UNCLASSIFIED

USS
Meeting of the Election Protocol Panel of Five

October 14, 2020, 15:00-16:00

Objectives

- Discuss threat assessment prepared by Security and Intelligence Threats to Elections (SITE) Task Force (classified document to be forwarded by CSIS).
- Inform other Panel members of new challenges GAC's Rapid Response Mechanism (RRM) Canada team is facing in identifying foreign threats online.
- Highlight ongoing challenges in determining impact of online disinformation.
- Discuss Privy Council Office (PCO) Democratic Institutions-led process to protect Canada's democracy: Protecting Democracy 2.0.

Run of Show

- PCO has billed this meeting as an informal conversation to: (1) reconnect Panel of Five members; (2) provide the National Security Advisor an opportunity to brief on the current threat picture should a federal election be called; and (3) discuss the PCO Democratic Institutions-led process to help protect Canada's democracy.

Key Messages

Evolving threat environment

- It's clear current global threat environment is different from last fall.
- COVID-19 is important factor: more Canadians online and global infodemic mean more scope than ever before for malign activity to reach Canadians unchecked.

New challenges to identifying foreign threats to democracy online

- At the same time, it's more difficult than ever to identify foreign state sponsored information manipulation online.
- First, our adversaries are employing increasingly sophisticated tactics to blur lines between domestic and foreign activity, and between overt and covert messaging, leveraging a multiplicity of social media platforms and, increasingly, web sites.
- For example, instead of creating fake personas with large follower bases, they are amplifying polarizing domestic narratives using a combination of platforms.
- China demonstrated new willingness and capacity to leverage online information manipulation in the context of COVID-19, where we saw a new convergence of Chinese, Russian and Iranian narratives.
- Second, we have reduced technical capacity to monitor the online environment.
- GAC's Rapid Response Mechanism recently lost access to Twitter's Application Programming Interface (API), which is the primary way RRM Canada obtained structured open source data from the platform.
- Twitter cut off [redacted] our access [redacted], claiming no government should have access to their API for the purpose of identifying foreign disinformation.
- Facebook continues to deny RRM Canada access to its API for the same reason.
- RRM Canada is exploring mitigation measures.
- The analysts are developing tools and methods to conduct web scraping to extract and analyse publicly available data from social media platforms and web sites, working closely with technical experts across the Government of Canada, including at the research team at the Communications Security Establishment, while working with the Department of Justice and the Office of the Privacy

Date [APG]
BPTS #

Commissioner to ensure compliance with applicable domestic and international laws. There is no Government of Canada policy on scraping.

- They are also concluding open contracts with trusted non-government partners to strengthen the capacity of civil society to monitor the online space for foreign state sponsored information manipulation and to support and complement RRM Canada's efforts.
- Both initiatives will take time, especially the former, and may slow down RRM Canada's real time assessment capacity leveraged during the 2019 election. However, in the longer term, we anticipate that the self-sufficiency and flexibility afforded by fit-for-purpose tools and methods developed in house will support our mandate better.
- We are also exploring joined-up advocacy vis-à-vis the platforms but timing will be important, as we would like to ensure any engagement is not coloured by the current US election context.

Ongoing challenge of determining impact of threats to democracy online

- As we saw in the last election, we cannot determine the impact of activity in the online information space the same way we might with cyber or human activity.
- First, it is almost impossible to attribute disinformation online with high certainty. Often times, attribution, if possible at all, is a long process – much longer than the writ period.
- Second, it is almost impossible to determine the impact of disinformation. There is no way to calculate how many Canadians have been exposed to the disinformation nor to what extent it affects their voting intentions.
- By attempting to debunk disinformation, media or others may inadvertently amplify the same disinformation, giving it even great profile.

Protecting Democracy 2.0

- There is a great deal of overlap between what is proposed in this deck and what will be proposed in the Hostile Activity by State Actors (HASA) deck that goes forward later this fall. We should ensure that the two complementary processes are consistent and cross referenced.
- Assume we will be engaging social media companies once again and, in doing so, data transparency should be front of mind. GAC looks forward to working with PCO in this respect.

Context

Previous Interactions:

- The Panel of Five met in advance of and during the writ period of the 2019 Federal Election.

Key Issues:

- In the context of COVID-19, the world is facing an "infodemic" – an overabundance of information, some accurate, some not – that can make it hard to identify reliable information. A combination of misinformation (erroneous) and disinformation (deliberate), propagated by both state and non-state actors, is polluting the information environment, spreading at unprecedented rates online
- The tactics that hostile states employ are constantly evolving. State actors are leveraging covert activities in support of overt information dissemination. They are also leveraging ideologically motivated fringe narratives and conspiracies to polarise societies and undermine trust in democratically elected governments. These tactics are challenging the conceptual and methodological frameworks that guide foreign policy responses as they blur the distinctions between influence *versus* interference, covert *versus* overt, domestic *versus* foreign and state *versus* non-state hostile activity.
-
- Canada has led the G7 Rapid Response Mechanism (RRM) to identify and respond to foreign threats to democracy since leaders committed to its creation in 2018. Canada has leveraged its leadership

[APG]

of the G7 RRM to detect and share information about disinformation online among G7 and likeminded partners, including during the COVID-19 pandemic, when disinformation became a top-of-mind issue. To do this, our support unit, which we call RRM Canada, has used open source data analytics.

- This data analytics capacity has grown increasingly constrained in recent months. The primary reason is a sudden and unforeseen denial of sanctioned access to data generated on social media platforms. By sanctioned access we mean access that has been explicitly granted by social media platforms, usually by allowing third party commercial providers to access the platforms' Application Programming Interface (API). Social media platforms' terms of service and decision-making on access to their APIs are business decisions, which do not have to consider national security or national interest.
- This threatens to limit RRM Canada's ability to support whole-of-government efforts aimed at safeguarding Canadian elections.
- GAC is considering two mitigating measures. We plan to conduct web scraping (technique that allows analysts to extract large amounts of publicly available data from social media platforms or web sites saved to a local file or database for analysis without having to use the social media platforms' APIs) from social media platforms and web sites, including Twitter and Facebook, while concurrently completing our Privacy Impact Assessment in consultation with the Department of Justice and the Office of the Privacy Commissioner. This will require the continued development of in-house tools, including in collaboration with other government and non-government partners, in order to scrape effectively. Development of in-house fit-for purpose tools to counter information manipulation by foreign malign actors online will likely serve the Government of Canada well in the longer term, though it may slow down RRM Canada assessments in the shorter term. In this respect, the RRM Canada team will also continue to be a leader in experimentation and innovation at the Department.
- Second, we plan to conclude paid contracts with trusted non-government partners, such as the Atlantic Council's Digital Forensics Lab, Graphika and the Australian Strategic Policy Institute, to strengthen the capacity of civil society to monitor the online space for foreign state sponsored information manipulation and to support and complement RRM Canada's efforts. We have identified these potential partners based on our threat assessment, the gaps in our own analysis, and these organisations' comparative strengths (e.g., in-depth knowledge of Twitter, Facebook, Chinese social media platforms and Persian information environment). This arrangement will complement –not replace – RRM Canada's independent data collection and analysis in support of national security imperatives.
- PCO Democratic Institutions is leading a Protecting Democracy 2.0 initiative that builds on the Government of Canada's successful effort to safeguard the 2019 federal election and lessons learned. This initiative is meant to be broader and enduring, aiming to protect Canada's democracy writ large and not simply the next federal election. As such, there is a lot of overlap with ongoing Government of Canada work, including Public Safety's Hostile Activity by State Actors (HASA) strategy and Heritage Canada's work on platform governance. s. 39 - Cabinet Confidence

s. 39 - Cabinet Confidence

Author's name/division/tel.: Gallit Dobner/IOL
Consulted divisions/departments: Nil
Approving ADM: IFM
Name and symbol of departmental officer attending/tel.: NA

[APG]