PROTECTED B
April 2021

APRIL 2021

SITE TF UPDATE TO EC EXCOM

SITE STATUS UPDATE AND SUMMARY OF FOREIGN INTERFERENCE THREATS TO CANADIAN DEMOCRATIC INSTITUTIONS - 2021

SITE TF Status Update

- (PB) SITE TF remains focused on Foreign Interference (FI) threats to Federal elections (re-affirmed at DM-level discussions in December). This ensures that SITE TF has a clear mission focus, and provides continuity of the model successfully used during GE43.

- (U) SITE TF continues to meet (virtually) on a weekly basis, monitoring the threat landscape, producing reports and engaging with key domestic stakeholders and allies, as it prepares for a state of readiness for a Spring election (in line with Elections Canada).

- (PB) SITE has also held several in-person meetings to review foundational documents, including:

    - Threat Coverage Review: Coverage and collection against threat actors that have been identified as posing the most significant threats to our electoral processes (Includes the usual state actors, but also IMVE as a theme, following recent events in the US). This review will help steer and refine collection efforts, in order to support better situational awareness and intelligence sharing on key threats.
    - Internal Communications Protocols: To ensure SITE is well-positioned to coordinate and communicate operational responses during the writ period.
    - Threat Categorization and Response Matrix: To ensures that all SITE members have a consistent understanding of how to triage incoming threat information and to facilitate quick decision-making and identification of leads during peak operational periods (i.e. during the writ).

- (U) Partner engagement has also been at the forefront of our efforts. SITE TF has held a series of workshops with key allies to ensure that the lessons learned from GE43 are remembered, shared and applied to efforts moving forward. These included:
    - 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); and,
    - A classified discussion with FVEY partners on elections lessons learned (including ODNI).

- (U) Lastly, SITE TF will hold a classified deep dive session with the US Elections Security Group on 15 April to review, in detail, the USIC's most recent experience dealing with foreign threats to the US 2020 Elections.

Executive Summary of the Threat Environment

- (PB) SITE has no intelligence at this time indicating that any hostile states are planning interference campaigns specifically targeting Canadian electoral processes.

- (PB) On balance, SITE assesses that Canada's electoral systems and processes remain resilient to the current level of FI, as was evidenced by the assessed low impact of these activities in the last election.

- (U) There has been no significant shift in adversary behavior with regard to Canadian democratic processes. Though COVID-related restrictions have limited some FI activities (person-to-person), it has also created additional opportunities for cyber activities and online disinformation campaigns.

The Information Environment

(U) GAC/RRM Canada produces a monthly trends report summarizing findings from research and analysis aimed at detecting foreign interference in the Canadian digital information ecosystem in support of work with SITE TF. In February, RRM Canada did not observe any significant indicator of foreign interference, including with respect to the Canada-led Statement against Arbitrary Detention and parliamentary vote on Uighur Genocide. However, partner reporting indicates that covert and inauthentic social media campaigns aimed at undermining politicians and organizations critical of China's actions in Xinjiang are underway. Partner reporting also indicates that a number of influencers, media outlets and journalists supporting India's ruling party worked in concert, likely employing covert or automated accounts, to target Canadian activities on social media. This serves to remind us that Canada, while traditionally not a primary target, is not immune to foreign state sponsored disinformation.

Threat Actor Targets, Methods and Intent

(U) State adversaries use a variety of means to interfere in Canadian democratic process, aiming their efforts at a range of targets, including politicians, specific diasporas and the broader Canadian public. Often, state adversaries look to cultivate relationships with current MPs in order influence their views on issues of strategic importance. Frequently, such efforts are aimed at MPs from particular ethnic backgrounds and/or who represent ridings with a significant diaspora community. It is important to note that FI activities may target all levels of government – not just federal – and often transcends political party lines and takes place over a period of several years. This ensures that levers of influence exist at multiple levels of government, which can be used at the time and choosing suitable to the adversary.

(U) Diaspora communities are frequently targeted either directly via Canadian proxies or via specific native-language media. Sometimes this is with a view to ensure that regime maintains influence over the behaviors and views of diaspora communities; in other cases, they are targeted in order to counter any perceived threats

to the adversary state from within Canada, such as those stemming from Canada-based oppositionists or dissidents.

(U) International students and student/campus associations are another vehicle for influence and interference efforts, providing adversary states with access to a ready-made network for messaging and other activities. These groups are mobilized, sometimes coercively, to promote regime agendas via marches, protests, flash-mobs or the organization of petitions and social media campaigns.

(U) Outside of native language media platforms, the broader Canadian public is also subject to state adversary FI efforts through the creation, copying or promotion of online content that mirrors or is sympathetic to adversary government narratives, or seeks to stoke divisive social issues. Increasingly, state adversaries are creating fake online personas to amplify official state accounts in order to increase the visibility of messaging.

(U) Adversary intent varies significantly and typically fall into the following categories:

- To support, in a clandestine and deceptive manner, as many candidates as possible who either seem to be receptive to or actively promote viewpoints beneficial to the adversary state.
- To seek to promote a positive image of the adversary state within the Canadian political environment
- To discredit democratic institutions and processes, with an ultimate goal of destabilising or delegitimising democratic states.

(U) While some state clearly have the capability to engage in FI activities against Canada, they lack the intent, as Canada may not be perceived as key threat or adversary when compared to the US. In some cases, the effort is not worth the reward, as there are no significant differences between Canadian federal parties in their stance toward particular adversary states.

Ideologically Motivated Violent Extremism (IMVE)

(U) Given the recent issues in the US, culminating in the riots on Capitol Hill in January of this year, SITE TF has added IMVE to the list of issues and actors of interest. At present, there is no indication that IMVE pose a threat to Canada's elections. However, there is an increased extreme IMVE narrative opposed to COVID-19 restrictions and a range of perceived grievances focused on Canadian politicians (at every level of governance) and other state representatives including law enforcement officials and judges. As of April 2021, it is assessed that IMVE threat actors in the Canadian context will not be concerned with the next Canadian federal election until it is called.

Foreign Threats to the 2020 US Federal Elections

(U) Learning from the experiences of our partners is a critical aspect of SITE TF's work, as adversary behaviours evolve over time; we look to learn from our allies and their most recent knowledge and experiences, so that we may modify (where necessary) our own efforts. On 15 March the National Intelligence Council released the USIC's Assessment of Foreign Threats to the 2020 US Federal Elections. The following key points offer unique insight into the US experience, but also provide great insight into adversary capabilities and intent.

(U) The USIC definition of Election Influence includes overt and covert efforts by foreign governments or actors acting as agents of foreign governments intended to affect directly or indirectly a US election; Election

PROTECTED B
April 2021

Interference is a subset of election influence activities targeting the technical aspects of the election, including voter registration, casting and counting ballots. [1]

(U) Key Takeaways from US 2020 Federal Election:

- There were no indications that any foreign actor attempted to alter any technical aspect of the voting process in the 2020 US elections, including voter registration, casting ballots, vote tabulation, or reporting results.
- The USIC assesses that President Putin authorized, and a range of Russian government organizations conducted, influence operations aimed at denigrating President Biden's candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US. Unlike in 2016, the USIC did not observe persistent Russian cyber efforts to gain access to election infrastructure. A key strategy of Moscow's strategy this election cycle was its use of proxies linked to Russian intelligence to push influence narratives – including misleading or unsubstantiated allegations against President Biden – to US media organizations, US officials, and prominent US individuals, including some close to former President Trump and his administration.
- The USIC assess that Iran carried out a multi-pronged covert influence campaign intended to undercut former President Trump's reelection process – though without directly promoting his rivals – undermine public confidence in the electoral process and US institutions, and sow division and exacerbate societal tensions in the US.
- The USIC assess that China did not deploy interference efforts and considered but did not deploy influence efforts intended to change the outcome of the US Presidential election.
- The USIC assess that a range of additional foreign actors – including Lebanese Hizballah, Cuba, and Venezuela – took some steps to attempt to influence the election.

(U) While not all of these adversaries would take a similar approach in a Canadian context, we can draw out some interesting themes, such as the increased use of online proxies to obfuscate state involvement, and continued efforts to discredit and undermine traditional media. SITE incorporates this analysis into our own work as we continually refine collection efforts and understanding of foreign adversary interference activities.

[1] SITE TF defines foreign interference as *"Activity conducted or supported by a foreign state/actor that is detrimental to Canadian national interests & is covert, deceptive or coercive. Objective is to affect electoral outcomes and/or undermine public confidence in Canadian democratic institutions."* This differs from foreign influence which is overt and can include public diplomacy.