Election Security Communications

PCO Communications

May 15, 2019

Overview

- In January of 2019, the Government of Canada announced a series of measures to safeguard Canada's 2019 Federal Election.
- The Critical Election Incident Public Protocol (the Protocol) lays out a simple, clear and impartial process by which Canadians should be notified of a significant threat to the integrity of the 2019 General Election.
- The protocol includes provisions for: informing candidates, organizations or election officials if they have been the known target of an attack; informing the Prime Minister and other party leaders (or their designates) that a public announcement is planned; and notifying the public.
- The protocol will be implemented by a five-member panel of Canada's senior public servants: the Clerk of the Privy Council; the National Security and Intelligence Advisor; the Deputy Minister of Justice and Deputy Attorney General; the Deputy Minister of Public Safety; and the Deputy Minister of Global Affairs Canada.
- The threshold for the Panel's intervention during the election will be very high. It will be limited to addressing exceptional circumstances that could impair Canada's ability to have a free and fair election.
- It will be activated for incidents that may occur within the writ period and that do not fall within Elections Canada's areas of responsibility (i.e., the administration of the election).

Current Initiatives

Government

- Security and Intelligence Threats to Elections (SITE) Task Force
- G7 RRM (GAC) will produce social media analysis and reports on threat patterns and trends based on open source information
- Engagement with digital platforms

Political Parties

- CSIS, CSE and RCMP providing classified threat briefings to key leadership in political parties
- CSE providing cyber technical advice, guidance, and services to political parties

Public

- Digital Citizen Initiative
- *GetCyberSafe* Public Awareness Campaign
- 2019 Update: Cyber Threats to Canada's Democratic Process

Considerations

Diverse threat landscape, involving many partners

- Cyber threats to political parties and electoral machinery (CSE, CSIS, RCMP, Elections Canada)
- Criminal activity (RCMP, Elections Canada)
- Foreign interference and disinformation (GAC, Public Safety)

Challenges of election context

- Caretaker convention makes a response to disinformation or an incident during the election more difficult; low risk tolerance
- Interest from media and public about potential impacts on the electoral campaign will be considerable

Machinery challenges

- Little capacity to identify disinformation within departmental social media teams
- Governance for assessment of incident impacts on the election and decision-making remains unclear
- Information-sharing between Communications and National Security Organizations can be challenging due to classification regimes and or security clearance

Strategic Approach

Establish GOC Communications Governance for Election Security

- GOC Election Communications DG working Group (PCO Chaired)
- Joint planning of proactive communications, issues management, disinformation response
- Ensures structure to provide recommendations to senior management in the case of an incident that threatens Canada's federal election
- Leverages information flow from DG ESSC, and provides analysis and recommendations to ADM ESSC.
- Supported by interdepartmental strategic communications and social media working group

Strategic Approach (Continued)

Proactive Media Engagement

- Coordinated media outreach campaign to engage and educate journalists about the types of threats to the election seen and the activities being undertaken by the GoC
- The events will be framed as a dialogue and should be “lock-up” style where media can pose questions and engage directly with experts (CSE, GAC, CSIS, Public Safety, Heritage, Elections Canada)
- Events will be held monthly, beginning in June 2019 and through to end of the election

Strategic Approach (Continued)

Single Channel: ELECTIONSAFE.gc.ca, @electionsafecanada

- Consolidated web and social media channel that would be a non-partisan focal point for communications about threats to the election, foreign influence and disinformation
- The channel would be a place for the government to provide updates about analysis suggesting emerging threats or to make general statements about the state of preparedness (outputs?)
- It would also serve as a place where known tactics of inauthentic actors would be explained
- The single channel would also promote awareness of other efforts (Cyber Centre, etc.) to build resilience in the Canadian population

Strategic Approach (Continued)

Disinformation: Analysis and Response

- Disinformation is the deliberate creation and/or sharing of false information with the intention to deceive and mislead audiences
- Throughout the election RRM to conduct regular SM monitoring and reporting to identify evidence of foreign disinformation*, based on the top 10-15 issue profiles developed with input from GOC departments. This will be supplemented by monitoring conducted by Federal Departments.
- Departments will also develop and pre-approved messaging to address key issues, in the event of a likely incident.
- When RRM identifies disinformation issues through its trend analysis, PCO Communications will work with departmental communications to quickly analyze the issue, identify its objective and offer tactics to address it.
- This information will be fed into SITE and the counsel (G5 Secretariat) as well National Security Community

*Response to disinformation perpetrated by domestic actors will be also identified and considered through this process.

Disinformation Response prior to the Election

- If significant disinformation is detected prior to the election, PCO Communications will coordinate with the National Security Community, Democratic Institutions and the implicated department(s) to develop a integrated approach to address the issue.
- Approach will consider the objective and impact of the incident and identify tactics to respond, as necessary.
- When appropriate, the response will include notification through the single channel and outreach to media.

Disinformation Response during the Election

- A communications response to disinformation during the election must respect the caretaker convention.
- If significant disinformation is detected during the election, PCO Communications will coordinate with the National Security Community, Democratic Institutions and the implicated department(s) to develop a communications approach to address the issue in a significantly more sensitive environment
- Significant and rapid notifications will need to be sent throughout the system including up to the deputy level.
- This information will be fed into SITE and the counsel (G5 Secretariat) who decide if the disinformation would fall into the Critical Incident Response Protocol
- If it is not part of the protocol, responses, if appropriate, would come from the affected department once coordination and approvals are complete

Communications election preparedness working group

- PCO will convene regular meetings with implicated heads of communications (will need to engage head of comms for Elections Canada)
- This group of heads of Comms will validate choices of a working level group who will determine:
  - Spokespersons
  - Media protocol
  - An information sharing protocol
  - The planning media engagement campaign noted above
  - Content for the consolidated channel
  - On-going communications about Canada's preparations to address threats to elections

Detailed next steps

- Communication working group (established), who will focus on info sharing and discussions in advance of and throughout the election.
- Determine how communications fits into G5 discussions and briefings supporting them.
- Launch of central channel; nature of context (clinical, without attribution)
- Embed a communications expert in SITE
- Disinformation Playbook (could be longer term question)

Rollout

- Confirm Communications Approach
- Possible Ministerial announcement—Update from Jan 30
- Media Engagement Sessions
- Establish Single Channel
- Disinformation Playbook