Safeguarding Elections from Foreign Interference:
Lessons from Home and Abroad

Summary

On behalf of the Security and Intelligence Threats to Elections (SITE) Task Force, Rapid Response Mechanism (RRM) Canada coordinated a series of five workshops for Government of Canada departments and agencies in preparation for General Election 44 (GE44) in February and March 2021, as follows:

1) Research methods, privacy, and operational security for open source analysts (February 1)
2) FVEY Elections Lessons Learned (February 4)
3) GE43 Lessons Learned (February 11)
4) Digital Foreign Interference Trends and Counter-measures (February 19)
5) Cyber-enabled Foreign Interference Threats in Elections and Referendums (March 23)

The aim of the series was to contribute to a comprehensive awareness of the threats to Canadian election from foreign interference, including information manipulation and disinformation. The series included a day-long training course for open source researchers and analysts. The workshops featured government experts and trusted civil society partners from Canada, the FVEY states as well as the G7. Each workshop was attended by an average of 40 Government of Canada participants.

Key Takeaways

Research methods, privacy, and operational security for open source analysts

The full-day training, provided by Intel Techniques, was aimed to help open source researchers and analysts better understand, reduce and manage risks associated with online research. The training covered the following subjects:

- Current trends and challenges, such as the growing use of social engineering tactics by hostile actors and social media platforms changing their policies, making investigations more difficult.
- Best practices in conducting open source analytics, putting emphasis on demonstrating how an efficient and secure work environment reduces the risk of compromise, including reducing the risk of digital cross-contamination and minimizing digital footprints, while also optimizing note-taking for better reporting and research accountability.
- Digital hygiene, including techniques and practices necessary for protecting researchers and their organizations. The training stressed the importance of a common understanding of risks, robust threat modelling, and a collective approach to safety.

FVEY Elections Lessons Learned Highlights

*Please note that this was a classified workshop and only a few high level points are shared below.

FVEY discussion revealed common challenges and approaches to countering foreign interference, with discussion focussing on countering information manipulation. The following high level points stood out:

- Shared experience in preparatory measures, including challenges related to whole-of-government coordination;

[APG]

- Preponderance of domestic as opposed to foreign disinformation leading to and during elections or referendums;
- Difficulty in assigning attribution, assessing impact, and weighing public notification in case of information manipulation incident;
- Hostile state actors discussed were broadly the same, along with tactics deployed;
- FVEY partners share the same predicament when it come to the evolving digital ecosystem and must look to addressing emerging tactics as opposed to always looking backward.

GE43 Lessons Learned Highlights

Panelists: Jim Judd (former CSIS Director), Lyall King (SITE Chair), Emerson Brooking (Resident Fellow at the Atlantic Council's Digital Forensic Research Lab (DFRLab)), Taylor Owen (Max Bell School of Public Policy, McGill University), Sarah Stinson (PCO –DI), Gallit Dobner (RRM)

- The Critical Election Incident Public Protocol (Protocol) played an important role in safeguarding the 2019 General Election from interference.
- Going forward, consideration should be given to implementing the Protocol for the next general election, broadening its time frame to include the pre-writ period, lowering the threshold triggering its use, establishing the same relationships with political parties (particularly with respect to guidance and support around cyber issues).
- Canadian political information ecosystem is likely more resilient than that of other countries, in particular the US, due to a populace with relatively high trust in the traditional news media, relatively homogenous media preferences with only a marginal role for hyper-partisan news, high levels of political interest and knowledge, and fairly low levels of ideological polarization overall.
- Canada benefited from lessons learned from other jurisdictions, especially the 2016 US presidential elections and UK Brexit referendum.
- Canadian policy makers took these potential vulnerabilities seriously, introducing the Elections Modernization Act, as well as a number of additional initiatives to attempt to address some of the key weaknesses seen in other jurisdictions.
- While Canada distinguished itself as a pioneer in the field of digital resilience and democratic defense, several additional measures should be considered to better safeguard Canada's democracy:
  1. new law to designate foreign agents, particularly during elections;
  2. reconsider the evolving nature of foreign interference (including by entities from allied states) and the overlap between domestic and foreign information manipulation;
  3. revisit the remit of bodies intended to counter foreign interference; and, build more government oversight and enforcement capability for social media.

Digital Foreign Interference Trends and Counter-measures Highlights

Panelists: Chloe Coliver (Chloe is Head of Digital Policy and Strategy) and Milo Comerford (Head of Policy & Research, Counter-Extremism) from the Institute for Strategic Dialogues (ISD); [redacted] (RRM)

The presentation and discussion during this workshop was based on ISD report *Best Practices in Detecting and Analysing Foreign State Online Manipulation* (available upon request).

[APG]

- Digital information manipulation is a new form of attack on democracies that is constantly evolving.
- The challenge of identifying and exposing covert use of online information systems is complex – it goes beyond singular events (elections), a few key actors (Russia and China), and most prominent tactics and techniques (inauthenticity and coordination).
- Coordination, not just in terms of information sharing, but also in sharing lessons and leveraging the capabilities of various sectors (i.e. CSO, government, private, media) allow for more effective responses.
- The need for analytical rigor is critical to those researching and detecting disinformation. In order to work most effectively empirical insight needs to connect well with strong concepts and definitions.
- An ideal capability to conduct rigorous online manipulation research should rely on six guiding principles:
    1. It must rely on data from the full range of platforms and online spaces relevant to online manipulation activities online.
    2. It should have a detection function to identify and filter social media data based on conformance to a series of behaviors related to online manipulation.
    3. It should be sensitive to platform specifics while able to operate across platforms.
    4. It should keep evolving, acquiring additional analytical and technological capacities.
    5. It should have a cyclical discovery function, enabling the system to stay on top of constantly evolving tactics, actors and targets in the digital space.
    6. The empirical outputs should contribute to, and draw from conceptual and definition work.

Cyber-enabled foreign interference in elections and referendums

Panelists: Jacob Wallis (Senior Analyst, International Cyber Policy Centre, Australian Strategic Policy Institute); [redacted]

The presentation and discussion during this workshop was based on an ASPI report titled *Cyber-enabled foreign interference in elections and referendums*. Key takeaways included:

- The threats posed by cyber-enabled foreign interference in elections and referendums will persist, and the range of state actors willing to deploy these tactics will continue to grow.
- Responses to these threats should be calibrated according to the identified risks and vulnerabilities of each state.
- The report proposes recommendations based on four broad themes:
    1. Identify vulnerabilities and threats as a basis for developing an effective risk-mitigation framework;
    2. Protect societies by improving societal resilience through raising public awareness and nurturing cyber-related research capacity;
    3. Improve cyber-enabled foreign interference detection capabilities; and,
    4. Nurture and leverage response capabilities to defend against the threat.

Drafted by: RRM Canada, [redacted]
Approved by:

[APG]

Released: