For Public Release

Government of Canada | Gouvernement du Canada
Privy Council Office | Bureau du Conseil privé

UNCLASSIFIED

Protecting Canada's Democracy: Overview

Overview

- On January 30, 2019, the Minister of Democratic Institutions, alongside the Ministers of Public Safety and Defence, announced the plan to safeguard the 2019 General Election and Canada's democratic institutions from interference.

- Canada's whole-of-society approach includes 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

- In addition to the various activities the Government of Canada has already been undertaking, as well as the ongoing operations of Canada's security and intelligence agencies, Canada is taking the following new measures to protect the 2019 General Election:

Enhancing Citizen Preparedness

- Creating the **Digital Citizen Initiative** to support digital, news and civic literacy programming and tools to improve Canadians' resilience against disinformation. (Canadian Heritage)
  - $7 M in digital, news and civic literacy programming and tools to improve Canadians' resiliency against online disinformation

- 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)

Improving Organizational Readiness

- 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. (Communications Security Establishment, Canadian Security Intelligence Service, Royal Canadian Mounted Police)

Combatting Foreign Interference

- 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)

- Forming a **Foreign Interference Actor Investigative Team** to investigate and disrupt criminal acts conducted as part of foreign interference. (Royal Canadian Mounted Police)

- 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)

Expecting Social Media Platforms to Act

- **Engaging with social and digital platforms** to encourage them to implement specific measures to increase transparency and combat the spread of disinformation. (Privy Council Office)

Background on the Communications Security Establishment's 2019 Report, entitled *2019 Update: Cyber Threats to Canada's Democratic Process*

- In response to a request from the Minister of Democratic Institutions, the Communications Security Establishment (CSE) produced and made publicly available an updated assessment of the cyber threats to Canada's democratic process. Its purpose is to let Canadians know about the cyber threats to our democratic process ahead of Canada's General Election in 2019

- The report found that in 2018, half of all advanced democracies holding national elections had their democratic processes targeted by cyber threat activity. While cyber threats continue to target the three aspects of the democratic process – voters, political parties, and elections –, foreign cyber interference targeting voters has become the most common type of cyber threat activity against democratic processes worldwide.

- The report assessed that it is very likely that Canadian voters will encounter some form of foreign cyber interference related to the 2019 General Election, and that this foreign interference resembling activity undertaken against other advanced democracies in recent years. Foreign adversaries have attempted to sway the ideas and decisions of voters by focusing on polarizing social and political issues, promoting the popularity of one party over another, or trying to shape the public statements and policy choices of a candidate.

- Elections have also continued to be targeted by cyber threat activity over the past years. However, as noted in the 2017 report, Canada's federal elections are largely paper-based and Elections Canada has a number of legal, procedural, and information technology (IT) measures in place that provide very robust protections against attempts to covertly change the official vote count.

Background on the Communications Security Establishment's 2017 Report, entitled *Cyber Threats to Canada's Democratic Process*

- 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, focusing on elections, political parties, and the media. The assessment concluded that while there are no indications that nation-states have used cyber capabilities with the goal of influencing the democratic process during an election in Canada, cyber threat activity is increasing globally and Canada is not immune.

- The report identified a number of cyber threats to Canada's democratic processes and actors. CSE assessed that, at the federal level, political parties, politicians, and the media are more vulnerable than the elections themselves. The types of threats they face include attempts to sway opinion against political candidates, and to manipulate both traditional and social media to influence political discussion or reduce trust in the democratic process. 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 the spread of

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

- 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.

- CSE found that over the past five years there has been an upward trend in cyber threat activity against democratic processes around the globe. CSE judges that it is highly probable that cyber threat activity against democratic processes worldwide will increase in both volume and sophistication in the next year and beyond.

Government of Canada / Gouvernement du Canada
Privy Council Office / Bureau du Conseil privé

UNCLASSIFIED

Protecting Canada's Democracy: Speaking Points

- A healthy democracy is built on fair and free elections. Protecting that democracy should matter to everyone: Canadians, political parties, governments and the private sector.

- Canada is in an election year and we recognize that bad actors may use cyber technology to interfere and influence Canadians, as they have done or attempted to do in other democracies.

- Canada has a government-wide plan to prepare and respond to this dynamic and evolving threat. We have taken the necessary steps to understand the threats, where they come from and how they could affect our electoral system and democratic institutions.

- We are mobilizing whole-of-government expertise in an ongoing effort to anticipate, recognize and respond to these threats. The Government also regularly tests its capacity, in order to probe its readiness and practice and refine its efforts.

- Canada's approach will remain nimble and responsive in order to continue to combat foreign interference activities.

- All Canadians have a responsibility to help ensure Canada has a free and fair 2019 General Election, and must do their part to protect Canada's democratic institutions.

Enhancing citizen preparedness

- Canada's best defence against threats to democracy remains an engaged and informed public.

- By understanding common online deceptive tactics like phishing or trolling, Canadians can be less susceptible to online manipulation.

- We are encouraging Canadians to think more critically about what they see online, and to think before they share as a way to stop the spread of disinformation.

Improving organizational readiness

- We are mobilizing government wide expertise to enhance systems and practices to ensure we can prepare for, respond to, and mitigate election interference.

For example:

- On an ongoing basis, the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) are informing Elections Canada of threats, potential tactics and systems vulnerabilities.

- The Government will provide technical advice to political parties and election officials to help them better protect their own cyber systems.

- The Government will continue to organize exercises where various departments use scenarios and potential incidents to test plans and responses to threats.

Combatting foreign interference

- Canada's security and diplomatic organizations are at the frontline of Canada's effort to combat foreign interference campaigns.

- This broad coordination is reflected in the newly established Security and Intelligence (SITE) Task Force:
  - the Canadian Security Intelligence Service (CSIS);
  - the Royal Canadian Mounted Police (RCMP);
  - the Communications Security Establishment (CSE); and
  - Global Affairs Canada (GAC).

- Canada has been a leader in coordinating and responding to diverse and evolving threats to our democracy. It is leading the G7 Rapid Response Mechanism, to manage, triage, share information and identify opportunities for a joint G7 response to democratic threats.

Expecting social media platforms to act

- While social media platforms play an important role in connection people and communities, they have been manipulated by bad actors.

- These organizations have a role in helping Canadians understand where information is coming from, from whom, and for what purpose.

- We are having frank conversations with social media platforms to identify concrete steps they can take in preparation for the next election.