UNCLASSIFIED

May 29, 2023

SITE TF Briefing to Unclassified Political Parties

INTRODUCTION TO SITE

The Security and Intelligence Threats to Elections Task Force (SITE TF) consists of members from the Communications Security Establishment, the Canadian Security Intelligence Service, Global Affairs Canada, and the Royal Canadian Mounted Police. SITE TF was established in 2018 as part of the Government of Canada's efforts to safeguard Canada's democratic processes from foreign interference (FI).

SITE TF defines FI as: "activity conducted or supported by a foreign state/actor that is detrimental to Canadian national interests and is clandestine, deceptive or involves a threat to a person."

The key element here is that it is clandestine, deceptive, or involves a threat to a person.

SITE TF Mandate

- To provide a clear point of engagement with the security and intelligence community for Government partners engaged in related work.
- To review and focus intelligence collection, assessment, and open-source analysis related to foreign interference in Canada's democratic process in a coordinated manner.
- To provide situational awareness for Government partners, senior public servants, and other relevant partners.
- To promote the use of intelligence, assessment, and open-source information analysis in the protection of democratic processes through sharing with partners or, when respective mandates permit, take action to mitigate the threat.

While I understand that there has been a lot of recent reporting on FI in the media, this briefing will allow you to hear about FI directly from the security and intelligence community.

I would like to turn to each of my SITE colleagues to say a word on the roles and responsibilities of their respective agencies bring to the Task Force. I will begin with CSE:

CSE

GAC (G7 Rapid Response Mechanism)

RCMP (National Security)

CSIS' Role on SITE

- CSIS investigates threats which may, on reasonable grounds, be suspected of posing a threat to the security of Canada (such as foreign interference) and advises the GoC. We collect intelligence on those threats using a variety of investigative methods. CSIS has the authority, in certain circumstances, to take reasonable and proportionate measures to reduce the threats we detect. However, CSIS is not a law enforcement agency like a police force or the RCMP. We have no authority to arrest or detain people.

- CSIS uses its full authorities under CSIS Act to investigate allegations of interference by foreign states that would undermine Canada's democratic institutions, threaten the lives and well being of Canadians, or intimidate Canadian communities.

- During an electoral period, as a core member of SITE TF, CSIS collects information about foreign interference and provides advice, intelligence reporting and assessments to the GoC about these activities.

- At CSIS, accountability is at the centre of everything we do. The National Security and Intelligence Review Agency (NSIRA) reviews all our activities. We are subject to judicial oversight. For example, a warrant from the Federal Court is required for any intrusive investigative measure we use. We are also subject to annual review from the National Security and Intelligence Committee of Parliamentarians (NSICOP) on foreign interference.

What does foreign interference look like?

- Foreign interference is not the normal diplomatic and public relations activity that is carried out by foreign states to influence policy outcomes. Those activities, when they take place overtly, are acceptable activities in Canada – even when conducted vigorously. They are not foreign interference. Foreign interference activities are different. They cross a line. They attempt to undermine our democratic processes or threaten our citizens in a covert and clandestine manner.

- The most important step you can take is to be aware that you, your staff and elected officials are of immediate and constant interest to certain hostile state actors seeking to interfere in Canada's democratic and electoral institutions and processes. You should also be aware of how they target elected officials and their staff as well as the tradecraft they use.

- CSIS released a public report on Foreign Interference Threats to Canada's Democratic Process. If you have not already done so, I invite you to consult it. The website link will be shared with you.

- A section of this report serves to inform the public of the techniques foreign states use to conduct foreign interference. They include from elicitation, cultivation, coercion, illicit and corrupt financing, cyber attacks, as well as disinformation and espionage.

Elicitation is when a targeted individual is manipulated into sharing valuable information through a casual conversation.

  - For example, a threat actor could knowingly seek to provide someone with incorrect information, in the hope that the person will correct them. A threat actor may also share some form of sensitive information with the individual in the hopes that the individual will do the same – a technique referred to as the "give to get" principle.

Cultivation: Effective threat actors seek to build long-lasting, deep, and even romantic relationships with targets.

  - These relationships enable the manipulation of targets when required, for example, through requests for inappropriate and special "favours".

  - Establishing a relationship first comes via cultivation, all while the threat actor's affiliation to a foreign state is not readily known. Shared interests and innocuous social gatherings are often leveraged for cultivation, and it begins with a simple introduction with the end goal of recruitment over time.

Coercion such as blackmail and threats are two of the most aggressive types of recruitment and coercion.

- If a threat actor acquires compromising or otherwise embarrassing details about a target's life, they can seek to blackmail the person. Sometimes, blackmail or threats may occur after a long period of cultivation and relationship-building. A threat actor may also attempt to put someone in a compromising situation, just to blackmail the person later.

- Threat actors may also use covert operations, such as intrusions, to steal or copy sensitive information and later use that information to blackmail or threaten the individual.

Illicit and corrupt financing are inducements that may occur innocuously via a simple request for a favour.

- For example, a threat actor may ask a target to "pay someone back" or relay money to a third party on their behalf.

- Political parties and candidates may also receive funds (e.g., donations) seemingly from a Canadian, though this may have originated from a foreign threat actor.

Cyber attacks: As mentioned by my CSE colleague. Threat actors can compromise electronic devices through a range of means. Socially-engineered emails (i.e., spear-phishing emails) can trick the recipient into clicking a specific link thereby sharing details about their devices, or can potentially introduce harmful malware into their systems.

- These cyber attacks enable threat actors to collect potentially useful information (e.g., voter data, compromising information about a candidate) that can be used in a foreign influenced operation.

Disinformation: As mentioned by my GAC colleague. Threat actors can manipulate social media to spread disinformation, amplify a particular message, or provoke users (i.e., "troll" users) when appropriate to serve their interests.

- A growing number of foreign states have built and deployed programs dedicated to undertaking online influence as part of their daily business. These online influence campaigns attempt to change voter opinions, civil discourse, policymakers' choices, government relationships, the reputation of politicians and countries, and sow confusion and distrust in Canadian democratic processes and institutions.

Espionage: While distinct threats, foreign interference and espionage are often used together by foreign actors to further their goals.

- For instance, information collected or stolen through espionage can be very useful in planning and carrying out a foreign influence or public disinformation campaign.

Specific States

- The People's Republic of China (PRC) is by far the most active state due to the scope of its foreign interference activities and the level of resources it expends. Other countries, including Russia, also engage is such activities, but not on the same scale.

- The PRC leverages a vast range of tools in Canada: the United Front Work Department (UFWD), its diplomatic corps and non-government assets such as community groups and trusted contacts

    - The UFWD is an entity of the Chinese Communist Party. Its primary role is to ensure, through its vast network that work that furthers the influence and interests of the CCP is carried out effectively both inside and outside the PRC.

    - The overarching goal of the "United Front Work" is to co-op elites both within and outside of China, and to marginalize and silence those it cannot.

    - While the primary targets of this work are entities from the broader Chinese diaspora, elites from beyond the diaspora are also targets, including academics, media personalities, business people, and politicians and political staffers.

Communities

- Foreign states or their proxies have also threatened and intimidated persons in Canada, including members of Canadian communities, to attempt to influence their opinions and behaviours.

- These states, such as the PRC, may use a combination of their intelligence and security services as well as proxy agents to assist them in conducting various forms of threat activities.

- States may attempt to threaten and intimidate individuals outside their country ostensibly in pursuit of anti-corruption efforts or to bring criminals to justice. These tactics can also be used as cover to silence dissent, pressure political opponents, and instill a general fear of state power, no matter where a person is located.

- To be clear, the threat does not come from the Chinese people, but rather from the Chinese Communist Party and the Government of China.

- In Canada, we know that the PRC regularly targets members of groups from what its calls "the Five Poisons" – Falun Gong, Taiwan, Tibet, Uighur, and pro-democracy movements – that represent perceived challenges to the Chinese Communist Party's stability and legitimacy.

- The PRC attempts to intimidate and silence members of these communities by threatening family members residing in the PRC, or denying visas to those wishing to travel back to visit.

Media

- Both traditional media outlets, such as publications, radio and television programs, and non-traditional media, such as online sources and social media, can be targeted to advance a foreign state's intent.

- Mainstream news outlets, as well as community sources, may also be targeted by foreign states who attempt to shape public opinion, debate, and covertly influence participation in the democratic process.

Current Assessment

- Specifically related to the current By-elections, from the Service's perspective, we have no information indicative of FI.

What is SITE broadly seeing now?

- The greatest strategic threat to Canada's national security comes from hostile activities by foreign states, including the threats posed by China and Russia.

While we focus on protecting our citizens, we bear witness to foreign states leveraging all elements of their state apparatus to advance their national interests at Canada's expense.

- We are also increasingly seeing states leverage media to spread disinformation or run influence campaigns designed to confuse or divide public opinion, interfere in healthy public debate and political discourse, and ultimately create social tensions.

- The current geostrategic environment has emboldened a variety of countries to assert their interests more aggressively through foreign interference. These activities have also become more sophisticated and technology has opened doors to new types of foreign interference.

- Hostile activities by certain state actors, such as the PRC, seek to manipulate and abuse Canada's democratic system to further their own national interests, or to discredit Canada's democratic institutions and erode public confidence.

- Threat actors have sought to clandestinely target politicians, political parties, electoral nomination processes, and media outlets in order to influence the Canadian public and democratic processes.

- Specifically related to the current By-elections, nothing has come to SITE's attention to date that is indicative of potential FI.

What can be done with the information you hear/receive today:

- Improve your awareness and help you to recognize potential risks areas
- Inform your decision-making in your current roles or official capacity
- Assist in opening a 2-way dialogue with the S&I community (i.e. provide indicators as to when members might want to engage for advice and guidance).

If you ever feel like you or your staff are being targeted by a hostile state or state-linked threat actors, please contact us. We are here to help as much as possible, whenever we can.

Information related to foreign interference may be reported to CSIS by contact 1-800-267-7685.

Extra Info:

Academic Institutions

- Some foreign states engage in foreign interference activities that undermine Canadian academia by monitoring the view expressed by students and academics, and in some cases threatening retribution if those views are deemed inappropriate.