed to act with restraint.

The Protocol is one element of an integrated approach to addressing election interference. Understanding how it fits into this broader set of measures is important. Therefore, Section 2 briefly describes the entire suite of measures that have been put into place.

Section 3 will address the implementation of the Protocol. It will examine the following aspects:

A) Pre-election communications
B) Scope of application of the Protocol
C) Issues concerning the composition and role of the Panel
D) Continuity of Panel members
E) Consensus rule and quorum
F) Support to the Panel
G) Role of the National Security Agencies
H) Determining whether the threshold has been met
I) Should there be public notification below the threshold?

Section 4 will discuss the views of political party representatives on the Protocol as well as several other issues raised by them.

Section 5 will provide an overall assessment of the Protocol.

Section 6 will contain a summary of recommendations.

Section 1: Problems the Protocol is intended to address

The Protocol addresses two problems: First, it is one of a series of measures aimed at the problem of election interference. Second, it is specifically directed at the problem of addressing interference during the caretaker period.

A. The issue of election interference

Section 1.0 of the 2021 Protocol states that "national security threat and risk assessments, along with the experience of key international allies, underscore that Canada's general elections may be vulnerable to interference in a number of areas".

The term "interference" is not defined in the Protocol. It is generally understood to mean involving oneself in a situation where one's involvement is not wanted or is not helpful.

An important element of the problem of interference in democratic processes is that the information ecosystem has fractured and there is no longer a commitment to a common factual understanding. A growing number of people get their information from outlets that simply reaffirm their beliefs and are distrustful of opposing views. [3] There is greater receptiveness to false narratives attacking Canadian institutions. They are resistant to attempts by government, media, social media or civil society to correct or suppress false information.

Those engaged in activities intended to interfere with democratic processes, including elections, may have short-term as well as medium to long-term objectives. [4]

Short-term goals may include:

- shaping narratives around strategic interests;
- amplifying false or polarizing discourse;
- burying legitimate information;
- covertly influencing election outcomes in favour of a preferred candidate or party;
- suppressing voter participation;
- distracting voters from important election issues; and
- reducing public confidence in the outcome of an electoral process.

[3] Aengus Bridgman et al., "Mis- and Disinformation During the 2021 Canadian Federal Election". (68).

[4] Canadian Security Intelligence Service. (2021 July). Foreign Interference Threats to Canada's Democratic Process. and Canadian Security Establishment. (2021 July Update). Cyber Threats to Canada's Democratic Process. Although the CSIS publication was describing the objectives of foreign interference, many of them are applicable to domestic malign actors as well. The CSE publication was describing the effects of cyber activities on democratic processes. However, many of the activities it describes are relevant whether carried out by cyber or analogue means.

Mid-term and long-term goals may include:

- reducing the public's trust in the democratic process;
- increasing polarization and decreasing social cohesion;
- weakening confidence in leaders;
- lowering trust in journalism or the media;
- promoting the strategic interests of foreign states; and
- creating divisions in international alliances.

Professor Lisa Young has described a taxonomy of threats to election campaigns, which is reproduced in the table below.[5] She uses two variables to categorize these threats. The first is the identity of the actors, who can be domestic, foreign or instrumental foreign. This latter group is intended to describe a domestic perpetrator and beneficiary, using foreign means such as an offshore server to disguise their identity. The second variable is whether the threats are being carried out using analogue or digital means.

[5] Lisa Young, Canada's Response to the Cyber-Security threats to Elections; in Cyber Threats to Canadian Democracy. (31-54). Reproduced with permission.

Table 2.1: Taxonomy of threats to electoral campaigns (Young 39)

	Analog	**Digital**
Domestic (perpetrator and beneficiary) Harm = Loss of public confidence in electoral process	Domestic actors intervening in election campaigns using traditional media, such as newspapers, television, or radio. Examples include: • illegal or unreported election spending • vote fraud • threats against or intimidation of voters • disinformation spread through leaflets, posters, or word of mouth	Domestic actors intervening in election campaigns through digital means. Examples include: • amplifying or suppressing messages on social media • digitally spreading "high velocity" disinformation • hacking party or candidate computers • distributing damaging material, or delivering digital threats or intimidating voters
Instrumental Foreign (domestic perpetrator and beneficiary, using foreign means) Harm = Loss of public confidence in electoral process; evasion of election laws by domestic actors		Domestic actor intervening in election campaigns through digital means, using foreign intermediaries or servers to avoid detection or prosecution; same examples as above
Foreign (foreign perpetrator and beneficiary) Harm = Loss of sovereignty; loss of public confidence in electoral process	Foreign actors intervening in elections through analog means. Examples include: • making illegal foreign-sourced campaign contributions or third-party spending • threatening or intimidating voters directly or through family members outside the country • agents of a foreign state/entity running for office	Foreign actors intervening in election campaigns through digital means. Examples include: • amplifying or suppressing messages on social media • spreading "high velocity" disinformation digitally • hacking party or candidate computers and distributing damaging material • delivering digital threats or intimidating voters

i. Foreign interference

When the Protocol was first announced in 2019, the major concern was with foreign interference. This was made explicit in section 1.0 of the 2019 Protocol, which stated that: "Canada's 2019 general election may be vulnerable to foreign interference in a number of areas".

There had been well documented attempts at foreign interference in recent elections in the United States, United Kingdom, France and Germany, and in the Brexit referendum, for example. Over the past decade, there have been instances of interference that affected nearly 40 countries, Canada among them.

In the context of Canadian elections, the objective of foreign interference is to affect electoral outcomes or undermine public confidence in Canadian democratic institutions or both.

Foreign interference is different from normal diplomatic activity which is overt and an accepted part of diplomacy. Interference can be carried out by foreign states or persons acting on their behalf, including Canadians. It can also be carried out by non-state actors. These may be closely aligned with hostile governments, or they may be non-state actors from friendly jurisdictions.[6] Given the clandestine and deceptive nature of the activities, it is often not possible to determine whether a malign actor is working on behalf of a foreign state.

Foreign interference involves:

- Activities with or relating to Canada;
- These activities are detrimental to the interests of Canada; and
- The activities are deceptive or clandestine in nature or involve a threat to any person.

Foreign interference is considered an incursion into national sovereignty.

The 2019 Annual Report from the National Security and Intelligence Committee of Parliamentarians (NSICOP) contained a chapter addressing the threat of foreign interference.[7] The Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) both released reports on foreign interference in July 2021. CSIS stated that it "continues to observe steady, and in some cases increasing, foreign interference activity by state actors". CSIS was of the view that these activities will almost certainly intensify.[8]

[6] James Judd, Report on the Assessment of the Critical Election Incident Public Protocol (2020 May). Provided an example of friendly foreign actors, fake news sites, single issue groups or chaos promoters.

[7] NSICOP (2020 March); National Security and Intelligence Committee of Parliamentarians Annual Report (2019) (56-109).

[8] CSIS (2021 July). Foreign Interference Threats to Canada's Democratic Process. (3).

CSE assessed that "changes made around the world in response to the COVID-19 pandemic, such as moving parts of the democratic process online or incorporating new technology into the voting process, almost certainly increase the cyber threat surface of democratic processes. Most significantly, threat actors can harness and amplify false narratives related to the COVID-19 pandemic to decrease confidence in elections".[9]

CSE, in its 2021 report, found that between 2015 and 2020, cyber threat activity was targeted at voters more than at political parties or elections. CSE assessed that the Canadian democratic process remains a lower priority target for state sponsored cyber activities relative to other countries. However, they considered it very likely that Canadian voters would encounter some form of foreign cyber interference ahead of and during the 2021 federal election.[10]

During the course of the election, SITE provided the Panel the following information:

- RRM Canada did not observe any significant indicators of foreign state-sponsored information manipulation in its monitoring of the broader Canadian digital information ecosystem during the period of September 9.

- RRM Canada assesses the majority of English and French-language content originated from recognizable Canadian news sites.

- A Global Times editorial commented on the Conservative Party of Canada's (CPC) platform in an article titled: "A campaign platform that "almost wants to break diplomatic relations with China"! Is the US about to get another loyal dog?" The title in part quotes an 8 September Hill Times article which in turn quoted a Canadian columnist; the Hill Times article and statements by the columnist also featured in two Global Times articles yesterday. Today's editorial notes that if "the CPC comes to power, its policy is likely to be more hard-line and arbitrary compared to Trudeau's", that "it is not likely to sever diplomatic relations" but would likely "cooperate more actively with the U.S. to contain China at all levels." The editorial does not urge Canadians of Chinese heritage to vote for a particular candidate or party.

- Today Commercial News, a Chinese-Canadian newspaper that publishes the People's Daily overseas edition in Canada, posted a WeChat story that claims bill C-282, introduced by the CPC's Kenny Chiu, would require "all individuals or groups with ties to China" to register as agents of the Chinese government. The story urges users to "spread the word" about Chiu's bill that "suppresses the Chinese community." In a recent article in Business Intelligence Vancouver, Chiu had claimed misinformation was circulating on WeChat with respect to this bill. RRM Canada notes that bill C-282 calls for a foreign influence registry requiring individuals lobbying the Canadian government on behalf of a foreign government to register publicly.

[9] CSE (2021 July Update) Cyber Threats to Canada's Democratic Process. (13).

[10] CSE (2021 July Update) Cyber Threats to Canada's Democratic Process. (31).

- [***]
- [***]
- [***]
- [***]
- Over the course of the writ period, SITE Task Force saw no evidence to indicate that foreign state actors were specifically targeting Elections Canada (EC) or Canadian electoral systems and networks.

The House of Commons Standing Committee on Procedure and House Affairs has undertaken a study on foreign election interference. On November 1, 2022, Michelle Tessier, Deputy Director of Operations, CSIS and Alia Tayyeb, Deputy Chief of Signals Intelligence, CSE, appeared before the committee. They offered the following observations about foreign interference in Canada's elections:

- Misinformation, disinformation and malinformation propagated by state-sponsored cyber threat actors represent an ongoing persistent threat. CSIS is of the view that the activities of foreign state actors to influence elections are increasing.
- From 2015 to 2021, cyber activities were mainly attributed to state actors, especially Russia, China and Iran.
- In 2019 and 2021, the Panel, as part of the Protocol, determined that the government of Canada did not detect foreign interference that threatened Canada's ability to have free and fair elections.
- However, the national security agencies saw attempts at foreign interference, but not enough to have met the threshold of impacting electoral integrity.
- Social media is a very large source of the problem but it is not exclusive to social media. CSIS is concerned about the use of all types of media by hostile state actors as a tool for foreign interference.
- There are online platforms hosted in other countries with whom CSE does not have relationships. These are the ones CSE is looking at to determine whether foreign governments are using platforms to disseminate information in Canada.
- During the COVID pandemic, CSIS saw interest by foreign state actors to spread disinformation.
- CSIS is concerned about foreign interference, including by the Communist Party of China.

- CSIS expressed concerns that China notably tried to target elected officials to promote their national interests and encouraged individuals to act as proxies on their behalf.

- CSIS stated that China uses many techniques including threats to the Chinese community in Canada. However, the use of proxy agents makes it difficult to know that China is behind it.

Foreign interference raises several challenges. The first is that it is often difficult to determine whether incidents were coordinated and involved inauthentic amplification through the use of proxies, or whether they are honestly held views of Canadians who may have legitimate interests in supporting good relations with a foreign state. We need to understand better how foreign state actors influence and interfere with the information provided to Canadians, particularly through social media. This is necessary to enable better judgments on state directed interference.

Second, the high threshold to be met in order to notify the public underscores the importance of not being overly reliant on public notification as the main instrument for countering foreign interference. There is a need for ongoing investment in defensive measures like building public and media awareness and strengthening cyber defences.

Third, there should be an analysis of whether our legislative and regulatory tools to address foreign interference need to be updated. For example, there has been much commentary on the need to modernize the *CSIS Act*. There have also been calls for legislation to establish a foreign influence registry to require public disclosure of the activities of agents acting on behalf of a foreign principal or government.

Fourth, the motivation to interfere will vary over time. Motivation may be higher when a foreign state considers that its interests are threatened by a particular party or policy. Understanding these areas of interest, which will be different for each state, is important in developing strategies to counter interference and build public resilience.

Fifth, members of diaspora communities may be vulnerable to being targeted by foreign state actors. There needs to be a better understanding of their relationships to their countries of origin. At the same time, there are risks that concerns about foreign interference from a particular country can result in resentment and backlash against members of these communities, whose loyalty to Canada is unjustly impugned. Strategies to counter foreign interference need to guard against marginalizing diaspora communities.

Sixth, several of the activities attributed to China, like targeting elected officials to promote Chinese state interests, encouraging individuals to act as proxies and threatening members of the Chinese community in Canada, are not restricted in time to election campaigns. Nor are they restricted in scope to attempting to influence election outcomes. Confronting these require strategies that operate on an ongoing basis.

ii. Emerging concerns about domestic interference

Two changes were made to the Protocol in 2021 to reflect the changing nature of election interference. Whereas section 1.0 of the 2019 Protocol had identified the problem as vulnerability to foreign interference, the 2021 revision removed the word "foreign".

Second, section 6.0 of the 2021 Protocol clearly states that interference may emanate from a domestic or foreign source. The language used in the 2019 version had been more ambiguous, as to whether domestic actors were a problem unless they were acting on behalf of foreign interests. The government understood much of the disinformation around the legitimacy of the 2020 United States (U.S.) election had come from domestic sources. There were concerns that Canada could face a similar problem.

The government was also mindful that the next election could well take place in the middle of a pandemic. The government's approach to managing the pandemic was likely to be an election issue. There was a large amount of misinformation circulating about vaccine requirements and other public health measures, much of it being spread by domestic actors. There was also significant resistance to these measures.

Elections Canada was projecting an unprecedented number of mail-in ballots and possible delays in declaring results. The uncertainty engendered by the pandemic created opportunities for malign actors to use social media to make claims of voter fraud.

Another emerging factor was the growing threat of violence during the election campaign. This was driven, in part, by opposition to COVID-19 restrictions. Concerns about violence were also linked to the proliferation of extremist, racist and anti-government views that proliferated online and in some cable television outlets.

The 2021 election saw a surge in violent discourse, online anti-government behaviour, and threatening messages.[11] The national security agencies and the political parties were both concerned about a significant increase in the number of threats made against party leaders, candidates, and election officials. There were several threats and actual incidents of violence.

There are a number of issues to be considered as a result of the increased emphasis on domestic actors. First, prior to the calling of the 2021 election, there had been no public communications plan about the government's approach to protecting the integrity of the election. This could have offered a clear rationale for the increased focus on domestic actors. The Directive itself does not offer an explanation for this change. In future, a communications plan should set out a clear explanation for the focus on domestic interference and the types of activities that are of concern.

[11] Alex Boutilier, "Extremists Saw 2021 Federal Election as an 'Opportunity' to Plan Violence: CSIS." Global News, (May 2022).

Recommendation one

Public communication about the Protocol should provide a clear explanation for the inclusion of domestic actors and of the types of activities that are of concern.

Second, although threats or acts of violence can certainly interfere with campaign events, they may affect physical safety. Therefore, protecting the safety of the public, candidates, and election officials must be a priority. Intelligence and information gathering resources need to be deployed to identify these physical threats.

Recommendation two

Preparations for the next election should include an assessment of whether ministerial security, Royal Canadian Mounted Police protective policing, and local policing capabilities are adequate for the level and persistence of threats and whether there is effective coordination among these bodies. There should also be a review of the coordination between political parties and the government with respect to campaign and security operations.

Third, the inclusion of domestic actors raises political sensitivities around government monitoring the online activities of Canadians. There are clear legal parameters to protect the *Canadian Charter of Rights and Freedoms* (the *Charter*) and privacy rights and review bodies as well as the courts to hold government actors accountable. This is an area where other actors, social media platforms, traditional media and civil society have an important role to play. In a report to the French government issued in 2018, one of the recommendations was to emphasize the important role of civil society in protecting against information manipulation.

"Avoiding heavy handedness: Society (journalists, the media, online platforms, NGOs, experts and academics) must remain the first line of defence against information manipulation in liberal democratic societies. The most important recommendation for governments is to retain as light a footprint as possible – for the sake of their values but also out of concern for effectiveness".[12]

While this applies to all efforts at manipulation, it has particular resonance for dealing with malign domestic actors.

Fourth, as concerns about the role of malign domestic actors grows in the U.S. and other countries, it will be important to share information about changing tactics and strategies being deployed in other countries.

Fifth, although the 2021 Protocol has clarified that domestic interference is a problem in and of itself, it will be important not to ignore foreign states acting through domestic actors. Foreign actors can exploit the free speech protections possessed by Canadians to sow disinformation. This is an area that can benefit from research to better understand these relationships.

[12] Jean Baptiste Jeangene Vilmer, "Effective State Practices against Disinformation: Four Country Case Studies." The European Centre of Excellence for Countering Hybrid Threats, Hybrid COE, (2022 March) (25).

Finally, the organizational machinery, specific to the Security and Intelligence Threats to Election Task Force (SITE), was put in place in 2019 to address election interference largely focused on foreign interference. Does this organizational structure need to be modified to reflect the evolving nature of the challenge?

Recommendation three

There should be an assessment as to whether any adjustments should be made to the role of the SITE membership in light of the growing problem of domestic interference.

B. Addressing interference after the election is called

As James Judd noted in his report on the evaluation of the 2019 Protocol:

"In essence the creation of the Protocol and its Panel was intended to avoid a situation such as occurred in the 2016 U.S. elections. There was a significant degree of foreign interference in the election that was not made known to voters before the election occurred. It was not made public for fear that such a revelation might be construed as having been done for partisan reasons". [13]

The Canadian Government sought a credible mechanism to alert the public of an incident or incidents that jeopardize a free and fair election, and to do so in a manner that would not result in the government being perceived as interfering with the election for partisan purposes. The approach taken was grounded in the Caretaker Convention.

This convention puts into practice the principle that government is expected to exercise restraint in its activities and restrict itself in matters of policy, spending and appointments during the election period, except where action is urgent and in the national interest. The Caretaker Convention does not preclude public communications by the government that are intended to protect public health and safety. For example, during the election campaign, there were regular written updates about COVID-19 from the Chief Public Health Officer (CPHO). It would be consistent with the Caretaker Convention for the CPHO to issue a statement correcting false information about COVID-19 health measures.

One consequence of restraint is that, during this period, announcements that must proceed are to be made in the name of the department to ensure a distinction between official business and partisan activity.

Section 2.0 of the Protocol states that the Caretaker Convention typically begins on the dissolution of Parliament and ends when a new government is sworn in or a result returning an incumbent government is clear. The Protocol only operates during the caretaker period. [14]

[13] James Judd, Report on the Assessment of the Critical Election Incident Public Protocol (2020 May).

[14] Protocol at section 2.0.

Consistent with the Caretaker Convention, the Protocol was grounded in the view that any announcement during an election campaign that could have an impact on that election should come from a non-partisan source. In Canada, that non-partisan source is the Panel of senior deputy ministers.

Section 2: The Protocol as one element of an integrated approach

The Protocol is only one element in a much larger set of measures aimed at addressing election interference. The complexity of the challenge calls for a multifaceted approach involving several interconnected initiatives. This has been referred to as an "electoral ecosystem approach".

An electoral ecosystem approach has been described in the following terms:

"Under an electoral ecosystem approach, the electoral system is viewed as an interconnected network of institutions, processes, and actors, all of which must coordinate together to ensure electoral effectiveness and legitimacy. An electoral ecosystem is comprised of multiple institutions and actors, including governments, political parties, voters, online platforms, and electoral management bodies. Given the interdependence and interconnected nature of an election system, there are multiple points of vulnerability that must be defended. An electoral ecosystem approach does not depend on any one single line of defence but instead relies on a multiplicity of strategies that protect the institutions and individuals that comprise the ecosystem."[15]

In January 2019, the Government of Canada announced the Plan to Protect Canadian Democracy (the Plan), which adopted this integrated approach. The Plan was updated and renewed before the 2021 election.

The Plan has four pillars:

- Enhancing citizen preparedness;
- Improving organizational readiness;
- Combatting foreign interference; and
- Building a healthy information ecosystem.

A. Enhancing citizen preparedness

The aim is to educate citizens to understand the constantly changing tactics used by malicious actors online to manipulate opinions. The Protocol is one of the initiatives under this heading. Another is the Digital Citizen Initiative led by Canadian Heritage. Its objective is to support skills development through the use of awareness sessions, workshops and learning materials.

Citizen preparedness was also supported by the government's Get Cyber Safe public awareness campaign about internet security, which added content about cyber threats to Canada's democratic processes.

Prior to the 2019 election, the government had provided journalists with training on foreign interference and convened regular press briefings. This did not occur in advance of the 2021 election.

[15] Yasmin Dawood, Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats, 20 Election Law Journal, (2021 March).

There were also changes to Canada's election laws that expanded the CEO information and education programs aimed at the Canadian public.

B. Improving organizational readiness

Government departments and agencies were briefed on how to identify threats, emerging tactics and systems vulnerabilities in order to strengthen security practices and behaviours. Political parties and election administrators were provided with technical advice to help them better protect their own cyber systems. Political party representatives were also provided with classified briefings on threats.

Organizational readiness had also been reinforced in 2018 with the establishment of the Canadian Centre for Cyber Security (CCCS), with a budget of $155 million over five years.[16] CCCS is responsible for monitoring threats, protecting national critical infrastructure against cyber incidents, and coordinating the national response to any incidents related to cyber security.

C. Combatting foreign interference

There are two key institutional initiatives that were put into place. The first is the establishment of the Security and Intelligence Threats to Election (SITE) Task Force.

SITE is a coordinating body comprised of the CSE, the CSIS, the Royal Canadian Mounted Police (RCMP) and the Rapid Response Mechanism (RRM) housed in Global Affairs.[17] SITE is tasked with building awareness of threats to Canada's federal election processes and preparing the government to assess and respond to those threats.

Each agency leverages its mandate to bring to the table unique information on threats to Canadian security in order to effectively share intelligence, contextualize the threats based on information received through a range of partnerships, and review together any potential actions to mitigate threats directed at Canadian federal elections. SITE supports the Panel by providing them with up-to-date intelligence and information.[18]

---

[16] Canadian Centre for Cyber Security.

[17] Government of Canada Backgrounder on Combatting Foreign Interference
CSE's role is to protect government systems and networks, as well as offering cyber advice to Elections Canada and political parties. CSIS actively monitors and reports threats to the government and provides classified briefings to political parties on potential threats. The RCMP detects and disrupts attempted foreign interference activity and investigates criminal activity related to interfering or attempting to influence Canada's electoral processes.

[18] SITE is one element of a structure that supports information sharing and coordinates action about election interference. This structure has four components:
1.The Panel of Deputy Ministers
2.The SITE Task Force

SITE has met regularly since 2019. They now meet on a monthly basis. The rate of meetings accelerates as the election gets closer. During the 2021 election, SITE met on a daily basis.

The second initiative was the RRM. The RRM is an initiative that was announced at the G7 Summit in Charlevoix, Quebec in 2018. Its purpose is to strengthen coordination across the G7 in identifying, preventing and responding to threats to G7 democracies.

In the context of Canadian general elections, RRM Canada serves as a member of the SITE Task Force. It leverages its G7 RRM network to share with other SITE agencies lessons learned from interference attempts in other countries' elections as well as strategies used to combat them. It also serves as an early warning system by using open data analytics to monitor for foreign state-sponsored inauthentic or coordinated information manipulation activity in the online environment targeting Canada. RRM supports SITE in providing regular briefings to the Panel of deputy ministers.[19]

Canada's ability to counter interference in Canada's democratic processes had been bolstered in 2019 with the coming into force of Bill C-59, An Act respecting National Security Matters. This legislation provided both CSIS and CSE with the ability to engage in threat reduction measures (TRMs), subject to legal authorization.[20]

Canada's election laws have been modified to more effectively counter foreign interference. The *Elections Modernization Act*, (Bill C-76), came into force in June 2019. This legislation prohibits a foreign person or entity from unduly influencing an elector to vote or refrain from voting, or to vote or refrain from voting for a particular candidate or registered party. It prohibits third parties from using foreign funds for partisan advertising and activities, and prohibits foreign entities from spending on partisan advertising and activities during both the pre-election and election periods. It also requires online platforms to publish a registry of partisan advertising published during the pre-election period and all election advertising during the election period. Finally, there is a provision that prohibits knowingly making or publishing a false statement to affect election results.

3.The Election Security Coordinating Committees. These are the series of committees composed of Senior officials and co-chaired by Elections Canada and the Privy Council Office. Participants include Elections Canada, the Privy Council Office, representatives of the SITE agencies, Public Safety Canada, Health Canada and the Public Health Agency of Canada (PHAC). Their role is to maintain situational awareness on security issues, including pandemic related issues, election plans and operations.
4. Engagement with political parties. The objective is to improve the parties' organizational readiness by providing classified threat briefings, sensitizing them to the nature of interference and disinformation practises and provide advice on keeping their online systems safe.

[19] Rapid Response Mechanism Canada, Global Affairs Canada.

[20] Leah West, Defending Democracy from Foreign Cyber-Interference, in Cyber Threats to Canadian Democracy (2021). (70-76). For a discussion of the use of threat reduction measures, see section 3, part G of this report. There is a more fulsome exploration of the issues around TRMs and their relationship to the Protocol.

When the government unveiled its Plan to Protect Canadian Democracy, one of the measures it announced under the heading of combatting foreign interference, was the need to work with external partners in Canada and globally, from academia, industry, and civil society, to support information integrity during elections. These external partners play several important roles. They have perspectives on the evolving threat environment that may differ from those of the national security agencies. They have a public education role. They can also alert the public to attempts at interference both before and during the campaign.

There were a number of comments in the interviews conducted for this report emphasizing the importance of working with these external partners and that encouraged the government to provide adequate, predictable and ongoing funding in order for them to perform these roles effectively.

D. Building a healthy information ecosystem

A large and growing number of Canadians are relying on social media as a source of political information. This creates a growing danger that people will mostly be exposed to information that reinforces their existing views and filters out other perspectives.[21] The use of social media platforms as a source of false election-related information has been well documented.

Discussions between the government and the social media companies resulted in the Canada Declaration on Election Integrity Online (the Declaration), which sets out commitments by online platforms and the Government of Canada to safeguard elections from malicious interference and create a healthier online ecosystem. For example, pursuant to the Declaration, platforms commit to work to remove malicious abuses of platforms, such as fake accounts, coordinated inauthentic behaviour, and malicious automated accounts. The 2021 Declaration was endorsed by Facebook, Google, LinkedIn, Microsoft, TikTok, Twitter and YouTube. The Declaration was first implemented in 2019. It was updated prior to the 2021 election.[22]
The Declaration is a positive development, but the problem of the use of social media platforms to sow disinformation persists.

The Canadian Election Misinformation Project did an analysis of the role of social media platforms in spreading false information. They found that, notwithstanding more assertive moderation and election integrity policies, large social media platforms continued to be home to widespread misinformation. Moreover, users are finding ways to evade moderation through the use of a variety of strategies. These include the use of coded language, like intentional spelling mistakes, private and closed groups, multiple accounts and choosing to reduce their reach by omitting hashtags. Groups that are concerned by what they consider to be moderation overreach

[21] Aengus Bridgman et al., Mis- and Disinformation During the 2021 Canadian Federal Election.(68).

[22] Government of Canada News Release on Electoral Integrity Online;
The Government of Canada updates the Canada Declaration on Electoral Integrity Online.

and collusion between tech companies and the government have migrated their political speech to smaller social media platforms with less moderation.[23]

It should be noted that there have been changes made to elements of the Plan. The next section of this report will describe changes made to the Protocol. The Declaration was amended in 2021. The Government's 2022 Budget contains several measures aimed at combatting misinformation and disinformation, including resources to renew and expand the RRM, ongoing cyber activities to protect against disinformation as well as a commitment to support research at public institutions. There are also resources provided to the Privy Council Office (PCO) to coordinate, develop and implement government wide measures designed to combat disinformation and protect Canadian democracy. [24]

Election interference and the broader problem of efforts to undermine democratic institutions continue to evolve. Purveyors of disinformation continue to innovate and adapt in order to circumvent measures taken by governments and social media platforms. [25] There is also significant adaptation by governments across the democratic world with respect to all aspects of this challenge. It will be important for democratic countries to share best practices. It will also be important for the government to regularly review all elements of its integrated approach to ensure that it continues to be responsive to the problem.

[23] Aengus Bridgman et al., "Mis- and Disinformation During the 2021 Canadian Federal Election." (28-32).

[24] Government of Canada, Department of Finance. "Chapter 5: Canada's Leadership in the World: Budget 2022." Chapter 5: Canada's Leadership in the World, Budget 2022, Government of Canada, (2022 April).

[25] Steven Lee Myers, Russia Reactivates Its Trolls and Bots Ahead of Tuesday's Midterms, New York Times, (2022 November).

Section 3: Implementation of the Protocol

The Protocol underwent an independent review following the 2019 General Election. It was slightly modified in 2021, based on the independent review and as a result of internal deliberations within the government.

The key changes were as follows:

1. Removal of a reference to a specific general election to make the Protocol applicable in all future general elections, until or unless replaced or repealed by Cabinet.

2. Alignment of the Protocol's application with that of the Caretaker Convention.

3. Explicit provision for the Panel to consult with the Chief Electoral Officer, as appropriate.

4. Provision for the ability of political parties to alert security agencies of incidents that could threaten a free and fair election.

5. Recognition of the Panel's ability to examine domestically driven interference.

6. Recognition of the Panel's ability to receive information from sources other than the security agencies, at its discretion.

7. Independent review of the Protocol no longer includes an assessment as to whether to establish the Protocol on a permanent basis.

A. Pre-election communications about the Protocol and Panel

James Judd, in his report on the 2019 Protocol, said the following about the government's communications approach prior to the 2019 general election:

"The Protocol and the Panel's institutional makeup had first been made public nearly nine months before the election occurred.

Senior government officials gave detailed and candid briefings of the national media on the Protocol and the Panel on two occasions – the first at the time of the Ministerial announcement on them, the second in July 2019 when the Cabinet Directive was published. The latter was focused exclusively on the Protocol and Panel, providing a good assessment of the challenges and, no less, the activities of the Panel to that date. In both instances questions from the media were responded to as fully as possible.

Subsequent to that July briefing the PCO's Communications Secretariat and other government organizations regularly responded to media inquiries on the work of the Panel".[26]

[26] James Judd, Report on the Assessment of the Critical Election Incident Public Protocol. (2020 May) (13).

By way of comparison, in 2021, there was a minority government and an uncertain election date. There was no public communication about the extensive measures that were in place, including the Protocol, until the election was called. At that time, the Cabinet Directive was posted on the PCO-Democratic Institutions website. The absence of a robust, timely communications strategy led to criticism from the media, from academics and from politicians about what appeared to be the government's lack of action to safeguard the election.

An early, fulsome communications approach explaining the role of the Panel would have been helpful in reinforcing the legitimacy of its role. The fact that there was no prepositioning would have made it more difficult for the public to understand why a group of unelected officials were telling the country that their election was being undermined, should an announcement have been necessary.

It would be desirable, in future, to emulate the communications approach taken in advance of the 2019 election. An initial announcement should take place reasonably early in the government's mandate. This is especially important in a minority government situation when waiting too long to make the announcement would risk setting off speculation about an imminent election call.

The announcement could explain concerns about threats to democratic institutions, including elections. It would remind the public about all of the measures being taken. These would include the Protocol and the role of the Panel. It could explain that although the Panel would not become operational until an election was called, that Panel members would be meeting periodically throughout the mandate to be briefed on the evolving threat environment. Once the election was called, there could be another announcement reminding the public of the measures in place and explaining that the Protocol is operational throughout the caretaker period.

Recommendation four

There should be an announcement, within a year of the previous election, about the government's plan to safeguard the integrity of Canada's elections, including an explanation of the reason for the Protocol.

B. Scope of application

Section 3.0 describes the limited mandate of the Protocol. There is a temporal limitation. The Protocol will only be initiated to respond to incidents that occur during the caretaker period. Outside that time frame, incidents are to be addressed through regular government channels.

There is also a jurisdictional limitation. It will not respond to incidents that fall under the responsibilities of Elections Canada with regard to the administration of the election, as identified in the *Canada Elections Act*. For example, an attempt to mislead voters as to the time or place they can vote would be within the purview of Elections Canada to deal with.[27] By

[27] The report of the Chief Electoral Officer on the 2021 general election highlighted the steps taken by Elections Canada to address mis- or disinformation:

contrast, covert attempts by a foreign entity to, for example, spread false accusations about the private life of a party leader or to misrepresent the policy position of a political party would fall under the Protocol. However, the incident would still be required to meet the threshold for informing the public set out in section 6.0, for it to result in a public announcement.

There appears to be a general agreement that this division of responsibility works well. The Protocol did anticipate that there may be issues of interference that are possibly relevant to both the CEO and the Panel. For example, if the CEO himself is a target of a disinformation campaign claiming a conflict of interest. In such cases the Protocol provides that the Panel may consult with the CEO. (Section 5.4). I am not aware of any such issues arising during the 2021 election campaign.[28]

There is a concern with the limitation of the Protocol to incidents occurring during the caretaker period. As James Judd pointed out in the review of the 2019 Protocol, it is unlikely that any potential foreign interference would be confined to the writ period alone. The Judd report recommended changing the operational timeframe of the Protocol to include both the writ and the pre-writ periods. This would allow the revelation of any interference to be made by a non-partisan body, thereby diminishing the possibility that the government might be accused of using national security for partisan advantage.

This recommendation was not accepted by the government. According to those interviewed within government, it was felt that the normal principle of ministerial responsibility should apply outside the caretaker period.

While James Judd's recommendation was not adopted, the problem he identified is real. False information about parties, candidates, or leaders can be spread well in advance of the campaign. Cyber attacks on political parties can occur before the election is called. Covert attempts by foreign actors to secure the nomination of candidates who might be favourable to foreign interests would occur in the months leading up to an election.

The government's integrated plan described above is not clear on how pre-election attempts at interference will be addressed. It would be helpful if the government's plan and public communication expressly acknowledged the problem of interference activity before the election

---

> "Elections Canada's engagement with electors on social media platforms increased considerably during the 44th general election. This coincided with an improvement in the agency's ability to monitor certain election related topics in the public environment and to address potential mis- or disinformation that could affect electors' ability to vote. The agency created its Environmental Monitoring Centre in 2020, enabling it to deepen its understanding of the information environment and observe inaccurate narratives as they developed, before and during the general election. This in turn allowed Elections Canada to pre-emptively develop messaging for all its channels and share them with its followers, and to quickly craft reactive messages to respond to inaccurate information. These efforts, along with the agencies outreach and stakeholder mobilization initiatives, served to reaffirm Elections Canada as the official source of information on the federal democratic process."

[28] There was engagement with the CEO and the Commissioner of Canada Elections to ensure that there was a clear understanding of respective roles.

is called. It should also provide some detail on how this is intended to be addressed, beyond simply saying that it will be handled through normal ministerial channels.

Recommendation five

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. It should be clearer on how and by whom pre-election interference will be addressed, beyond saying that it will be handled through normal ministerial channels.

C. Issues concerning the composition of the Panel

Section 4.0 explains the composition and role of the Panel. It identifies which civil servants are to compose the Panel. It is comprised of individuals holding the following positions:

The Clerk of the Privy Council;

The National Security and Intelligence Advisor to the Prime Minister;

The Deputy Minister of Justice and Deputy Attorney General;

The Deputy Minister of Public Safety; and

The Deputy Minister of Foreign Affairs.

As James Judd explained in the first review of the Protocol, these people were chosen due to the responsibilities of their offices/organizations.[29] The only member who was on the Panel for both the 2019 and 2021 elections was the then Deputy Minister of Foreign Affairs. In addition, the Deputy Minister of Justice during the 2019 election had taken on the role of Deputy Clerk of the Privy Council and she attended the 2021 Panel as an observer. All other members of the Panel were new.

[29] Report on the Assessment of the Critical Election Incident Public Protocol (2020) (21).

> "The Clerk of the Privy Council is the highest-ranking public servant in the federal government and has a specific responsibility in regard to the continuity of government. The National Security and Intelligence Advisor is the senior most official in the Canadian security and intelligence community, with a key role in coordinating the members of that community. The Deputy Minister of Justice and Deputy Attorney General is the senior officer and legal advisor to the Government and plays a critical challenge function, including on Charter related issues. The Deputy Minister of Foreign Affairs is the senior official in the domain of foreign policy and foreign relations, a role that was important here given the issue of possible foreign interference. The Deputy Minister of Public Safety is the most senior public servant in a department with responsibilities for cyber policy, the Royal Canadian Mounted Police, Canadian Security Intelligence Service, border security, corrections and emergencies."

The Panel is responsible for determining whether the threshold for informing Canadians set out in section 6.0 has been met. In order to make this determination, the Panel will work with the national security agencies within the agencies' existing mandates.

There was a range of comments about the composition of the Panel. Some comments were to the effect that a group of eminent Canadians would have more public credibility than a group of senior deputy ministers, should it become necessary to have an announcement that there are threats to Canada's ability to have a free and fair election.

However, a Panel composed of senior deputy ministers has several advantages. The composition of the Panel is based on their knowledge, experience and judgment and the working relationship among them. They are skilled at drawing out the expertise of the SITE agencies. They are also adept at assessing the information they receive and in challenging it, where necessary. Moreover, a group of eminent Canadians may be associated with interests or causes that may become election issues, raising questions as to their neutrality. Representatives of the three parties that chose to receive briefings during the last election all continue to support a Panel composed of senior public servants.[30]

There were a number of comments about adding other members to the Panel, including the CEO. There were also questions as to why the Public Health Agency of Canada (PHAC) was not represented on the Panel, given the amount of disinformation around COVID-19 and its implications for the management of the election.

In my view, the Protocol as written, is effective in enabling the Panel to have input from outside the national security agencies, as required. As previously noted, there is an explicit provision in section 5.4 that the Panel may consult with the CEO. Given that the Panel is not responsible for matters of election administration that fall under Elections Canada, I believe that the consultation provision is more appropriate than including the CEO on the Panel.

One of the changes made to the Protocol in 2021, at section 5.1, recognized that the Panel may receive information and advice from sources other than the national security agencies. The language is broad enough to encompass advice both from within and outside the government. During the 2021 election this advice would have been provided to the Panel via briefings from the Privy Council Office and from SITE. Information from PHAC about the pandemic was provided to the Panel as required, via the Election Security Committee Structure that PHAC was a part of. Section 5.1 is flexible enough to enable expertise relevant to any future event to be provided to the Panel.

D. Continuity of Panel members

Another concern is with continuity. Deputy Minister shuffles can occur late in a government's mandate and Panel incumbents may be moved to new positions or may retire. In June of 2021, the National Security and Intelligence Advisor to the Prime Minister retired. He was replaced by the Prime Minister's Foreign and Defense Policy Advisor at the Privy Council Office (PCO),

[30] The Bloc Quebecois and the Green Party chose not to participate in the briefings offered to political parties.

who took on the role of acting National Security and Intelligence Advisor to the Prime Minister (NSIA).

Where a Panel member remains in government, but in a different position, it may be possible that they attend meetings of the Panel, as an observer, as occurred with the former Deputy Minister of Justice who became the Deputy Clerk. This would maintain continuity and take advantage of the knowledge they have acquired. There should also be enough flexibility for those Panel members who have taken on other roles close to an election to remain as full members of the Panel.

It was also noted that the members of the Panel all have very demanding jobs, and many competing priorities for their attention. Yet, it is essential that these senior deputy ministers are supported in devoting the time needed to develop a nuanced understanding of the challenges of election interference. If the current composition of the Panel is to be effective, membership on the Panel should be described as a core responsibility of each of these positions. Briefings of new members should begin immediately after they assume their positions.

Recommendation six

It is recommended that the government consider options to ensure that the Panel is well-prepared in advance, and as much as possible, continuity of members is maintained between elections.

E. Consensus rule and quorum

Section 5.4 describes the process to be followed by the Panel in determining whether the threshold for informing the public has been met. It provides that the Panel will operate on a consensus basis. This is interpreted by the members of the Panel as requiring unanimity. This requirement reinforces the notion of restraint inherent in the Caretaker Convention and is consistent with the high bar to be overcome in order for the Panel to inform the public that Canada's ability to have a free and fair election is threatened.

During the 2021 caretaker period, two of the Panel members had to be out of the country on other business. While secure video conferencing is available in many locations, this may not always be the case. This raises the issue of quorum for any decision by the Panel to call for a public announcement.[31] The rule requiring consensus on a decision around determining whether the threshold has been met, effectively requires all members of the Panel to be involved. It should be clear that during the caretaker period, attending the Panel is the overarching priority for all Panel members. It is reasonable to either arrange for a substitute to attend to commitments out of Ottawa, or at least to ensure that there is a functioning secure video conference capability at their destination.

[31] For meetings where no decision was required, three Panel members in attendance were considered quorum.

F. Support to the Panel

i. Pre-election support

The Panel began meeting in May of 2021, around four months before the election. They met four times throughout May, June and July. They received briefings from the PCO Secretariats responsible for Democratic Institutions, for National Security and Intelligence, and for Communications. They also received briefings on the threat environment from the agencies that made up the SITE Task Force. [***] . The Panel reviewed the Cabinet Directive on the Protocol and their mandate. There were discussions about the information ecosystem and the roles and responsibilities of government agencies, Elections Canada, and the social media companies. There were also discussions about the changed context between 2019 and 2021, and notably with regard to the impact of COVID-19. The Panel also began working through scenarios to develop a common understanding of the threshold for their intervention.

Panel members were generally satisfied with the content of their pre-election briefings although there was a view that the process seemed somewhat rushed. There was agreement among the Panel members that Panel briefings should begin earlier in the mandate. Providing more time to be briefed is especially important for new members. In 2021, all of the Panel members were new, except for the Deputy Minister of Foreign Affairs. An earlier start would provide an opportunity to deepen their understanding of the changing threat environment, including information on interference efforts in elections in other democratic states and the measures those states took to counter these efforts.

An earlier start could also provide time for the Panel to be briefed by non-government actors with expertise on interference and disinformation. This would include civil society organizations and academic researchers, as well as social media platforms. This is an important part of the education of Panel members since they are likely to be exposed to different perspectives on the challenges than those received from the national security agencies. There was broad support, among the people I interviewed, that the Panel should have the opportunity to hear the perspectives of external experts in the months leading up to the election campaign.

Recommendation seven

Briefings of the Panel should begin much earlier in the mandate and include non-government actors with expertise on interference and disinformation.

ii. Support during the caretaker period

The 2021 election was called on August 15. From then until election day on September 20, the Panel held six weekly meetings. They were provided with threat briefings by SITE. The Panel had the opportunity to review and discuss numerous hypothetical scenarios to determine whether the threshold would be triggered. There was only one of these scenarios where there was a consensus of the Panel that the threshold for an announcement would be met.

The Panel was briefed by the SITE agencies on [***]. SITE provided updates throughout the election period [***]. SITE also provided the Panel with its initial observations shortly after Election Day, [***].

There were two parts to the Panel meetings. During the first part, the Panel would receive its briefings from representatives of the SITE group. This reflects the roles of the national security agencies, set out in section 5.1, to provide regular briefings to the Panel on emerging national security developments and potential threats to the integrity of the election.

During the second part, the Panel would meet without the national security agencies being present. In other words, the practice that evolved was to draw a clear distinction between that part of the meeting where the Panel received intelligence and other information about threats and the opportunity for the Panel members to deliberate on what they had heard.

The practice of two-part meetings reflected the different roles and responsibilities of the two groups. The Panel members were designated as the decision makers on whether a public announcement from them was warranted. SITE was tasked with providing information to the Panel but did not have the authority to decide.

Panel members were generally positive on the briefings they received from PCO and SITE during the election campaign. The approach taken by SITE was not to hold anything back, and to provide the Panel with anything they felt could be relevant to the election. It would be for the Panel to decide whether an incident or accumulation of incidents met the threshold.

G. Role of the national security agencies

The NSAs have a primary role in providing regular briefings to the Panel on emerging national security developments and potential threats to election integrity. As noted above, during the caretaker period, there were weekly opportunities for SITE to brief the Panel. The Panel also received daily written updates.

Section 5.3 describes the role of the NSAs when they become aware of interference in the General Election. Note that section 5.3 speaks of "interference" and not interference which necessarily meets the threshold. The NSAs are required to consult with each other and consider all options to effectively address the interference. They are required to inform the Panel.

Barring any overriding national security or public security reasons, the agencies will inform the affected party of the incident directly.[32] Affected parties could include a candidate, a political party or Elections Canada.

[32] An example of a national security reason not to inform an affected party could be if providing the information might lead to placing a confidential human source in danger.

What is the possible range of options available to the agencies? Section 5.3 only mentions that the agencies will inform the affected party of the incident directly. But there is a range of other possible actions. Both CSIS and CSE have the ability to take measures to disrupt threats to the security of Canada, including foreign influence. [33]

Where a measure does not infringe Charter rights, CSIS has an internal approval process, but does not require ministerial or court approval. An example of this type of measure would be a discussion with a foreign diplomat cautioning them about interfering in a Canadian election. Another example would be to notify social media platforms of accounts CSIS has identified as being fakes or bots spreading disinformation.[34]

However, if Charter rights would be interfered with, then an authorization from the Federal Court of Canada would be required and the Minister of Public Safety must approve the court application.[35]

These threat reduction powers were added to the *CSIS Act* by Bill C-59, which entered into force in 2019. To date, there has been no resort to the use of court authorized threat reduction measures.

However, Professor Leah West has noted an issue, should this power be used during the caretaker period:

"Importantly, before applying for a threat reduction warrant, the Director of CSIS or their delegate must obtain the approval of the Minister of Public Safety. This requirement means that an elected official could influence whether or not CSIS takes action to defend a rival political party or campaign from foreign influence. The opportunity for partisan politics, or even the perception of partisanship, to influence Canada's response to foreign interference is precisely the type of situation the government sought to avoid by establishing the CEIPP".[36]

Professor West suggests that this problem could be mitigated by amending the Protocol to require a record of any decision made by a minister on measures taken or not taken by CSIS to reduce threats during the caretaker period. Furthermore, this record should be subject to review by either the NSICOP or the National Security Review Agency (NSIRA).[37]

CSE has broad powers to protect both government cyber networks, as well as private networks designated by the Minister of National Defence as being of importance to the Government of Canada should the network owner request it. Furthermore, foreign cyber operations (FCO) are

[33] *CSIS Act* at s. 12.1, *CSE Act* at s.16.

[34] Leah West, Defending Democracy, *Cyber-Threats to Canadian Democracy* (2021). (71).

[35] *CSIS Act* s.21.1(1).

[36] Leah West, Defending Democracy, *Cyber-Threats to Canadian Democracy* (2021). (72).

[37] Leah West, Defending Democracy, *Cyber-Threats to Canadian Democracy* (2021). (72).

the newest aspect of CSE's mandate, dating back to the *CSE Act* in 2019. These authorities enable Canada to take action in cyberspace against foreign adversaries in matters relating to Canada's international affairs, defence or security, or to help protect the information infrastructures of federal institutions or infrastructures designated as being of importance to the Government of Canada.

Subdivided into defensive cyber operations (DCO) and active cyber operations (ACO), these authorities give Canada the option of acting on what CSE learns through our signals intelligence and cyber security mission.

Similar to the issue with CSIS, CSE requires a Ministerial Authorization to carry out any of the above noted activities. Each Authorization is valid for up to one year. While multiple foreign operations may be conducted under a single Authorization, there are also cases where an Authorization may be anticipatory, with no operations required in the end. The DCO Authorization to protect the Canadian federal election is an example of this. CSE has the capabilities and the legal mandate to disrupt malicious online activity that threatens Canada's democratic processes. In the lead up to Canada's 2021 federal election, CSE had defensive cyber operations authorities in place to protect the electronic infrastructure used by Elections Canada. Had there been malicious cyber activity targeting the election process, CSE would have been ready to act on it right away.

Professor West notes the same problem of providing ministers with the final say on whether CSE acts to defend a rival political party from foreign influence. In the case of CSE, unlike CSIS, this problem is mitigated by CSE's Ministerial Authorization process that authorizes activities for up to one year. It is possible for CSE to have authorization already in place, going into an election campaign, as it did in 2021, in order to disrupt malicious online activity that threatens Canada's democratic processes. As is the case for CSIS, Professor West recommends recording any decision by a minister to authorize measures against cyber-threats during the writ period and having these decisions reviewed by NSICOP or NSIRA.[38]

Recommendation eight

There should be an opportunity for a review body to assess the decisions of ministers with respect to the use of threat reduction measures during the caretaker period.

H: Determining whether the threshold has been met

Section 5.4 requires the Panel to evaluate incidents to determine if the threshold for informing the public, set out in section 6.0, has been met. The Panel operates on a consensus (unanimous basis) and may consult with experts across government and with the CEO. If a public announcement is deemed necessary, the Panel will inform the Prime Minister, the other party leaders or their designates and Elections Canada. A public statement informing Canadians of the incident can then be made. The Clerk of the Privy Council, on behalf of the Panel, may either

[38] Leah West, Defending Democracy, *Cyber-Threats to Canadian Democracy* (2021). (74).

issue a statement or ask the relevant agency head(s) to issue a statement to notify Canadians of the incident(s).

Section 7.0 provides that the announcement would focus on a notification of the incident, what is known about it and steps Canadians should take to protect themselves, if relevant.

Section 6.0 sets out the standard to be met for there to be a public announcement. The Panel would have to determine that an incident or an accumulation of incidents has occurred that threatens Canada's ability to have a free and fair election.

Perhaps the most important statement in section 6.0 is that determining whether the threshold is met will require considerable judgment. The legitimacy of the Panel is based on its non-partisan nature but also on the confidence in the judgment, perspectives, and experience of the Panel members.

As James Judd noted in the review of the 2019 Protocol:

"The threshold within the Protocol for any action by the Panel did not easily lend itself to the application of quantifiable metrics upon which to arrive at any decision. In the final analysis, determinations about the context of the interference were necessary [both the action and the potential impact upon the election campaign of any interference]".

Section 6.0 sets out a number of considerations that could be included in making this judgment:

- the degree to which the incident(s) undermine(s) Canadians' ability to have a free and fair election;
- the potential of the incident(s) to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence or information.

Section 6.0 contains a concluding paragraph which provides further elaboration of some of the challenges facing the Panel in making its determination as to whether the threshold has been met:

"A disruptive event or incidents of interference may emanate from domestic and or foreign actors. Attribution of interference attempts may be challenging or not possible within the timelines permitted by events, given that attempts to unduly influence the election may involve misdirection and disinformation. Further, it is possible that foreign actors could be working in collaboration with, or through, domestic actors. Ultimately, it is the impact of the incident on Canada's ability to have a free and fair election that is at issue in the determination of whether the threshold has been met, and if a public announcement is required. For clarity, Canadians – and democracy – are best served by election campaigns that offer a full range of debate and dissent. The Protocol is not intended to, and will not, be used to respond to that democratic discourse".

Both the standard and the considerations are quite vague. By themselves, they offer little guidance on when it would be appropriate for the Panel to act.

The considerations described in section 6.0 are all in aid of determining whether the threshold has been met. There are two other types of considerations that the Panel should take into account in its deliberations. The first would be whether there is any action short of an announcement that can prevent or mitigate the problem. For example, this could be a threat reduction measure by one of the NSAs or an action by a social media platform to flag or remove content.

The second type of consideration would be relevant in the event the Panel concluded that an incident or incidents had occurred that threaten the ability to have a free and fair election. Even where this threshold is met, might there be overriding national security or public interest considerations that should prevent an announcement from being made? For example, would a public announcement place a human source in danger? It might also include a consideration of whether an announcement made late in the campaign might be seen to unfairly advantage or prejudice one political party. Of course, a decision not to make an announcement where the threshold has been met would also engender controversy.

The Protocol already recognizes that sometimes there are overriding reasons why action should not be taken. As noted earlier, section 5.3 contemplates the possibility of national security/public security reasons for not informing an affected party. The same approach should be considered in assessing whether to make an announcement under section 6.0.

Recommendation nine

The government should consider amending section 6.0 to provide that, barring any national security or public interest reasons, an announcement would be made if the threshold is met.

There are some areas where the threshold and the considerations to be taken into account could be clarified.

i. Clarifying the standard required for the threshold to be met

Section 6.0 is somewhat confusing as to what is required in order for the threshold to be met. The opening paragraph stipulates that an announcement would only occur if the Panel determines that an incident or an accumulation of incidents has occurred that threatens Canadians' ability to have a free and fair election.

There are also three other standards embedded in the considerations set out in section 6.0: The degree to which the incident(s) undermine(s) Canadians' ability to have a free and fair election, the potential of the incident(s) to undermine the credibility of the election, and the degree of confidence officials have in the intelligence or information. However, as noted above, the final paragraph in section 6.0 contains the following sentence: "ultimately, it is the impact of the incident on Canada's ability to have a free and fair election that is at issue in the determination of whether the threshold has been met, and if a public announcement is required".

The sentence about impact is problematic. Officials may have a high degree of confidence in intelligence or information about the incident or incidents. How are they to assess, within the brief period of an election campaign, what the impact is? How are they to determine how many Canadians have been exposed to false information? How are they to distinguish the impact of interference or disinformation from the variety of other factors that voters take into account? [39] While surveys of voter reaction to disinformation may be possible early in the campaign, this becomes less feasible if the interference happens closer to the final day of voting. There is also the question of how reliable the survey results would be as voters continue to form their views after surveys are taken.

The challenge of measuring impact was highlighted in public commentary examining pro-Beijing disinformation campaigns targeting Conservative candidates. Were Conservative losses in several ridings with large Chinese diaspora communities due to attacks on the Conservative platform and on one of its candidates by media associated with or sympathetic to the Chinese government? Or were they the result of the Conservatives simply not being able to connect with sufficient numbers of voters in those communities?

As argued by Kenton Thibaut, "it is difficult to measure direct impact of such messages on election outcomes, especially given community concerns about the recent uptick in anti-Asian racism and the COVID-19 pandemic more broadly. Prior to the election, polling firm Mainstreet Research found that nearly 2/3 of self-identified Chinese voters surveyed stated that they would be supporting non-conservative candidates, a change from previous voting behavior".[40]

The government may wish to consider making actual, or potential impact, one of the considerations that the Panel takes into account in exercising its judgment as to whether the threshold has been met. It should clarify section 6.0 to avoid the interpretation that an inability to prove impact would prevent the threshold from being met.

Recommendation ten

The government should consider removing the fourth sentence in the final paragraph of section 6.0 and clarifying that actual or potential impact is one of several considerations that the Panel takes into account in exercising its judgment as to whether the threshold has been met.

---

[39] Multi-Stakeholder Insights: A compendium on countering election interference. – prepared by the Alliance for Securing Democracy (ASD), the Government of Canada, and Microsoft.

> "… Evaluating impact is almost impossible with some forms of foreign interference. For example, how can one evaluate the impact of a disinformation campaign on an election outcome in view of the complexity of the information ecosystem and voter intentions? In recent elections, after extensive analysis, it is impossible to determine with confidence that foreign intervention swayed the result nor that it was chiefly responsible for greater polarization."

[40] Kenton Thibaut, "China-Linked WeChat Accounts Spread Disinformation in Advance of 2021 Canadian Election." *Medium*, DFRLab, (2021 Nov).

ii. Attribution and timing

Section 6.0 acknowledges that attribution of interference attempts may be challenging or not possible within the timelines permitted by events, that is, within the caretaker period. This is because attempts to influence an election may involve misdirection and misinformation. The later during the campaign the incident takes place, the more difficult it would be to determine who is behind it. This problem was discussed by the Canadian Election Misinformation project in their report on the 2021 election:

"… It is becoming more difficult to detect disinformation and coordinated information operations. The rise of platforms like Rumble and Gettr that exercise minimal moderation and focus on privacy means that bad actors can more easily produce and widely disseminate content anonymously. Monitoring closed groups and encrypted communications is challenging to do at scale. This more vibrant and chaotic set of information vectors provides opportunities for those seeking to mislead, misinform, or manipulate. Thus, detecting and hopefully countering misinformation is becoming more challenging".[41]

Given the acknowledged challenges of attribution, one may ask whether the threshold for an announcement can be met even if it is not possible to attribute the source of the interference? For example, if it is clear that a party's data has been hacked and leaked, could there be grounds for informing the public even if the perpetrator cannot be identified in a timely way?

Section 7.0 appears to allow for that possibility. It only requires that an announcement focus on the notification of the incident, what is known about it (as deemed appropriate) and any steps Canadians should take to protect themselves.

The question of whether attribution to a specific malign actor should be included in the announcement is one for the Panel to decide. They will want to ensure that any announcement will be seen as credible by the public and the media. In some cases, that may be possible without attribution to a specific actor.

I: Should there be public notifications below the threshold?

The wording of section 6.0 leaves open the possibility that the threshold could be met even if the interference affects a small number of ridings or a specific targeted group of citizens. However, the context around the origins of the Protocol leads to the conclusion that the threshold is being interpreted as requiring an incident or incidents that threaten the integrity of the entire election. This view is reinforced by the following considerations:

- the development of the Protocol was influenced by the significant interference in the U.S. 2016 election

[41] Aengus Bridgman, et al., Mis- and Disinformation During the 2021 Canadian Federal Election. (68)

- the 2019 statement by the Minister of Democratic Institutions that there is a very high threshold for a public announcement and the hope that such an announcement never happens

Moreover, there are concerns that a Panel announcement itself could have the unintended consequence of affecting public confidence in the integrity of the election. According to testimony from the Deputy Director for Operations at CSIS, the national security agencies saw attempts at foreign interference in 2019 and 2021, but not enough to have met the threshold of impacting the integrity of the election.[42]

This leads to the question of whether the Protocol should countenance the possibility of a statement to the public for smaller scale incidents of interference that do not reach the high threshold of section 6.0. This is an issue that arose repeatedly during my consultations. An example could be voters in one riding or in a diaspora community receiving emails from malign actors threatening that if they did not vote for a particular candidate, they would regret it. While this would be unlikely to meet the threshold of threatening the integrity of the entire election, it could have an effect on the voting behaviour of those targeted.

A situation like this occurred near the end of the U.S. 2020 presidential election. It is described in the following excerpt from an article that was published in the New Atlanticist.[43]

"Thirteen days before the election, a surprise federal government press conference revealed that Russia and Iran had both obtained U.S. voter registration information, possibly from publicly available sources. While Russian usage was reported to be narrowly localized in its targets, Iran used the data to send barrages of spoof emails to sow chaos. The emails warned Democratic voters in Florida, Alaska, and elsewhere that 'we will come after you' if they did not vote for President Trump. The threatening messages claimed to be from the far-right group called the Proud Boys. While Director of National Intelligence John Ratcliffe argued that 'these actions are desperate attempt by desperate adversaries', FBI Director Chris Wray insisted that claims online that question the voting process should be met with 'a healthy dose of skepticism.'

Germany provides another example of public announcements about interference shortly before a national election. In September of 2021, less than three weeks before the date of the German national election, the federal prosecutor's office in Germany announced publicly that it was investigating who was responsible for a spate of hacking attempts aimed at lawmakers. Although the federal prosecutors did not name the country that was the subject of the investigation, there had been a statement from the German Foreign Ministry that it had protested to Russia, about attempts to obtain passwords and other personal information from federal and state legislators.[44]

[42] Irem Koka, "Foreign Interference Didn't 'Impact' Integrity of Federal Election." Thestar.com, Toronto Star, (2022 November).

[43] David Wemer, "Why Foreign Election Interference Fizzled in 2020." Atlantic Council, (2020 Dec).

[44] Melissa Eddy, "Germany Investigates Russia over Pre-Election Hacking." The New York Times, (Sept. 2021).

This is an area where there was no clear consensus among the individuals interviewed. Those who were opposed to a below the threshold announcement based their view on the need for a very high bar during the caretaker period. The threshold for an announcement was purposely set very high with the understanding that the intervention itself may contribute to the erosion of trust in the election. There is also the possibility that an announcement about interference could influence the results of the election. A decision to allow announcements for incidents below the threshold would fundamentally depart from the notion of an announcement as a measure of last resort to be invoked only in the most serious cases.

There were those who were in favour of greater transparency with the public to increase public understanding, build resilience and increase the public's confidence that the government was protecting the integrity of Canada's elections. If there was a clear case of interference that affected a single riding or targeted an ethnic group, it is unlikely to be considered significant enough to threaten the credibility of the entire election. And yet, if there is no mechanism to inform the voters targeted, they may exercise their votes based on false information or be intimidated into not voting at all.

There was a related concern that withholding information and having it come out after the election would decrease public confidence in the government's approach to countering election interference.

This is an issue that deserves further study. One needs to proceed carefully to import practices from other jurisdictions without fully understanding how those practices would fit within the institutional context and political culture of Canada.

There are communications challenges. It would be critical to educate the public and the media well before the election is called, that an announcement about smaller scale interference is very different from an announcement that the threshold has been met. There may be some guidance taken from the American and German examples where the announcements were made by either national security heads or prosecution office officials. It may be prudent that such an announcement not come from the Panel to clearly differentiate a notification of a small-scale incident from one that addresses a breach of the threshold and the integrity of the election.

It may be preferable to have a public notification of a below the threshold incident come from the head of a national security agency. The Protocol could clarify that under section 5.3, if the head of an NSA becomes aware of interference that does not meet the section 6.0 threshold, one of the options available would be for that person to make a public announcement. Because it is up to the Panel to evaluate incidents to determine whether the threshold has been met, there would have to be provision made for a preliminary consultation with the Panel to give them the opportunity to decide this issue.

There would also need to be some criteria as to the types of interference that warrants an announcement. The Canadian Election Misinformation Project provides some considerations as to the types of activity that warrant a response:

"Strategic decisions should be made about which false claims to debunk based on their origin, attention and engagement, and their potential damage, as well as the likelihood of a successful intervention. Anonymous accounts and online trolls with low impact and reach will always continue to bellow falsehoods. However, more pernicious forms of misinformation include foreign interference, astroturfing (e.g., coordinated amplification), and fabricated content (e.g., news fabrication, deep fakes). It is these latter forms of misinformation that should be addressed while the former should be left to blow by without further engagement".[45]

In some cases, it may be preferable for others to take the lead in calling out interference. There should be consideration as to whether other players in the election ecosystem are taking action. Has the interference been called out by social media platforms, traditional media or civil society election monitors?

Finally, there are several operational issues. What is the degree of confidence in the information that could lead to an announcement? Would the same rules apply for informing the government and the political parties as for when the threshold is met? The role of the ministers responsible for the national security agencies would have to be clear. Would they simply be informed, or would they have any role in the decision and, if so, would that role be reviewed post-election? What role should the Panel have? Should they be informed, consulted or have the final decision on a below the threshold announcement.

Providing for the possibility of below the threshold announcements would be a significant change to the Protocol. The views of the political parties will be important. It will also be important to consider the views of the national security agencies about taking on this responsibility.

Recommendation eleven

There should be further study of the issue of whether the Protocol should be amended to provide for the possibility of announcements below the threshold set out in section 6.0.

[45] Aengus Bridgman, et al., "Mis- and Disinformation During the 2021 Canadian Federal Election." (70).

Section 4: Briefing the political parties

One of the changes made to the Protocol in 2021 was to add a provision to the effect that political parties will be instructed on how to report any interference they may experience during the election. (Section 5.2)

This provision does not reflect the more extensive engagement between the NSAs and the parties. In both 2019 and 2021 briefings were offered by the NSAs to parties represented in the House of Commons. [***] These briefings were provided to designated party representatives who had received security clearances at the Secret level.

Briefings were offered to all of the party representatives together. There were two types of issues covered in these briefings. The first concerned best practices to protect political party data from being accessed by malign actors. The second concerned information about threats that the NSAs were aware of that could affect the parties. Some of these dealt with possible covert attempts by foreign actors to spread disinformation. During the 2021 election campaign, more attention was focused on the growing number of threats of physical violence from domestic actors.

Some parties also asked for one-on-one briefings with an NSA to address specific threats that they or their leaders and candidates were facing.

Interviews with party representatives elicited several comments about the briefings and about the Protocol.

The party representatives were pleased with the thoroughness of the briefings and the openness of the NSA representatives. They appreciated the opportunity to ask questions.

They noted that there had been an earlier opportunity to engage in advance of the 2019 election. The 2021 process felt like more of an afterthought. There was support to start the process of briefing party representatives earlier in the mandate. Some felt that there should be periodic briefings throughout the mandate. Earlier briefings would be particularly important to bring new party representatives up to speed on the threat environment.

Location of the briefings during the campaign was an issue. These briefings took place in secure facilities outside downtown Ottawa. Given how busy party representatives are during the campaign, there was a desire expressed that these take place in a secure facility downtown. There was also a request that, as much as possible, the briefings be done on a set schedule, known in advance, so that party representatives could plan accordingly.

Recommendation twelve

There should be an effort made to provide briefings to political party representatives at downtown Ottawa secure locations.

Recommendation thirteen

The times for briefings of political party representatives should be fixed in advance, with flexibility to address urgent situations.

All party representatives expressed their support for a Panel that is composed of senior deputy ministers.

There were several other issues raised by some of the party representatives.

i) Briefings of parliamentarians

Party representatives were concerned that parliamentarians may be targets of foreign interference. Members of Parliament and Senators are susceptible to being targeted by foreign state actors or their proxies throughout the life of a parliamentary session. There is presently no initiative by the NSAs to brief Members of Parliament and Senators on cyber-safety or on threats of foreign interference.

There was strong support among party representatives for there to be even an unclassified briefing of parliamentarians to increase their awareness of these issues.

Recommendation fourteen

The national security agencies should develop a program of unclassified briefings to increase the awareness of Members of Parliament and Senators on foreign interference and on election interference and on measures they can take to safeguard themselves and their online information.

ii) Funding for cyber security

Some parties expressed concern that they could use more resources to improve the security of their online data. Some advocated targeted government financial support to keep their voter and election related data secure. One suggestion was a rebate up to a prescribed limit, upon proof that the money was spent on shoring up cyber security.

iii) Concerns about foreign states influencing party nomination contests to favour sympathetic candidates

There were also concerns raised by some that some foreign states have supported potential candidates for Parliament who will promote the interests of the foreign state. They may receive assistance from agents of the foreign state to sign up party members to help the preferred candidate win a party's nomination.

This is a good example of election interference that takes place long before the election has been called. The parties themselves have a limited ability to identify whether this is occurring. Some would like more assistance from the national security agencies.

Section 5: Overall assessment

Section 9.0 requires that there be an assessment of the implementation of the Protocol and an assessment of its effectiveness in addressing threats to the election. Section 9.0 is asking two different questions. An assessment of the implementation of the Protocol is about whether its constituent elements worked as contemplated. An assessment of its effectiveness in addressing threats to the election is about whether it contributed to reducing or mitigating these threats. I will address each of these separately.

A. Assessment of the implementation of the Protocol

Did the Protocol work as contemplated?

Several elements worked well. Panel members were pleased with the introductory briefings they received, even if many would have preferred an earlier start. They were satisfied with the support they received from the SITE agencies and the PCO secretariats. There were clear roles and responsibilities between the Panel and the CEO. The political party representatives were generally pleased with the information sharing with government, although they would have preferred that the process begin earlier.

There are a few areas where improvements should be considered. The first is with respect to communications. There were numerous comments on the need for an early announcement to communicate clearly to Canadians and to the media about the nature of the threat, the integrated plan put in place to address it, and the role of the Protocol and the Panel as one element of that plan. A more robust communications approach could also provide an opportunity to explain the reasons behind the express inclusion of domestic actors, and the kinds of harmful behaviours that are the subject of the Protocol.

The second issue was the need to begin preparatory activities earlier in the mandate. The communications plan referred to in the preceding paragraph needs to be rolled out early enough that it is not taken as a signal that an election is imminent. Some Panel members also noted that an earlier start would allow for more in-depth briefings. It would also provide an opportunity for the Panel to be briefed by civil society actors who would bring a different perspective than that provided by the SITE agencies. Political party representatives also expressed an interest in earlier opportunities to be briefed on both the threat and on measures they could take to protect themselves.

Another area for improvement is in clarifying some of the language in the Protocol. Most importantly, language used in section 6.0 to determine whether the threshold has been met should be made more consistent. The requirement to demonstrate impact should be removed or clarified. Section 6.0 should mirror the approach taken in section 5.3 to recognize that there may be overriding national security or public interest considerations that may preclude an announcement.

Finally, there should be further consideration of whether the measures in place to address interference that falls below the section 6.0 threshold are adequate. In particular, should there be the possibility of informing the public in such cases?

B. Assessment of the effectiveness of the Protocol in addressing threats to the election

When the Protocol was introduced in 2019, the concerns seem to be with large scale foreign interference along the lines of Russian actions in the 2016 U.S. election. The Panel did not find that there was interference of that magnitude in Canada either in 2019 or 2021.

However, as the NSAs noted, there were efforts at foreign interference, but not sufficient to meet the threshold in section 6.0. And there were threats of domestic interference such as pandemic disinformation and threats of violence during the 2021 election campaign.

The nature of the threats is evolving. It is becoming clearer that election interference is only one element of a broader series of threats to Canada's democratic institutions. As noted earlier, the medium to long-term goals of foreign interference efforts include reducing the public's trust in democratic institutions, increasing polarization, lowering trust in the media and promoting the strategic interests of a foreign state. Activities like the targeting of elected officials to promote foreign state interests, encouraging individuals to act as proxies for foreign states, and threatening members of diaspora communities, are occurring long before election campaigns begin.

The credibility of the Plan to protect Canadian democracy depends on public confidence in the government's ability to effectively address the full range of these threats, well beyond incidents which occur during election campaigns. Public confidence depends on clear articulation of the problem and the approach to addressing it. This would require a review of the adequacy of existing measures, including legislation and resources. It also requires a whole of society approach with strong partnerships with civil society, academia, political parties and social media platforms.

Within this broader challenge is the issue of the effectiveness of the Protocol as one element of an integrated approach, focussed on interference during the caretaker period. The need for a non-partisan approach to addressing interference during this limited timeframe is valid. However, there has been undue emphasis placed on one element of the Protocol, the possibility of an announcement by the Panel if they determine that the threshold has been met. As discussed earlier, this was always seen as a measure of last resort. However, that option should remain. It is impossible to predict the future intentions of malign actors with respect to Canadian elections. The fact that the threshold has not been met to date is no guarantee that there will not be attempts at wholesale election interference during the caretaker period in the future.

However, the Protocol is about more than the possibility of an announcement by the Panel. It is supported by a robust information sharing infrastructure. The NSAs provide regular briefings to the Panel on the full range of threats, not just those which might meet the threshold. The Protocol provides for consultation mechanisms with the CEO. There are interactions between

PCO secretariats and the NSAs with civil society actors and social media platforms. Most importantly, the Protocol provides that the NSAs may take actions to address interference.

In explaining the Protocol to the public and the media, the emphasis should be less on the possibility of an announcement by the Panel and more on the full range of activities that occur during the caretaker period. The government may also wish to consider whether to add a preamble to the Protocol explaining this.

Recommendation fifteen

The Protocol should be maintained with the modifications noted in this report.

Recommendation sixteen

Public communications on the Protocol should emphasize the full range of activities that occur during the caretaker period, rather than being focused on the announcement by the Panel.

Section 6: Recommendations

A. By order in document

Recommendation one

Public communication about the Protocol should provide a clear explanation for the inclusion of domestic actors and of the types of activities that are of concern.

Recommendation two

Preparations for the next election should include an assessment of whether ministerial security, Royal Canadian Mounted Police protective policing, and local policing capabilities are adequate for the level and persistence of threats and whether there is effective coordination among these bodies. There should also be a review of the coordination between political parties and the government with respect to campaign and security operations.

Recommendation three

There should be an assessment as to whether any adjustments should be made to the role of the SITE membership in light of the growing problem of domestic interference.

Recommendation four

There should be an announcement, within a year of the previous election, about the government's plan to safeguard the integrity of Canada's elections, including an explanation of the reason for the Protocol.

Recommendation five

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. It should be clearer on how and by whom pre-election interference will be addressed, beyond saying that it will be handled through normal ministerial channels.

Recommendation six

It is recommended that the government consider options to ensure that the Panel is well-prepared in advance, and as much as possible, continuity of members is maintained between elections.

Recommendation seven

Briefings of the Panel should begin much earlier in the mandate and include non-government actors with expertise on interference and disinformation.

Recommendation eight

There should be an opportunity for a review body to assess the decisions of ministers with respect to the use of threat reduction measures during the caretaker period.

Recommendation nine

The government should consider amending section 6.0 to provide that, barring any national security or public interest reasons, an announcement would be made if the threshold is met.

Recommendation ten

The government should consider removing the fourth sentence in the final paragraph of section 6.0 and clarifying that actual or potential impact is one of several considerations that the Panel takes into account in exercising its judgment as to whether the threshold has been met.

Recommendation eleven

There should be further study of the issue of whether the Protocol should be amended to provide for the possibility of announcements below the threshold set out in section 6.0.

Recommendation twelve

There should be an effort made to provide briefings to political party representatives at downtown Ottawa secure locations.

Recommendation thirteen

The times for briefings of political party representatives should be fixed in advance, with flexibility to address urgent situations.

Recommendation fourteen

The national security agencies should develop a program of unclassified briefings to increase the awareness of Members of Parliament and Senators on foreign interference and on election interference and on measures they can take to safeguard themselves and their online information.

Recommendation fifteen

The Protocol should be maintained with the modifications noted in this report.

Recommendation sixteen

Public communications on the Protocol should emphasize the full range of activities that occur during the caretaker period, rather than being focused on the announcement by the Panel.

B. By category

Communications

- Public communication about the Protocol should provide a clear explanation for the inclusion of domestic actors and of the types of activities that are of concern. (1)

- There should be an announcement, within a year of the previous election, about the government's plan to safeguard the integrity of Canada's elections, including an explanation of the reason for the Protocol. (4)

- 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. It should be clearer on how and by whom pre-election interference will be addressed, beyond saying that it will be handled through normal ministerial channels. (5)

- Public communications on the Protocol should emphasize the full range of activities that occur during the caretaker period, rather than being focused on the announcement by the Panel. (16)

Panel considerations

- It is recommended that the government consider options to ensure that the Panel is well-prepared in advance, and as much as possible, continuity of members is maintained between elections. (6)

- Briefings of the Panel should begin much earlier in the mandate and include non-government actors with expertise on interference and disinformation. (7)

Protocol changes

- The government should consider amending section 6.0 to provide that, barring any national security or public interest reasons, an announcement would be made if the threshold is met. (9)

- The government should consider removing the fourth sentence in the final paragraph of section 6.0 and clarifying that actual or potential impact is one of several considerations that the panel takes into account in exercising its judgment as to whether the threshold has been met. (10)

- There should be further study of the issue of whether the Protocol should be amended to provide for the possibility of announcements below the threshold set out in section 6.0. (11)

- The Protocol should be maintained with the modifications noted in this report. (15)

Political actors

- There should be an effort made to provide briefings to political party representatives at downtown Ottawa secure locations. (12)

- Briefing times should be fixed in advance, with flexibility to address urgent situations. (13)

- The national security agencies should develop a program of unclassified briefings to increase the awareness of Members of Parliament and Senators on foreign interference and on election interference and on measures they can take to safeguard themselves and their online information. (14)

Security issues

- Preparations for the next election should include an assessment of whether ministerial security, Royal Canadian Mounted Police protective policing, and local policing capabilities are adequate for the level and persistence of threats and whether there is effective coordination among these bodies. There should also be a review of the coordination between political parties and the government with respect to campaign and security operations. (2)

- There should be an assessment as to whether any adjustments should be made to the role of the SITE membership in light of the growing problem of domestic interference. (3)

- There should be an opportunity for a review body to assess the decisions of ministers with respect to the use of threat reduction measures during the caretaker period. (8)

Annex A

Glossary of terms

Misinformation - False information that is not intended to cause harm.

Disinformation - False information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction.

Malinformation - Information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm.

Caretaker Convention - A convention under which the government of the day deals with only routine matters of administration and refrain from taking significant decisions related to matters such as policy, spending or appointments when it is unclear whether the government enjoys the confidence of the House of Commons.

Caretaker period - The Caretaker Convention typically begins on the dissolution of Parliament. It ends when a new government is sworn-in or a result returning an incumbent government is clear.

Writ period - Period commencing with the issue of a writ for an election and ending when the candidate or candidates have been returned as elected. Must be at lease 36 days and no more than 50 days.

Election and campaign period – Same time frame as writ period.

Pre-writ period – The *Canada Elections Act* (CEA) establishes a pre-election period during a fixed date general election. This period begins on June 30th and ends the day before the election writs are issued. During this period, there are spending limits for registered political parties and third parties, together with reporting obligations for third parties that meet a certain threshold for contributions received and/or expenses incurred**.**

Pre-election period – Time period commencing prior to the election being called. May include but is not limited to the pre-writ period.

Annex B

Morris Rosenberg biography

Morris Rosenberg had a long and distinguished career in the federal public service. He worked in the Department of Justice from 1979 to 1989 and was then appointed Assistant Deputy Minister in the Department of Consumer and Corporate Affairs. From 1993 to 1997, he was Assistant Secretary to the Cabinet, Economic and Regional Development Policy, at the Privy Council Office. He was appointed Deputy Secretary to the Cabinet (Operations) in 1996. Two years later, he was appointed Deputy Minister of Justice and Deputy Attorney General of Canada, a post he held for six years. He was then appointed Deputy Minister of Health Canada from 2004 to 2010 when he became Deputy Minister of Foreign Affairs. In 2013 Morris retired from the federal public service. He served as President and CEO of the Trudeau Foundation from 2014 to 2018.

Morris was appointed a Member of the Order of Canada in 2015 for his “sustained commitment to our country and for his effective and ethical leadership as a senior public servant.”

Annex C

Critical Election Incident Public Protocol

Cabinet Directive on the Critical Election Incident Public Protocol

1.0 Introduction

The protection and preservation of Canada's democratic institutions and practices is one of the core responsibilities of the federal government.

National security threat and risk assessments, along with the experience of key international allies, underscore that Canada's general elections may be vulnerable to interference in a number of areas. Recognizing this, significant work has been undertaken within the federal government to protect and defend electoral systems and processes. As part of this work, the Government of Canada has established the Critical Election Incident Public Protocol (CEIPP) in order to ensure coherence and consistency in Canada's approach to publicly informing Canadians during the caretaker period about incidents that threaten Canada's ability to have a free and fair election.

2.0 Purpose

The *Cabinet Directive on the Critical Election Incident Public Protocol* sets out the ministers' expectations with respect to the general directions and the principles to guide the process for informing the public of an incident that threatens Canada's ability to have a free and fair election during the period that the Caretaker Convention is in effect.

The Protocol is an application reflective of the Caretaker Convention. The Caretaker Convention puts into practice the principle that the government is expected to exercise restraint in its activities and "restrict itself" in matters of policy, spending and appointments during the election period, except where action is "urgent" and "in the national interest". The Caretaker Convention typically begins on the dissolution of Parliament. It ends when a new government is sworn-in or a result returning an incumbent government is clear.

During the caretaker period, announcements that must proceed are to be made in the name of the department to ensure a distinction between official government business and partisan activity.

3.0 Scope of Application

The Critical Election Incident Public Protocol will have a limited mandate. It will only be initiated to respond to incidents that occur during the caretaker period, and that do not fall within Elections Canada's areas of responsibility (i.e., with regard to the administration of the election, as identified in the *Canada Elections Act*). Incidents that occur outside of the caretaker period will be addressed through regular Government of Canada operations.

4.0 Panel

The Protocol will be administered by a group of senior civil servants who will, working with the national security agencies within the agencies' existing mandates, be responsible for

determining whether the threshold for informing Canadians has been met, either through a single incident or an accumulation of separate incidents.
This Panel will be comprised of:

- the Clerk of the Privy Council;
- the National Security and Intelligence Advisor to the Prime Minister;
- the Deputy Minister of Justice and Deputy Attorney General;
- the Deputy Minister of Public Safety; and
- the Deputy Minister of Foreign Affairs.

5.0 Process

The Protocol lays out a process through which Canadians would be notified of an incident that threatens Canada's ability to have a free and fair election, should notification be necessary.

During the caretaker period, the Protocol for a public announcement would be:

1. The national security agencies will provide regular briefings to the Panel on emerging national security developments and potential threats to the integrity of the election. The Panel may also receive information and advice from sources other than the security and intelligence agencies.

2. Political parties will be instructed on how to report any interference that they may experience during the election.

3. If the head of a national security agency (i.e., the Communications Security Establishment, the Canadian Security Intelligence Service, the Royal Canadian Mounted Police or Global Affairs Canada, working within their respective mandates) becomes aware of interference in a general election, they will, in consultation with each other, consider all options to effectively address the interference. As part of this process, they will inform the Panel. Barring any overriding national security/public security reasons, the agencies will inform the affected party (e.g., a candidate; a political party; Elections Canada) of the incident directly.

4. The Panel will evaluate incidents to determine if the threshold (as set out in Section 6 below) for informing the public has been met. The Panel will operate on a consensus basis and will draw on expertise from across government, including national security agencies working within their existing mandates. The Panel may consult with the Chief Electoral Officer (CEO) to ensure mandates are being respected should issues of interference arise that are possibly relevant to both the Panel and the CEO.

5. If a public announcement is deemed necessary, the Panel will inform the Prime Minister, the other major party leaders (or designated senior party officials who have received their security clearances sponsored by the Privy Council Office) and Elections Canada that a public announcement will be made. These leaders would all receive the same briefing information.

6. Immediately after having informed the Prime Minister, the other political parties and Elections Canada, the Clerk of the Privy Council, on behalf of the Panel, may either

issue a statement or ask the relevant agency head(s) to issue a statement to notify Canadians of the incident(s).

6.0 Threshold for Informing the Public

A public announcement during the caretaker period would only occur if the Panel determines that an incident or an accumulation of incidents has occurred that threatens Canada's ability to have a free and fair election.

Determining whether the threshold has been met will require considerable judgement. There are different considerations that could be included in making this judgement:

- the degree to which the incident(s) undermine(s) Canadians' ability to have a free and fair election;
- the potential of the incident(s) to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence or information.

The Panel brings together unique national security, foreign affairs, democratic governance and legal perspectives, including a clear view of the democratic rights enshrined in the *Canadian Charter of Rights and Freedoms*.

A disruptive event or incidents of interference may emanate from domestic and/or foreign actors. Attribution of interference attempts may be challenging or not possible within the timelines permitted by events, given that attempts to unduly influence the election may involve misdirection and disinformation. Further, it is possible that foreign actors could be working in collaboration with, or through, domestic actors. Ultimately, it is the impact of the incident on Canada's ability to have a free and fair election that is at issue in the determination of whether the threshold has been met, and if a public announcement is required. For clarity, Canadians – and democracy – are best served by election campaigns that offer a full range of debate and dissent. The Protocol is not intended to, and will not, be used to respond to that democratic discourse.

7.0 Announcement

The announcement would focus on:

a. notification of the incident;
b. what is known about the incident (as deemed appropriate); and
c. steps Canadians should take to protect themselves (e.g., ensure that they are well informed; cyber hygiene), if relevant.

8.0 Existing Authorities

Nothing in this Directive in any way alters or expands the mandates of the national security agencies or any other department or agency. Specifically, nothing in this Protocol supersedes the RCMP's independence.

9.0 Assessment

Following each general election, an independent report will be prepared, assessing the implementation of the Critical Election Incident Public Protocol and its effectiveness in

addressing threats to the election. This report will be presented to the Prime Minister and to the National Security and Intelligence Committee of Parliamentarians. A public version will also be developed. These reports are intended to help inform whether adjustments to the Protocol should be made to strengthen it.