

SECRET

**REPORT ON THE ASSESSMENT OF THE CRITICAL ELECTION INCIDENT PUBLIC
PROTOCOL**

May, 2020

SECRET

INTRODUCTION

On January 30, 2019, in recognition of the importance of protecting Canada's electoral process from foreign interference, the Government of Canada announced a number of measures to defend Canadian democracy and further strengthen our electoral systems against foreign cyber-enabled, and other threats.

Among these was the Critical Election Incident Public Protocol (the Protocol). It tasked a panel of five senior public servants (the Panel) with informing Canadians of any incidents or threats to the 2019 federal election that were deemed to be severe enough to undermine the integrity of the election or to impair Canadians' ability to have a free and fair election. This role was to be operative only during the election itself (the writ period).

The Cabinet Directive establishing this Protocol and the Panel was made public on July 9, 2019. A copy is appended as is a biography of the author of this report.

The Cabinet Directive also required that an independent review be carried out after the election that would assess the implementation of the Protocol and its effectiveness in addressing threats to the 2019 election.

The review was also meant to inform the decision as to whether the Protocol should be permanently established to help protect the integrity of future elections. If it were to continue, potential amendments that could strengthen the Protocol should also be examined. Should the recommendation be to continue the Protocol, the assessment should identify any potential adjustments to strengthen the mechanism.

The review was intended to focus on the model, the processes in place and the usefulness and timeliness of the information, rather than the outcome of any decision-making.

The assessment was conducted through a series of interviews with current and former government officials, political party representatives, and think tanks. As well, there was a review of Government documents, classified and others, foreign government public documents, domestic and international media reports as well as domestic and international reports from a variety of non-governmental organizations. It did not include intelligence briefings to the Panel (which were classified above the Secret level).

The assessment reviewed related developments in Canada (and a selection of foreign jurisdictions) from late 2016 until the after the election of 2019.

A broader perspective was adopted to provide a better understanding of the larger context within which the decision was made to create and implement the Protocol. It was also necessary because the Protocol cannot be adequately judged without

Page [APG] of 31

SECRET

reference to other related initiatives designed to safeguard the integrity of the election, some of which related directly to the Panel's operations.

In essence, the greater the effectiveness of other steps to strengthen the electoral process, the less likely it would be that the Panel would need to act during the writ period.

Page [APG] of 31

SECRET

BACKGROUND

Recent global developments:

Foreign interference in another country's elections is not a new phenomenon. It has, however, achieved a much higher profile in the last five years because of such efforts in elections and referenda in a number of Western democracies (the US, the United Kingdom, France, Germany and others). Those actions have stimulated a number of governments around the world to implement new measures, legislative and other, to mitigate against the risk of foreign interference in their electoral processes.

Canada was among those seeking to put in place new initiatives to this end given the experience elsewhere and the potential vulnerability to similar interference activities in this country. The development and implementation of new measures to help safeguard electoral systems in a number of Western countries is continuing.

Foreign interference:

The phenomenon of foreign interference in another country's affairs, including elections/referenda, is currently categorized in two forms:

- (a). "traditional" foreign interference. The 2019 Annual Report of the National Security and Intelligence Committee of Parliamentarians provides a comprehensive overview of this type of activity in Canada. However, the report did not deal with such interference in electoral processes (nor with the newer phenomenon of "cyber" interference).

Traditional electoral interference can include bribery, blackmail, illegal funding, coercion and intimidation, disinformation efforts and others intended to affect voter behavior or candidate selection processes. Many of the methods of interference, electoral or other, and their perpetrators have been and are common in a number of other countries.

- (b). "cyber" interference is a newer form of interference which exploits modern technologies to interfere in another country's affairs. Canada's Communications Security Establishment has published several documents (most notably in 2017 and 2019) outlining the threat to our democratic process and institutions from these kinds of activities.

It should be noted that there has been, and is an ongoing, level of foreign interference in Canada of both the "traditional" and cyber kind. Some of this has been masked to give the appearance of emanating from domestic, non-governmental individuals or organizations.

SECRET

Secondly, foreign interference is not limited to “adversarial state institutions”. Such interference has also been mounted by non-governmental entities – e.g. anti-abortion advocacy groups in the Irish referendum on that country’s abortion law or non-governmental players in the French election.

In addition, disinformation campaigns and the use of “fake news” have also manifested themselves in electoral processes around the world. The impact of these has been amplified by the decline of traditional news media (200 newspapers have closed in Canada in the last decade while those remaining have suffered a degree of hollowing out). That in turn has been exacerbated by the growing dependence on social media as a source of news and information. The capacity to fact check has diminished. Again, the points of origin can be unclear – foreign or domestic, governmental or non-governmental.

CANADA’S RESPONSE TO FOREIGN INTERFERENCE IN AN ELECTION

The Canadian Government’s concerns with foreign interference were 2016 US elections and 2016 British “Brexit” referendum. They were further amplified by subsequent events elsewhere around the world (France and Germany among others).

The February 1, 2017 mandate letter for the then newly appointed Minister of Democratic Institutions defined as a priority the following:

“In collaboration with the Minister of National Defence and the Minister of Public Safety and Emergency Preparedness, lead the Government of Canada’s efforts to defend the Canadian electoral process from cyber threats. This should include asking the Communications Security Establishment to analyze risks to Canada’s political and electoral activities from hackers, and to release this assessment publicly. As well, ask the Communications Security Establishment to offer advice to Canada’s political parties and Elections Canada on best practices when it comes to cyber security.”

In addition, the same Minister was also asked to lead the effort to amend the *Canada Elections Act*. Those changes were incorporated in *Bill C-76 the Elections Modernization Act*.

The subsequent development of a Canadian action plan began with a number of advantages at the time that the Ministerial mandate letter was issued.

First, Canadian officials were able to develop a better understanding of the techniques used in other jurisdictions to effect foreign interference. It was especially useful for them to have access to the lessons learned by security officials elsewhere on their systemic vulnerabilities and ways in which they had been attacked.

Page [APG] of 31

SECRET

Second, they were able as well to study, assess and adopt (or adapt) mitigation measures that other jurisdictions had developed and implemented to counter such foreign interference. These ranged from deterrence, to forms of protection, to countering attempts at interference.

Third, Canada has capable and experienced security agencies in place that already had a good understanding of foreign interference techniques (both traditional and cyber). The work of those agencies was subsequently bolstered by the G7 Rapid Response Mechanism and the establishment of the Canadian Centre for Cyber Security.

Fourth, we have a professional and experienced electoral administration and enforcement regime in Canada based on a comprehensive legal and regulatory foundation. Election administrators have continuously bolstered their security regimes to insure against interference. Unlike some other jurisdictions, there is only one administrator in Canada for federal elections.

Fifth, our national election is based on a paper ballot. The non-use of electronic voting in Canada diminishes some opportunities for foreign interference in an election.

Finally, the next Canadian election was scheduled for more than two and a half years later. Time was available to plan and implement measures to help safeguard the electoral process.

Over the course of the remainder of 2017 and through much of 2018, senior level officials from a range of federal organizations were actively engaged in assessing the threat of foreign cyber and other forms of interference. Potential vulnerabilities in the “electoral universe” to such threats were identified as were ways in which those risks could be mitigated. The issues at play were reviewed and discussed at multiple meetings in that period.

Consultations were held with a number of other democratic governments who shared the same concerns and, in some instances (e.g. France and Germany), had been the target of foreign interference after the 2016 US election.

As well, advice was sought from a range of non-governmental experts from academia, industry and think tanks, both foreign and domestic. Work was commissioned on issues relating to disinformation and ways in which traditional media, civil society and others can respond to it.

A series of initiatives – legislative, budgetary, policy and programmatic, organizational and others – together constituted the action plan that was developed to specifically target the problem of potential foreign interference.

To the extent possible they were aimed at the constituent elements of what was termed the “electoral ecosystem”: voters, political parties, academia and civil society, the

Page [APG] of 31

SECRET

media, social media platforms, Elections Canada, the Commissioner of Canada Elections, and the security and intelligence agencies.

A number of these were novel in the Canadian context.

The action plan – *The Plan for Protecting Canada's Democracy* – was organized around four objectives:

- (i) enhancing citizen preparedness to support the development of an engaged and informed citizenry;
- (ii) improving organizational readiness to ensure that government institutions, political parties, Elections Canada and the media were able to effectively plan for, respond to, and mitigate electoral interference;
- (iii) expecting social media platforms to act to take concrete action to increase transparency and combat disinformation; and
- (iv) combatting foreign interference to ensure that Canada had both a comprehensive awareness of the threats and strong international partnerships.

The Plan was unveiled at the end of January, 2019 in a press conference given by the Ministers of National Defence, Public Safety and Emergency Preparedness, and Democratic Institutions. That Ministerial press conference had been preceded by a technical briefing for media on the plan given by a number of senior public servants.

The Plan was supplemented by other actions (legislative and organizational) that while not directly electoral security *per se*, were very helpful in buttressing the Government's action plan on safeguarding the electoral system and players. A good example of this is Bill C-59, *An Act Respecting National Security Matters*, which provided for new operational authorities for the Communications Security Establishment and the Canadian Security Intelligence Service. The legislation received Royal Assent on June 21, 2019.

In June 2017 the Communications Security Establishment published *Cyber Threats to Canada's Democratic Process*.

It may have been unprecedented in terms its candor and clarity as to the threats and methodologies (and potential vulnerabilities to those) of possible foreign cyber interference in a Canadian election. It garnered widespread attention both in Canada and abroad.

These issues were addressed as well at the 2018 G7 Summit, hosted by Canada, which led to the establishment of the G7 Rapid Response Mechanism. Its purpose was to strengthen coordination to prevent, thwart and respond to malign and evolving threats to G7 democracies by sharing information and threat analysis, and identifying opportunities for coordinated responses. A coordination unit was set up in Global Affairs Canada, which serves as the permanent G7 secretariat to the Rapid Response

Page [APG] of 31

SECRET

Mechanism. Membership has since been extended to include Australia, New Zealand, the Netherlands, and Lithuania.

In October, 2018 the Government established the Canadian Centre for Cyber Security. It amalgamated existing cyber security expertise from a number of federal agencies. It was intended to provide a single unified source of expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operators, the private sector, and the Canadian public.

Both the G7 Rapid Response Mechanism and the Canadian Centre for Cyber Security went on to play important roles in the Government's efforts to safeguard the 2019 election.

In December, 2018, the *Elections Modernization Act* received Royal Assent. It contained a number of provisions intended to address attempts to disrupt electoral campaigns or voting. These touched on, among other things:

- prohibiting third parties from using foreign funds for partisan advertising and activities;
- clarifying the prohibition on a person or entity from making or publishing a false statement during the election period with the intention of affecting the election result;
- requiring online platforms to publish a registry of a person's or group's advertising;
- requiring political parties to publish their privacy policies for protecting personal information on their websites;
- expanding the Chief Electoral Officer's public education and information programs to the public at large; and
- expanding the Commissioner of Canada Elections' powers to make it more difficult for law breakers to evade sanction.

Elections Canada was very active itself on communications to the public, political parties, candidates for office, and the media. It also monitored social media and took steps, where necessary, to have misleading or incorrect material regarding the election itself (e.g. polling locations) removed from social media platforms.

The Chief Electoral Officer's first Report on the 43rd General Election (released February 18, 2020) offers a more comprehensive description of the varied communications efforts undertaken by his office for the 2019 election. This report will be followed by others on the 2019 election later this year.

The Communications Security Establishment published a second threat assessment which was made public on April 8, 2019.

SECRET

As well, both the Communications Security Establishment and the Canadian Centre for Cyber Security issued a number of cyber security related backgrounders and guidelines in the 18 months preceding the election.

The Canadian Centre for Cyber Security also more widely promoted its existing program, Get Cyber Safe, providing guidance on good security practices for Internet users.

Enhancing citizen preparedness:

Additional funding for “citizen digital literacy” programming and research was also committed:

- for the Digital Citizen Initiative to promote civic, news and digital media literacy through third party educational activities and programs to help citizens become resilient against online harms;
- for a new Digital Citizen Research Program, as part of the Initiative, to help Canadians understand online disinformation and its impact; and
- for the Public Policy Forum Digital Democracy Project

Finally, the Government announced the Critical Election Incident Public Protocol. Its role was detailed in a Cabinet directive which was made public on July 9, 2019. The release of that was accompanied by a technical briefing provided by Government and Elections Canada officials. The role and operations of the Panel established by this Protocol are addressed in greater detail below.

Improving organizational readiness:

Elections Canada began planning for last year’s election immediately after the 2015 election. A good deal of the preparatory work focused on security related issues.

Section 6 of the Chief Electoral Officer’s Report on the 43rd General Election together with another publication from his office, *How Elections Canada Contributes to Election Security*, provide a comprehensive account of the various measures adopted to help safeguard the election.

His office maintained close links before and during the election to Canadian security agencies and the Panel established by the Critical Election Incident Public Protocol. A hot line with the Communications Security Establishment was created to assist that office with any cyber security issues.

Political party representatives were given threat briefings and cyber security guidance from the Canadian Centre for Cyber Security. The Communications Security Establishment put in place dedicated hot lines for the parties to deal with any cyber

Page [APG] of 31

SECRET

security issues that arose. Later, security cleared party representatives were subsequently provided with Security and Intelligence Threats to Election Task Force classified threat briefings in advance of the election.

Social media platforms:

In late May, 2019 the Government reached agreement with Facebook, Twitter, Google, and Microsoft on measures to guide the conduct of these platforms during and before the 2019 election. The agreement was set out in the Canada Declaration on Electoral Integrity Online which was made public in late May of 2019. The platforms also took voluntary actions in this regard while the *Elections Modernization Act* imposed other new obligations.

Combatting foreign interference:

The Government established the Security and Intelligence Threats to Election Task Force to provide coordinated, one stop intelligence status reporting before and during the election itself. It was focused only on issues potentially relating to electoral security. Chaired by the Communications Security Establishment, it included representatives from the Canadian Security Intelligence Service, the Royal Canadian Mounted Police and Global Affairs Canada's Rapid Response Mechanism.

It began operations more than a year before the election, producing amalgamated reports that incorporated both classified and unclassified inputs from the four member organizations of the Task Force. The frequency of reporting increased with time. By August of 2019 the reporting updates were on a daily basis.

The Royal Canadian Mounted Police assigned criminal investigative files regarding foreign actor interference to the already existing Integrated National Security Enforcement Teams. It also briefed members of the Canadian Association of Chiefs of Police (representing all major municipal police forces in Canada) on foreign interference threats.

The Canadian security agencies – especially the Communications Security Establishment and Canadian Security Intelligence Service – maintained close links with their Five Eyes partners (US, UK, Australia and New Zealand) throughout the pre-election and election periods to benefit from their intelligence gathering that might relate to the Canadian election. The Rapid Response Mechanism did the same with their G7 partners. Other foreign partners were also consulted in the same regard.

Communications:

A considerable effort was made to ensure that the potential threats to our electoral system security and the measures taken to safeguard the integrity of that system were

Page [APG] of 31

SECRET

made publicly known. This was also the case with publicizing the ways in which voters could take their own steps to raise their awareness and protect themselves from these threats.

Ministerial speeches and appearances before Parliamentary committees were supplemented by detailed technical briefings of the media by senior public servants.

The publications issued by the Canadian Security Establishment on the possible threats faced were accessed by large numbers of Canadians as were the cyber safety guidance documents coming from the Canadian Centre for Cyber Security.

These communications efforts stretched out for almost two years prior to the 2019 election. The threat of foreign electoral interference in Canada was further amplified by international developments through this period. Interference actions in the French, German, Australian and 2018 US mid-term elections were widely reported. So too were foreign government responses to such events, whether through the adoption of new counter measures or lengthy inquiries into past interference (e.g. Mueller inquiry).

Canadian actions were reported upon in foreign media and were also reviewed by international bodies such as the Transatlantic Commission on Election Integrity and the Organization for Security and Cooperation in Europe. Their reports were made public before the 2019 election. Some foreign media contrasted the Canadian actions very favourably relative to the efforts of other Western countries.

Most public commentary on the Canadian effort, domestically or internationally, was positive. The one common shortcoming identified was the treatment of social media platforms: it was seen as too limited in coverage (given the limited number of platforms) and in the rigour of governance and enforcement provisions. The Canadian approach was judged to be more constrained relative to, for example, measures taken in some Western European countries.

SECRET

CRITICAL ELECTION INCIDENT PUBLIC PROTOCOL

The Protocol was made public on January 30 by the Minister of Democratic Institutions during a press conference outlining the Government's initiatives to protect the Canadian electoral process.

The Minister said:

"The Protocol establishes a simple, clear and impartial process to inform Canadians of a threat to the integrity of the 2019 election.

It is designed to avoid the kind of gridlock that could prevent an effective response. The core responsibility for the Protocol resides in a group of senior civil servants.

This group brings together national security, foreign affairs, democratic governance and legal perspectives.

This group of public servants has the experience to critically assess the security and intelligence considerations as well as the implications of informing Canadians of a serious threat. They are the public service's most senior officials mandated to be impartial, transparent and fair.

Let me be clear: this is not about refereeing the election itself. This about alerting Canadians of an incident that jeopardizes their rights to a free and fair election. If something happens during the campaign, they can trust that the right people have decided to make it public and the information can be trusted to be true and accurate and not a political game.

Because this issue rises beyond partisan considerations. The Protocol has a narrow scope and a very high threshold for a public pronouncement. The protocol will only apply to incidents that occur within the writ period.

If the group determines that the threshold has been met, the Clerk of the Privy Council will direct the head of the relevant security agency to notify Canadians of the incident.

As we developed this protocol, we consulted on a number of occasions with the four major political parties in order to be fair and transparent.

It was important that political parties understood and trusted the purpose of the protocol and that decisions made by this senior group of public servants will be made in an impartial manner.

Page [APG] of 31

SECRET

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.”

In essence the creation of the Protocol and its Panel was intended to avoid a situation such as occurred in the 2016 US 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.

The Protocol appears to have been a uniquely Canadian invention. There does not appear to be any equivalent body elsewhere in the world.

Mandate:

Its mandate was very specific and circumscribed. It was, in effect, a contingency mechanism to be used only in very limited circumstances. It was based in part on the Caretaker Convention which sets out guidelines for conduct during an election period. As the Convention notes “it is incumbent upon a government to act with restraint during an election period”. It is as well premised on the practice of delegating necessary government business to officials during an election campaign and the expectation of public servants to act if deemed necessary.

Given the experience in the US election, it was equally grounded in the view that any announcement during an election campaign that could have an impact on that election should best come from a non-partisan source. In this case, unlike the US experience, that responsibility did not rest with one official but, instead, with a group of five senior non-partisan public servants arriving at any decision on a consensus basis.

The limitations in the mandate are explicit in the Protocol.

First, the mandate would only be “initiated to respond to incidents that occur during the writ 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*).”

Second, “a public announcement during the writ period would only occur if the Panel determines that an incident or an accumulation of incidents has occurred and 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;

Page [APG] of 31

SECRET

- the potential of the incidents(s) to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence or information.”

Third, in respect of the type of incidents at issue the Protocol stipulated: “Although a disruptive event or interference may emanate from domestic and/or foreign actors, as a starting point, the focus should be on foreign interference.” The protocol went on to add: “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 had been met, and if a public announcement is required.”

Fourth, the Panel had to operate on a consensus basis: all had to concur with any decision.

Finally, any public announcement would be limited: “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.”

It was understood that Elections Canada and the Commissioner of Canada Elections would act during the writ period to address issues within their jurisdictions. Similarly, both Canadian Security Intelligence Service and Communications Security Establishment were expected to respond to issues covered by their authorities if and when required.

Composition of the Panel:

The Panel selected for this task was one of several options considered by the Government. Other alternatives that were reviewed did not include any public servants.

The Panel that was established was composed 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 of Canada
- the Deputy Minister of Foreign Affairs Canada
- the Deputy Minister of Public Safety and Emergency Preparedness Canada

Those were chosen because of the responsibilities of their offices/organizations.

SECRET

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 to exert in coordinating the member organizations 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.

All were very experienced – an average of 24 years in the public service through assignments in a variety of departments and agencies. All had some exposure to security and intelligence issues and the agencies working in those areas; some had a very substantial experience with these matters. Each had a different experience base and different perspectives to bear on the issues before the Panel.

However, the personalities on the Panel changed between the time of its first announcement in late January and the election in October.

The Clerk of the Privy Council on January 30 subsequently resigned his post effective April 18, 2019 in the midst of the SNC Lavalin controversy. He wrote: “one of the key roles of the Privy Council Office is to be ready to assist whichever government Canadians elect in October”.

He went on to say: “It is now apparent that there is no path for me to have a relationship of mutual trust and respect with the leaders of the Opposition parties...Therefore, I wish to relinquish these roles before the election.”

Finally, in regard to the public service panel on which he was to serve for the coming election, he concluded: “It is essential that during the writ period the Clerk be seen as an impartial arbiter of whether serious foreign interference has occurred”.

He was replaced as Clerk by the then Deputy Minister of Foreign Affairs. The position of Deputy Minister of Foreign Affairs was filled by the then Deputy Minister of Immigration, Refugees and Citizenship.

Page [APG] of 31

SECRET

Separately, the then Deputy Minister of Public Safety Canada retired and was replaced by the Associate Deputy Minister of that department in May of 2019.

Finally, the Deputy Minister of Public Safety was subsequently replaced on the panel by the Associate Deputy Minister of Public Safety Canada for the writ period in the fall of 2019.

Challenges:

To begin with the Protocol was effectively an experiment never before seen in the Canadian context and without any international analog from which to draw comparisons or lessons.

Time was a critical factor in a number of respects. To begin with, there was relatively little time before the election to prepare the Panel. Secondly, the election campaign (the writ period) has a very compressed time frame of fifty days and is dynamic and fast moving. Any potential intervention - based on a consensus judgement - by the Panel had to be exercised quickly in the rapidly evolving circumstances of political campaigning and the 24/7 world of news and social media.

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). A second prerequisite was that any decision to intervene during the writ period would require consensus of the Panel.

The landscape of potential threats of interference brings to mind Donald Rumsfeld's universe of knowledge: known knowns; known unknowns and unknown unknowns. That is to say that the information upon which the Panel makes its decisions might not be perfect in terms of accuracy or completeness irrespective of whether it was coming from security agencies or social media analysis.

The range of potential perpetrators of interference was a large one: hostile state actors (either identifiable as such or masked as domestic actors), foreign non-state actors including those closely aligned to hostile state governments, foreign non-state actors from friendly jurisdictions (e.g. fake news sites, single issue groups or chaos promoters) or domestic actors with malign intentions.

Similarly, the gamut of interference actions could be very diverse: cyberattacks to cripple critical IT infrastructure; cyber attacks to steal data for public release (with or without amending some or all of it with false information), disinformation campaigns mounted through social media platforms (with potentially unknown initial origins - domestic or foreign) and a variety of traditional foreign interference applications.

Page [APG] of 31

SECRET

A particular problem, as was true of the experience in other jurisdictions, was with social media posts and the often difficult challenge of differentiating between purely domestic activity and foreign actions cloaked to present themselves as being of domestic origin.

The officials addressing their responsibilities as members of the Panel were also expected to continue to discharge the responsibilities of their own offices. In three cases the individuals were very new to their offices, having been appointed in April of 2019, meaning they were on a double learning curve.

Support for Panel:

The core support for the work of the Panel was provided by two secretariats of the Privy Council Office: Security and Intelligence (S and I), and Democratic Institutions (DI). Those two secretariats and the Panel were also supported by a third secretariat (Communications).

The two secretariats (DI and S and I) provided much of the material for the Panel in both the pre-writ and writ periods. This included a standard reference volume covering many of the basics on players, roles and responsibilities in the electoral security family. They also provided the scenarios used throughout the pre-writ and writ periods in the table top exercises that were a staple of the preparations of the Panel (although they were also used in other fora too, such as the security briefings for political party representatives).

The agendas, materials, and records of discussion for the Panel's meetings were furnished by these secretariats. Meetings with the Panel and various others (Elections Canada, security agencies) were coordinated and organized by them as well.

In addition, the secretariats responded to requests from the Panel for additional documentation and briefing materials. They responded similarly to requests from individual members of the Panel in order to help fill gaps in their knowledge base on specific issues.

More generally the secretariats provided coordination, with S and I leading on the work by other agencies involved in the election security domain such as the Security and Intelligence Threats to Election Task Force (and the individual organizations that contributed to the Task Force).

The S and I Secretariat additionally played a key role in the already existing inter-agency structure of national security committees of officials (at the Deputy Ministerial, Assistant Deputy Minister and Director General levels).

SECRET

Panel operations:

The Panel met for the first time at the end of May, 2019. Subsequent meetings continued on through the summer and through the writ period. It was understood, however, that through the writ period, the Panel was to be on call as required by circumstances.

The Panel focused its efforts in these areas:

- achieving a common understanding of the Protocol and its elements and especially the threshold for intervention by the Panel;
- understanding and becoming familiar with the roles, responsibilities, operations and personalities of their key interlocutors (Chief Electoral Officer and Elections Canada, the Commissioner of Canada Elections and the security agencies);
- comprehending the range of potential foreign interference threats in play for the electoral process. This also included the possible role domestic actors might play - as fronts for foreign interests or otherwise - and the roles that social media platforms could play as enablers of these activities;
- assessing the relationship between an act of interference and its potential or actual impact on the election and voters, (as well as the possible impact on those of an intervention by the Panel during the writ period);
- arriving at a common understanding of what the baseline was in Canada for ongoing foreign interference activities (cyber and traditional) on the assumption that this would be a constant going forward. New attacks above that level would therefore require particular scrutiny;
- working on team building so as to facilitate consensus decision-making.

Responding to these objectives was accomplished through various mechanisms.

The first meeting of the Panel focused on its mandate. The Protocol was reviewed and discussed in detail, clarifications were made and a clear understanding was achieved.

It was clear that it had a defined and limited role to play. It was not to be an election arbiter. It was to intervene publicly only during the writ period and only in exceptional circumstances where the threshold criteria were met. It was to act only on the basis of a consensus among the members of the Panel. The possible implications and consequences of any such intervention were clear.

The threshold became an ongoing focus of debate and discussion in the Panel from there and on through into the writ period. A wide range of scenarios of possible interference, the sources of those, and their potential implications – local, regional or beyond - were addressed in table top exercises and other group reflections. Some of these were carried out with the participation of other actors including the security agencies, Elections Canada, and the Commissioner of Canada Elections.

Page [APG] of 31

SECRET

The discussions, whether within the Panel or with a broader group of participants, elicited different perspectives and considerations all of which helped inform views on the threshold and the circumstances which might prompt the Panel to intervene.

The roles of the Panel and key partners – the security agencies, the Security and Intelligence Threats to Election Task Force, Elections Canada and the Commissioner of Canada Elections - had been addressed in the basic reference document. Clarifications on these, where needed, were arrived at through discussions among all of them in meetings prior to the writ period. The respective responsibilities and operations, under their individual authorities, were clearly understood by each of the actors.

The threat intelligence and information provided to the Panel began with the core threat assessments prepared and published by the Communications Security Establishment (which were incorporated in the basic reference documents for the Panel). These were subsequently augmented through briefings of the Panel by the security agencies at meetings in the pre-writ period. Those briefings covered the range of potential interference activity and sources, whether cyber or more traditional forms. Issues involving disinformation and “fake news” were also reviewed by the panel. Where required further individual briefings were organized for Panel members as requested.

In addition, the Security and Intelligence Threats to Election Task Force provided daily amalgamated multi-source intelligence and information (social media assessments) to the Panel members. These continued through to the election and ensured that the Panel was kept fully and currently apprised of developments.

The threat briefings also provided the Panel members with insights into baseline or ongoing interference in Canada by foreign actors. This, in turn, was factored into the Panel's consideration of the threshold and its possible application.

The Panel was in operation for nearly five months, from its first preparatory meeting at the end May until the October election. In that time frame its members developed a rapport and common foundation of understanding of the Panel's role and the varied challenges they all faced in meeting their responsibilities. Numerous discussions and debates brought forward different perspectives and considerations but also

promoted a degree of cohesion and basis for moving to consensus on issues they faced.

Communications/Reactions:

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

Page [APG] of 31

SECRET

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 Privy Council Office's Communications Secretariat and other government organizations regularly responded to media enquiries on the work of the Panel.

Overall public and media reaction to the Protocol and the Panel was neutral to positive, (and principally factual reporting). Political parties had been consulted in advance on the Protocol and concurred with the approach. Party representatives interviewed for this assessment similarly expressed acceptance of the concept. One recommended that it be re-constituted sooner rather than later so as to be prepared for the next election.

That said there were a few criticisms made of the Protocol and the Panel.

One was to the effect that there should be no Protocol or Panel on the grounds that any intervention by the Panel in the election campaign would do more harm than good. In other words, the potential confusion prompted by the intervention would be worse than the harm provoked by the interference the Panel was reporting.

Another argued that the composition of the Panel was wrong, either because they were not public figures and would therefore lack credibility, or because an election is a fundamentally political phenomenon beyond the survey of public servants. This had two variants. The first was that a Panel of public servants was entirely wrong. Instead the Panel should be composed of other personalities – eminent Canadians, former jurists, or former political leaders. The second was that the Panel that had been struck should have had as a member a representative of Elections Canada as the administrator of the election.

A third observation put forth by a political party representative interviewed for this assessment recommended that the Panel (or some government entity) had to play an ongoing role in addressing disinformation. This was predicated on the view that traditional "fact checkers" could no longer suffice in that regard.

Conclusions:

The Panel did not intervene during the 2019 election but it had been ready to do so if warranted. Intervening was not a test, in and of itself, of its utility; not intervening did in fact reflect a decision or decisions taken. There was no impact on the election as a

Page [APG] of 31

SECRET

consequence of any action by the Panel. That it did not have to intervene was good news.

The Protocol was an experiment put into place under tight time constraints. Many of the features of the Protocol were invented from whole cloth.

Most of them, the threshold especially, required judgement, knowledge and context. The types of issues with which they might have to contend do not readily lend themselves to detailed, guiding metrics.

The Panel put in place to implement the Protocol was diverse with a range of public service experience. Familiarity with security and intelligence matters varied but was supplemented where needed.

The Panel was well supported and enjoyed an informed and collegial relationship with its principal partners (Elections Canada and the security agencies). The intelligence and information inputs it received were timely, varied and considered.

On the whole the implementation of the Protocol had been successful.

SECRET

RECOMMENDATIONS

The next Canadian election is scheduled for October 16, 2023. However, the current Government is in a minority position – the sixth in the last fifty years. The life span of the past five minority governments has ranged between 209 days and just over two and a half years.

If the Government wishes to have the capacity to alert Canadians to a significant incident of interference in the next election the least risk option would be to put the Protocol and Panel in place for that purpose.

In this case the institutional composition of the Panel would remain the same. Similarly, the threshold and consensus provisions of the Protocol would remain unchanged. The high threshold would help avoid the Panel becoming a frequent intervener in any election, (something that was not envisioned when it was established). The consensus provision for decision making on any potential intervention by the Panel adds confidence and credibility to any such decision.

One possible revision to the existing Protocol could be considered: changing the operational time frame for the Panel to include both the writ and pre-writ periods. The rationale for this is two-fold.

The principal reason is that it is unlikely that any potential foreign interference would be confined to the writ period alone. A recent case in point is the cyber attacks on the Australian Parliament and three of the largest political parties. Those were carried out before the 2019 election campaign began.

Second, this would allow the revelation of any foreign 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 change would not be possible to make in the event of an unexpected earlier election were the Government to lose the confidence of the House of Commons before October 16, 2023.

The rationale for staying the course with the Protocol, amended or not, is based on both a simple cost-benefit analysis and a reasonable risk management consideration.

The model has already been accepted by Opposition parties. It has not been publicly or otherwise discredited.

There are still three members of last year's Panel in their same positions and they have an unparalleled experience now having participated in last year's proceedings.

Page [APG] of 31

SECRET

The two new members of the Panel would be the new Deputy Minister of Public Safety and the new National Security and Intelligence Advisor. Both could start to be groomed for a role on the Panel.

The original criteria for the Panel membership of a mix of different experience and perspectives would still hold. As well this Panel would be ready sooner than any alternative group given the experienced members from last year.

If the Protocol and Panel were to continue as recommended, that decision should be accompanied by an appropriate media strategy.

The Panel would have to be supported as it was last year (by PCO secretariats, security agencies and the Security and Intelligence Threats to Election Task Force).

A repetition of the collaborative relationship with Elections Canada would also be necessary.

The core support group could begin with preparing the two new members of the Panel and then arranging for meetings of the whole Panel to ready itself.

Monitoring and assessing any instances of foreign interference in coming elections in other democracies in the next two years should be a particular focus for the core support group. A number of countries previously subjected to foreign interference in their last elections have new elections scheduled in the coming two years. This year they are Singapore, Georgia, Lithuania and the United States; next year the Netherlands and Germany will have elections while France will have them in 2022.

In the event that there is foreign interference in any of those elections it will be especially important to pay heed to the application of new technologies and operational methodologies by the perpetrators. It will be equally important to take note of any new defensive measures (legal, regulatory, operational) adopted by any of the potential target states. Some might be transferable here.

Additionally, the Panel support group can also monitor and report on academic and think tank research here and elsewhere that might provide useful insights on election interference issues.

Consideration should also be given to moving forward now on one related issue.

The relationship with political parties represented in the House of Commons that was brought into effect for last year's election should be made operational again. Political parties in other jurisdictions have often been the primary targets of foreign interference (the USA with the Democratic National Committee in 2015, France with the President's party in 2017, and last year in Australia with three parties being the victims of cyber attacks).

Page [APG] of 31

SECRET

Party representatives here would benefit from both cyber security guidance and access to classified intelligence related to potential interference threats here (or the experience of foreign jurisdictions in the coming two years). Starting now with both types of collaboration would be reasonable given that their potential vulnerability to interference is not limited to the writ period of an election. They could be subject to attack at any point between now and the next election.

Rightly or wrongly, the arrangement with social media platforms, (the *Canada Declaration on Electoral Integrity Online*), received the most criticism from those assessing the Government's safeguard measures for last year's election. Several steps should be considered in this area looking ahead to the next election.

The first would be an evaluation of the extent to which the platforms lived up to their commitments in the 2019 agreement.

Second, a determination should be made as to whether any new agreement should extend beyond those covered by the 2019 agreement. In the first, instances some other North American platforms might be looked at for possible inclusion. As well, selected foreign language platforms might also be assessed for the same purpose.

Once these evaluations have been completed, discussions should be launched with the platforms concerned as to what the Government's expectations for their behaviour might be heading into the next election.

It was recently announced that Canada would lead a working group to ensure the protection of electoral processes. This is in the context of the recently created multilateral governmental/private sector's Paris Call for Trust and Security in Cyberspace. It established Nine Principles to that end of which the Third Principle is aimed at protecting the integrity of democratic elections. The work carried out here should be instructive as to the scope and objectives of any new Canadian agreement with social media platforms.

SECRET

CLASSIFIED**FOREIGN INTERFERENCE IN THE 2019 ELECTION**

At this juncture there appears to have been no significant foreign interference in last year's election—at least none that rose above the baseline level of ongoing interference thereby possibly triggering the Panel to intervene.

Unlike the 2016 US election, the 2017 French election and the 2019 Australian election there appears to have been no substantial cyber attack and theft of data.

The data systems and communications networks of Elections Canada and political parties do not seem to have been negatively affected by any foreign interference intrusions.

There does seem to have been some foreign origin social media activity but not at any significant level. Its impact, as with domestic origin social media activity in this period, does not appear to have been consequential.

The Digital Democracy Project of the Public Policy Forum and McGill's Max Bell Scholl of Public Policy monitored social media activity throughout the election campaign. Three citations from their final report are noteworthy in this regard:

“Interestingly, we found little evidence that the tense 2019 Canadian election influenced levels of affective polarization, which remained relatively stable throughout the campaign. Nor did we find evidence that social media exacerbates affective polarization, which seems to be driven by ideology, partisanship and perceptions of party extremity.”

“...neither automated nor manual analysis uncovered evidence of coordinated behaviour that we would label election manipulation or interference.”

“Our finding is that disinformation did not play a major role in the 2019 election campaign. This is consistent with the findings of many other investigations by journalists, academics, government agencies and officials and the private sector. That is not to say that there were no instances of disinformation, but what there was generally did not appear coordinated and had limited impact”.

Finally, there does appear to have been a few possible instances of attempts at traditional foreign interference but not of sufficient possible impact to have caused an intervention by the Panel.

Why is it that foreign interference seems to have played such a limited role in the election last year? A variety of explanations have been offered.

Page [APG] of 31

SECRET

One is that potential hostile foreign states (and their proxies) were generally satisfied with the political landscape in Canada prior to the election and sanguine about possible outcome of the vote.

Another is that some of the principal potential state actors were too pre-occupied with bigger priorities in other countries.

Russia, for example, was likely far more interested in the 2019 Ukrainian presidential election and in planning for potential interference in the 2020 American election. These would have been in addition to other reported instances of Russian interference in Georgia and Mozambique, among others.

China was far more focused on developments or interference in areas closer to them, including Hong Kong, because of the pro-democracy movement (democracy being one of the traditional Chinese government's "five poisons"). Interfering in the Australian elections, in a variety of ways, was also a major focal point for them going into 2019.



Finally, there is the view that efforts were made to carry out cyber attacks here but that they were ultimately unsuccessful and abandoned. A related thesis is that the array of new defensive measures (and security agency authorities) undertaken in the two preceding years, together with pre-existing strengths here, together acted as a deterrent to such interference efforts.

Whether the Protocol (and Panel) acted as a deterrent is difficult to assess. It may have had such an effect to the extent that it would have revealed interference activity that the perpetrators hoped would have been kept concealed from public view.

In the period leading to the currently scheduled Canadian election in 2023 there will be elections in a number of other democracies, all of which have been affected by foreign interference, to some extent or other, in their last elections.

The most notable of these is the American election this year. The American intelligence community's election threats executive said earlier this year that more nations may attempt more types of interference in this year's election. She said: "This isn't a Russia-only problem ... we're still also concerned about China, Iran, non-state actors, "hacktivists. And frankly ... even Americans might be looking to undermine confidence in the elections."

Page [APG] of 31

SECRET

Canadian vulnerability to foreign interference in our next election is difficult to gauge accurately at this point. Responsible caution, however, would dictate that we keep our guard up in the event that our perceived vulnerability grows, whether because of policy decisions (foreign or domestic), international developments, changes in technology or seeming laxness in defensive readiness.

Page [APG] of 31

SECRET

Appendix 1

James Judd

He joined the then Department of External Affairs in 1973 as a Foreign Service Officer. After several assignments in headquarters, he posted as Second Secretary in the Canadian Embassy in Caracas, Venezuela.

On return to Ottawa, he was assigned to the Personnel Bureau in headquarters. In 1981/82, he acted as Secretary to the Restrictive Trade Practices inquiry into the competitiveness of the Canadian petroleum industry. He returned to the Department of External as a senior advisor to the Assistant Deputy Minister (reorganization). In 1983 he was posted to the Canadian Embassy in Washington as Counsellor (Congressional Relations).

He returned to Ottawa to in 1987 as Senior Departmental Assistant to the Secretary of State for External Affairs, the Right Honourable Joe Clark. In 1991/92 he served as Chief of Staff to Mr. Clark, the then President of the Privy Council and Minister Responsible for Constitutional Affairs.

In 1992 and 1993, he worked in the Privy Council Office as Assistant Secretary to Cabinet for Foreign and Defence Policy. He returned to the Department of Foreign Affairs and International Trade on special assignment to the Deputy Ministers Office. In 1994, he became the Assistant Deputy Minister, Corporate Services.

He left the Foreign Service in 1996 to become the G7 Deputy and Assistant Deputy Minister, International trade and Finance in the Department of Finance. He was made Deputy Minister of National Defence in 1998. In 2002, he was appointed Secretary of the Treasury Board and Comptroller General of Canada. In 2004, he was named Director of Canadian Security and Intelligence Service. He retired in 2009.

Page [APG] of 31

SECRET

Appendix 2

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 2019 General Election may be vulnerable to foreign 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 writ 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 during the writ period of an incident that threatens Canada's ability to have a free and fair election.

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".

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.

SECRET

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 within the writ 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 prior to the writ period will be addressed through regular Government of Canada operations.

4.0 Panel

The CEIPP 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 writ 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.
2. 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) become aware of interference in the 2019 General Election, they will, in consultation with each other, consider all options to effectively address the interference. 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.
3. 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

Page [APG] of 31

SECRET

consensus basis and will draw on expertise from across government, including national security agencies working within their existing mandates.

4. 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.
5. 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, would 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 writ 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*.

Although a disruptive event or interference may emanate from domestic and/or foreign actors, as a starting point, the focus should be on foreign interference. That being said, attribution of foreign 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.

Page [APG] of 31

SECRET

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 the 2019 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 2019 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. The report is intended to help inform whether the Protocol should be established on a permanent basis going forward to help protect the integrity of future elections or what adjustments to the Protocol should be made to strengthen it.