UNCLASSIFIED

Cyber Threats – Protection of Canada's Democracy

Key Messages

Canada recognizes that bad actors may use cyber technology to interfere and influence Canadians, as they have done or attempted to do in other democracies.

Ahead of our 43rd General Election, Canada put in place a comprehensive, whole-of-society plan to counter foreign interference in our elections and safeguard our democratic processes.

The plan mobilized expertise from across 10 departments and agencies in an effort to anticipate, recognize and respond to any potential threats to the integrity of our election. Over the months leading up to the election, the Government regularly tested its capacity, in order to probe its readiness and practice and refine its efforts.

Based on a study entitled *Cyber Threats to Canada's Democratic Process* performed by the Communications Security Establishment, the Panel did not observe any activities that met the threshold for public announcement or affected Canada's ability to have a free and fair election.

Canada instituted a whole-of-society approach to safeguard the 2019 General Election and Canada's democratic institutions against foreign interference. The approach included activities under each of the four following pillars.

Enhancing citizen preparedness: Supporting the development of an engaged and informed citizenry.

Improving organizational readiness: Ensure that government institutions, political parties, Elections Canada and the media are able to effectively plan, respond, and mitigate electoral interference.

Combatting foreign interference: Ensure that Canada has a comprehensive awareness of the threats and strong international relationships.

Expecting social media platforms to act: Encourage social media to take concrete actions to increase transparency and combat disinformation.

[APG]

UNCLASSIFIED

Cyber Threats – Protection of Canada's Democracy

Issue

Cyber threat activity against the democratic process is increasing around the world, including in Canada.

States, groups, or individuals might use cyber capabilities to threaten or influence Canada's democratic process.

Adversaries may seek to change Canadian election outcomes, policymakers' choices, governmental relationships with foreign and domestic partners, and Canada's reputation around the world.

Anticipated Questions and Answers

How did Canada enhance citizen preparedness against foreign interference in the election?

Creating the **Digital Citizen Initiative** to support digital news and civic literacy programming and tools to improve Canadians' resilience against disinformation. (Canadian Heritage)

Canadian Heritage received $7M in off-cycle funding for digital news and civic literacy programming and tools to improve Canadians' resiliency against online disinformation. This will help to equip Canadians with a better understanding of deceptive practices used online, and give people the tools they need to navigate the internet, including tools to help them better understand the information they consume online.

Increasing the reach and focus of **Get Cyber Safe**, the national public awareness campaign created to educate Canadians about cyber security and the simple steps they can take to protect themselves online, to include greater linkages to cyber threats to Canada's democratic processes. (Communications Security Establishment)

Releasing an **update to the Cyber Threats to Canada's Democratic Process**, the public assessment of threats to Canada's elections, political parties and politicians, and media. (Communications Security Establishment)

Establishing the **Critical Election Incident Public Protocol**, a mechanism for communicating with Canadians during the writ period in a clear, transparent, and impartial manner about incidents that threaten the integrity of the election. (Privy Council Office)

[APG]

UNCLASSIFIED

Cyber Threats – Protection of Canada's Democracy

How did Canada improve organizational readiness against foreign interference in the election?

Offering additional cyber security technical advice and guidance to political parties to enhance security. (Communications Security Establishment)

Offering classified threat briefings to key leadership in political parties to promote situational awareness and help them to strengthen internal security practices and behaviours. (PCO, Communications Security Establishment, Canadian Security Intelligence Service, Royal Canadian Mounted Police)

Engaging with Elections Canada, who has leadership for the operational conduct of elections, to ensure seamless integration with the Government of Canada's national security apparatus.

How did Canada combat foreign interference in the election?

Leveraging the newly-established Security and Intelligence Threats to Elections (SITE) Task Force to improve awareness of foreign threats and support assessment and response. (Communications Security Establishment, with Canadian Security Intelligence Service, Royal Canadian Mounted Police, and Global Affairs Canada)

Activating the G7 Rapid Response Mechanism to strengthen coordination among G7 democracies in responding to threats to democracy, and monitoring malign actors in the social media space. (Global Affairs Canada)

How did Canada manage social media platform influence leading up to the election?

Establishing a common understanding with platforms about their responsibilities in the online democratic space through the Canada Declaration on Electoral Integrity Online.

[APG]

UNCLASSIFIED

Cyber Threats – Protection of Canada's Democracy

PCO's role

PCO works with departments and portfolio agencies to ensure it has up to date knowledge of the threat landscape and underlying trends, as well as initiatives being developed to mitigate threats and ensure that Canadians trust that the electoral process is fair, that our politicians are not beholden to foreign or criminal interests, and that the media is not influenced by foreign or criminal interests attempting to sway voters and the outcome of the democratic process.

Involvement/actions of other government departments

The Security and Intelligence Threats to Election (SITE) Task Force, made up of the Communications Security Establishment (CSE), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and Global Affairs Canada, worked to identify and prevent covert, clandestine, or criminal activities from influencing or interfering with the electoral process in Canada.

Based on a study entitled *Cyber Threats to Canada's Democratic Process* performed by the Communications Security Establishment, the Panel did not observe any activities that met the threshold for public announcement or affected Canada's ability to have a free and fair election.

As noted in the Cabinet Directive on the Critical Election Incident Public Protocol, an independent report will be prepared, assessing the implementation of the Protocol and its effectiveness in addressing threats to the 2019 general election. The report is intended to help inform the decision as to whether the Protocol should be permanently established to help protect the integrity of future elections and, if it is to continue, suggest potential adjustments that could strengthen the Protocol. A classified report will be presented to the Prime Minister and to the National Security and Intelligence Committee of Parliamentarians, with a public version made available shortly thereafter. It is expected that these reports will be available in Spring 2020.

[APG]

UNCLASSIFIED

Cyber Threats – Protection of Canada's Democracy

Financial or other tables (budgets, statements, other)

Budget 2019

The Protecting Democracy initiative received a total of $48M in Budget 2019, with the following year-by-year breakdown:

(Millions of dollars)	2018-2019	2019-2020	2020-2021	2021-2022	2022-2023	2023-2024	TOTAL (cash)
CSIS	0	0	2	3	6	12	23
CSE	0	2	1	1	0	0	4
PCH	0	5	5	5	5	0	19
GAC	0	1	1	1	0	0	2
TOTAL	0	8	9	10	11	12	48

To protect Canada's democratic institutions from cyber attacks, the Government is proposing to provide the Communications Security Establishment with additional funding of up to $4.2 million over three years, starting in 2019–20, to provide cyber security advice and guidance to Canadian political parties and election administrators.

To strengthen cooperation and information sharing in response to foreign threats to our democracies, G7 Leaders agreed during the June 2018 Summit in Charlevoix to each set up a Rapid Response Mechanism unit, with Canada taking on an added coordination role on behalf of the network. To support this commitment, the Government proposes to provide Global Affairs Canada with $2.1 million over three years, starting in 2019–20.

To strengthen Canadians' resilience to online disinformation and to help ensure Canadians have access to a wide range of transparent, high-quality information, Budget 2019 proposes to provide the Department of Canadian Heritage with $19.4 million over four years, starting in 2019–20, to launch a Digital Citizen Initiative. Funding would support research and policy development on online disinformation in the Canadian context. This investment would also enable Canada to lead an international initiative aimed at building consensus and developing guiding principles on how to strengthen citizen resilience to online disinformation. These guiding principles would then be adopted by Canada and other likeminded countries as a framework for efficient cooperation between governments, civil society organizations, and online platforms

CSIS was also provided with $23M to advance its efforts under this initiative.

[APG]

UNCLASSIFIED

Cyber Threats – Protection of Canada's Democracy

Additional background information (to be deleted)

Background on the Communications Security Establishment's *Cyber Threats to Canada's Democratic Process* Reports (2017 and 2019)

In 2017, in response to a request from the Minister of Democratic Institutions, the Communications Security Establishment (CSE) produced and made publicly available an assessment of the cyber threats to Canada's democratic process. The report's purpose was to let Canadians know about the cyber threats to our democratic process ahead of Canada's General Election. An update to this report was published in the months leading up to the election, focusing on the threats to (1) political parties and politicians, (2) elections, and (3) voters.

CSE assessed that, in the 2015 Canadian federal election, Canada's democratic process was targeted by low-sophistication cyber threat activity, likely perpetrated by hacktivists or cyber criminals. This activity had no effect on the results of the election and had no impact on the privacy of Canadians.

An update report published in 2019 found that half of all advanced democracies holding national elections in 2018 had their democratic processes targeted by cyber threat activity. Foreign cyber interference targeting voters has become the most common type of cyber threat activity against democratic processes worldwide. Elections have also continued to be targeted by cyber threat activity over the past years.

In addition to these threats, there is a growing recognition that digital platforms and social media companies have an important role in both the promotion of a democratic marketplace of ideas and the suppression of democratic values through the propagation of disinformation. Social media companies have a role to play in helping to reinforce the awareness and resilience of Canadians to information that could mislead them during the election.

The variety of both paper-based and electronic systems used to carry out elections in Canada means that vulnerabilities to cyber threats vary by jurisdiction. As noted in the CSE's 2017 report, federal elections are largely paper-based and Elections Canada has a number of legal, procedural, and information technology measures in place to mitigate cyber threats. Political parties and politicians are vulnerable to cyber attacks, including cyber espionage, information theft, and the spread of misleading information. Social media is vulnerable to misuse through

[APG]

the spread of fake news or the use of bots to amplify particular viewpoints, giving a false appearance of public consensus or discord.

[APG]