TOP SECRET/[redacted]/CEO

SITE Briefing to P5
2024 03 25

Good afternoon, it is a pleasure to be able to brief you this afternoon.

I am Vanessa Lloyd, Deputy Director Operations at the Canadian Security Intelligence Service and with me is Bo Basler, Director General of the CSIS Foreign Interference Tiger Team.

We thank you for having us.

We are here today to provide you with an updated threat briefing covering the SITE TF observations of foreign threat actor's intentions and activities relating to foreign interference. Some of you will recall that Bo's threat briefing early January that was followed by a SITE Threat Assessment of Foreign Interference Threats to Canadian Democratic Institutions that was published last month and was shared with this Panel.

Our assessment of the threat remains accurate. Today, we will provide you our key observations on main threat actors as well as speak on trends for the future.

As we continue to monitor activities relating to FI, we note that sophisticated, pervasive and persistent FI activities remain a serious threat to Canada's national security and the integrity of Canada's democratic institutions.

Certain foreign states continue to view FI activities as a normal pattern of behaviour in Canada as they develop important relationships year round that can be leveraged to their advantage during election periods.

It is a misconception to think that foreign interference only occurs during elections and the period leading up to those elections. Foreign interference takes place all year long, at all levels of government and across Canadian civil society. It transcends party lines, ideologies and ethnic backgrounds.

Foreign interference has become a normal pattern of behaviour for certain foreign states and their proxies. It allows them to exert their will on Canada in a manner that is difficult to detect and does not reach thresholds that would result in military conflict.

Further to SITE's latest threat assessment from February, the main FI perpetrators in Canada continue to be the People's Republic of China (PRC), India, Russia and Pakistan.

People's Republic of China

The PRC remains the most active state actor engaging in FI activities in Canada.

The primary goal of PRC FI activities in Canada is to further Party-state interests in a manner that protects and enhances the legitimacy and stability of the CCP domestically and abroad. To achieve these goals, PRC FI actors seek to target and leverage Canadian entities that are perceived to impact important CCP interests.

PRC FI actors are largely pragmatic and tend to pursue paths of least resistance by supporting whichever party or individual is believed to be 'friendliest' to the PRC's interests.

PRC officials continue to conduct FI activities through local networks that are tied to—but not necessarily directed by—PRC officials in Canada on a regular basis. Key components of these FI networks usually include i) PRC officials in Canada ii) leaders of local Chinese Canadian community groups; iii) staff of targeted candidates/elected officials; and, iv) political candidates/officials themselves. This network structure—used for interference at all levels of government—enables an adaptable, resilient approach to extending and enabling PRC covert influence.

A notable evolution in PRC electoral interference efforts is the increased use of social media and internet-based disinformation campaigns. For example, from July to September 2023, multiple Canadian MPs, including the Prime Minister and the Leader of the Opposition, were the subject of a PRC-linked information operation in which they were accused on social media of criminal acts and ethical violations. This so-called 'Spamouflage' campaign included deep fake videos of a Vancouver-based Chinese dissident and CCP critic making inflammatory accusations of the elected officials. While SITE assesses that the posts were ultimately meant to harm the standing of the Chinese dissident, the use of fabricated allegations against Canadian MPs, including digitally manipulated audio and video content, may be a realistic possibility during the next election cycle

Despite the current context of FI in Canada (Public Inquiry), PRC's interest in Canada's democratic processes and elected representatives.

India

Behind the PRC, India continues to be the second-most active state actor engaging in FI activities in Canada.

Indian foreign interference (FI) activities against Canada focus on the Indo-Canadian diaspora and Government of Canada (GC) institutions with the aim of influencing communities to promote a pro-India agenda and a positive image of India in Canada

and as well as monitoring individuals of interest and undermining support for Canadian policies related to issues such as Pakistan and Khalistani extremism.

Indian FI activity is largely focused on the Indo-Canadian diaspora communities; however, the GoI is also opportunistic and will seek to leverage prominent non-Indo-Canadians to achieve India's FI goals, where it suits India's interests.
SITE continues to assess that the GoI seeks to covertly influence Canadian officials at all levels of government to take positions and decisions that are favourable to the GoI.

The GoI its use of disinformation as a key FI tactic against Canada to pressure GC officials to counter all activities the GoI considers anti-India and to support the election of pro-GoI candidates and undermine the campaigns of perceived 'anti-India' candidates.

-
-
- GoI remains interested in supporting Canadian politicians who endorse pro-India views, and countering politicians deemed detrimental to India's interests. Attempting to influence Canadian elections, nomination races, etc. is one of the ways the (Hindu-centric) GoI gears Canadian policy and messaging toward India's interests, which, conversely, includes countering the influence of Sikhs in Canadian politics. (S)

Russia

Next, included among the top FI threat actors is Russia. The Kremlin's long-term goals for FI, continue to include (i) the removal of sanctions, (ii) weakening Western support for Ukraine, and (iii) confirming Moscow's 'rightful place' within the new international order.

however it has focused its FI activities globally on discrediting democratic institutions and processes, with the ultimate goal of destabilizing or delegitimizing democratic states.

Russian intelligence services (RIS) and other state-linked actors conduct disinformation and information campaigns to achieve Moscow's strategic goals of undermining public faith in Western governments and institutions, sowing discord, stoking fear and anxiety, and weakening social cohesion within Western societies.

Since the full invasion of Ukraine in February 2022, Russian officials have attempted to influence Canadians by (i) casting doubt on the Western narrative on the war, (ii) denouncing and discrediting the GC's support to Ukraine and activities of Ukraine, and, (iii) distracting public opinion from other Russian actions.

A recent report from the from Centre for Democracy & Resilience, GLOBSEC noted that the Kremlin meddled in Slovak parliamentary elections that took place in September 2023 utilizing a range of direct and indirect interventions to influence public opinion. The meddling was encouraged by the public's propensity to believe pro-Kremlin disinformation, the possibility of pro-Kremlin parties forming the government, and the existence of a large network of online sources and individuals willing to amplify and support the Kremlin's narratives.

The Kremlin used a blending of old Russian tactics (use of Kremlin-affiliated outlets) paired with newer ones (information operations, usage of AI-generated content) to attain maximum effect. The long-term public vulnerabilities in Slovakia, combined with strong distrust in institutions and widespread disillusionment were exploited to Russia's benefits in supporting pro-Kremlin governance (elected…).

Pakistan

And the last threat actor I will speak about today is Pakistan.

SITE continues to assess that the overarching aim of Pakistan's FI strategy in Canada is to promote stability in Pakistan and counter India's growing influence. Pakistan conducts a range of FI activities against Canada, which has included attempts to interfere in previous Canadian federal elections (2019), as well as transnational repression of dissidents and support of Khalistan extremists.

Although a second tier FI threat when compared to China or India, Pakistan FI threat actor against Canada particularly given the West's current pivot to the Indo-Pacific, Canada's growing focus on its relations with India,

Looking Ahead

Generative AI as an opportunity for Electoral FI

The example of Slovakia and to some extent the spamouflage campaign illustrates extremely well that current advancements in generative-Artificial Intelligence have significantly enhanced electoral interference opportunities. This results in an increased ability to create and control narratives, shape public opinion and to discredit factual information. In effect, it is possible to overload the information sphere so that it becomes difficult for citizens to discern what is true and what is false. These technical advances also enhance the capability of threat actors to acquire behavioural data on individuals that can be used to micro-target these individuals or civil groups with precise behavioural messaging. This can take the form of elected officials or public figures saying or doing something they haven't; or fabricating digital representations of human beings providing false "news" content.

The objectives of these actors is to cause citizens to give up on engaging in open democratic discussion or to change their beliefs and thought processes for how they do engage and on what subjects. It also potentially makes it harder for Canadians to trust legitimate online political messaging and may include encouraging portions of civil society to dis-engage from participating in democratic processes like elections.

SITE assess that AI synthetic content generation related to elections will certainly increase in the next two years, as this technology becomes more widely available. As synthetic content generation increases and becomes more widespread, it will almost certainly become more difficult to detect and attribute, making it harder for Canadians to trust online information about politicians or elections.

Cyber threat activities

Cyber threat activity targeting elections has increased worldwide. While state-sponsored cyber threat actors with links to Russia and China continue to conduct most of the attributed cyber threat activity targeting foreign elections, the majority of the cyber activities are unattributed.

In addition, the proliferation of tools and increased connectivity of our society allows for a wider range of actors to participate in FI – with or without explicit state tasking. Cyber threat activity by third parties, such as hacktivists and cybercriminals, or purchasing cyber tools and services from commercial providers and online marketplaces has been

observed and can help foreign adversaries obfuscate their operations. This will make it increasingly difficult to determine which adversaries we're facing.