SECRET//CEO

Speaking Points for EC Brief

The Security and Intelligence Threats to Elections (SITE) Task Force brings together operational leads and experts from CSE, CSIS, GAC and RCMP with the aim of improving awareness, collection, coordination and action in countering Foreign Interference in Canada's federal election.

- Complementary set of skills, knowledge, experience
- Been doing this since 2018 – already lived through one election – well-oiled

Prep

- **Review of key threat actors** – understand intent and capability (what they can do from afar; here in Canada – HIGH, MEDIUM, LOW – PRC, RU, IN, IR, PK),
- **Engagement** with partners is crucial
  - discussions with US ODNI – lessons learned
  - Engagement with broader 5EYE community on threat actors
  - a review of key lessons learned from GE43 with domestic partners (including Jim Judd, Taylor Owens of McGill, and Emerson Brooking of DFR Lab);
  - a discussion of new tactics and trends in digital and cyber threats to elections with international partners (including the Institute for Strategic Dialogue and the Australian Strategic Policy Institute)

  Review of our own internal protocols for communication/engagement/response

What is different?

- FI is better understood; we look at the issue on an ongoing basis, outside the election cycle
- Increased efforts – both CSIS and CSE
- GAC/RRM have broadened toolsets and partnerships to look at online information space; increase analytic capacity
- RCMP awareness of FI to enable better information flow from across country to HQ; centralizing processes

We are in a better position than we were, but challenges remain – blending of foreign and domestic actors online; speed of information flow online; difficulty of determining the impact of actions

Threats

Executive Summary of the Threat Environment

- (S//CEO) On balance, the Security Intelligence Threats to Elections Task Force (SITE TF) assesses that Canada's electoral systems and processes remain resilient to the current level of foreign interference (FI), as was evidenced by the assessed low impact of these activities in the 2019 federal election.
- (S//CEO) As COVID-related social and political restrictions begin to ameliorate, hostile foreign state HUMINT operations will likely increase.
- (S//CEO) PRC remains our biggest concern.

- (S//CEO) Other state actors, namely, India, Russia have not yet demonstrated a significant threat to the election process.
- (S//CEO) While many diplomatic activities are consistent with international practices and influence-based approaches to foreign relations, in some grey-zone areas, the accumulation of influence activities over time can shift into covert efforts that lack transparency.

The Information Environment

(U) Since resuming monitoring and monthly trend reporting in December of 2020, RRM Canada has not observed any significant indicators of foreign state sponsored interference targeting the Canadian digital information ecosystem.

(U) Moreover, recent foreign non-state campaigns continue to demonstrate how actors – even with limited resources – can impact the Canadian online information space. Canada has been the target of a campaign by student activists in India aimed at hastening the processes to grant student visas. Accounts promoting content associated with these campaigns have employed automation and other inauthentic techniques to amplify their messages at times; but we do not assess these campaigns to be state-sponsored or either coercive or clandestine.

Threat Actors

People's Republic of China (PRC)

(TS//CEO) The PRC remains the most significant FI threat to Canadian interests. The sophistication and intensity of FI activities, its broad spectrum of targets and methods, outpaces other hostile state actors.

(S//CEO) The PRC is highly capable and motivated against Canada, and acts in a sophisticated, pervasive and persistent manner in carrying out FI activities against all levels of Canadian government and civil society. PRC FI threat actors are pragmatic and tend to pursue paths of least resistance. Their activities often transcend political party lines, take place over several years, and may involve supporting many candidates who promote pro PRC views. Accumulation of activities

(S//CEO) The PRC continues its efforts to cultivate relationships with current MPs and influence their views on issues of strategic importance to the PRC.

The PRC is also interested in individuals who are viewed as 'pro-PRC' or 'neutral in key areas (regardless of ethnic background or riding association), or do not openly oppose viewpoints important to the PRC.

(S//CEO)

PRC FI threat actors have begun to reassert themselves as Canada normalizes and public officials increasingly discuss issues of concern to the PRC.

(S//CEO) This short-term reduction in activity does not appear to have affected the PRC's approach in the digital realm. There has been a significant increase by PRC cyber actors targeting Canada, and the PRC is increasingly engaging in online 'disinformation' efforts in areas such as COVID-19, vaccines, Hong Kong, and Xinjiang

(S//CEO) More broadly, the PRC looks to sway current and former Canadian politicians, political parties, and ethnic groups on issues such as Hong Kong, Taiwan, and Tibet. The aim was to win over the majority of Canadian legislators and exert pressure on local Chinese community leaders and prominent figures in electoral ridings with large Chinese-Canadian populations.

India

(S//CEO) Indian officials — — continue to conduct FI activities in Canada, both directly and through their Canadian proxies, primarily against Canadian politicians, Canadian democratic processes, and against the Indo-Canadian diaspora community. India's intent in conducting this FI is two-fold. First, it seeks to promote a positive image of India within the Canadian political environment and in ethnic media, thereby furthering India's interests in Canada. Second, Indian officials seek to counter any perceived threats to India from within Canada, such as those stemming from Canada-based Khalistani extremists.

Russia

(S//CEO) Russia has focused its FI activities globally on discrediting democratic institutions and processes, with an ultimate goal of destabilizing or delegitimizing democratic states. Russia has the capability to engage in FI activities against Canada. However, it lacks the intent as Canada is not perceived as an existential threat to Russia in the same way as the U.S. (Russia's 'main adversary'). Russia does not prefer a particular Canadian political party or leader through which Russian FI could be directed. The Kremlin likely assesses that major Canadian federal parties do not differ significantly in their stance toward Russia.

(S//REL TO CAN,) The primary target for Russian disinformation programs tends to be communities within Russia or its 'Near Abroad', though the capabilities and tactics used can be easily pivoted to target the west particularly to exploit social 'wedge' issues that gain momentum.

(S//CEO) As an example, a recent Russia Today opinion article has used revelations of indigenous child deaths in residential schools as an example of western hypocrisy and moral exceptionalism. Although this is not necessarily disinformation, the article is an example of Russian state media influence designed to amplify awareness of societal friction in a western democracy.

(S//CEO) Russian cyber actors remain active, targeting a wide range of global victims through known vulnerabilities in hardware and software. None of the observed activities appear to be focused specifically on Canada's democratic processes, but rather form part of broader and ongoing cyber espionage activities.

Iran

(S//CEO) Iran also targets dissidents and other critics of Iran's regime, and as such, targets individuals deemed to be a threat to the Iranian domestic political status-quo.

SECRET//CEO

Pakistan

Ideologically Motivated Violent Extremism

(S//CEO) There is no intelligence indicating that IMVE is a threat to Canada's elections.

(S//CEO) Within the IMVE milieu, a federal election provides an opportunity, particularly for those holding anti-authority views, to promote conspiracy theories and other extreme narratives including: government corruption, COVID-related restrictions and mandatory vaccinations, and, control of Canadian economy and mainstream media by international forces (often thinly-veiled anti-Semitic conspiracy theories). Others focus more on the loss of 'traditional values' and the perceived negative influences of immigration (in particular as a result of immigrants fleeing from Afghanistan).

(S//CEO) More recently, online discussions have raised concerns over the possibility of mask requirements at polling stations. Canadian conspiracy theorists could focus on the perceived illegitimacy of the election outcome ('Stop of Steal') especially if the results are in doubt or there is a delay in ballot counting. Of note, social media monitoring conducted by Elections Canada has observed a notable reaction to the Chief Electoral Officer's press conference on 18 August, and particularly his remarks that masks (as protection from COVID-19) may be required by voters to access polls depending on regional public health guidance. The volume of daily online rhetoric calling for Canadians to act against this policy on principle (i.e. access to democratic rights) is on a steady incline.

SECRET//CEO

(S//CEO) Extreme and polarizing narratives regarding Canadian elections do not usually manifest themselves as acts of violent criminal behaviour, they have the potential to undermine the fabric of Canadian society – including democratic processes.