Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

Foreign Interference in Canada - General

Issue: What is CSIS' understanding of this threat?

Key Messages

- Foreign Interference is one of the greatest strategic threats to Canada's national security because it undermines Canadian sovereignty, national interests and values.
- Foreign interference is a complex modern threat. States employ foreign interference activities against a range of Canadian interests, including the integrity of our political system and democratic institutions, economy and long-term prosperity, foreign policy and military, social harmony, and fundamental rights and freedoms.
- It is also a national threat. It targets all levels of government as well as communities across Canada.
- Foreign interference activities encompass a range of techniques, including human intelligence operations, the use of state-sponsored or foreign-influenced media, and sophisticated cyber tools.
- This threat activity has long been present in Canada, but its scale, speed, range, and impact have grown as a result of globalization and technology.
- In 2021, CSIS released a public report on Foreign Interference Threats to Canada's Democratic Process. As this report shows, foreign states and their proxies target politicians, political parties, and electoral processes in order to covertly influence Canadian public policy, public opinion and ultimately undermine our democracy and democratic processes.

Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

Foreign Interference Manifestations

Democratic institutions

- Democratic institutions and processes, including elections, are vulnerable and valuable targets for hostile activities by state actors. Canada is not immune to these threat activities. This is not new.

- Hostile activities by certain state actors, such as the Russian Federation and the People's Republic of China, 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.

- For instance, state-sponsored cyber threat actors use computer network operations to interfere with elections.

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.

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.

Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

Techniques Used to Conduct Foreign Interference

- The first and most important step you can take as an elected official is to be aware that you and your staff 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 you and their tradecraft.

- In July 2021, 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.

- 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.

    - How to avoid it: Be discreet, avoid "over-sharing", and assume public conversations are monitored.

Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

- **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.
    - How to avoid it: Be aware and keep track of unnatural social interactions, frequent requests to meet privately, out-of-place introductions or engagements, gifts and offers of all expenses paid travel, and odd attempts to seek employment with your office.
- **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.
    - How to avoid it: Avoid sharing compromising details or personal information with untrusted individuals, both in-person and online. Avoid placing yourself in compromising situations, and seek assistance if someone seeks to threaten or blackmail you.

Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

- **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.
    - How to avoid it: Be aware of inappropriate requests which involve money, and question the source of suspicious donations or “gifts”.
- **Cyber attacks**: 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.
    - How to avoid it: Practice good digital hygiene. Use strong passwords, enable two-factor authentication, don’t use untrusted applications, and don't click on links or open attachments unless you are certain of who sent them and why. Avoid mixing personal and professional devices.

Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

- **Disinformation:** 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.

    - How to avoid it: Be critical of what you are consuming online, careful what you share (or repost from others), and take note of unexpected online interactions.

- **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.

    - How to avoid it: Follow security of information protocols, don't disclose information to individuals who don't have a reason to access it, and be discrete about how you handle sensitive information.

- 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.

Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

Disinformation campaigns

- With regard to state-sponsored disinformation campaigns, CSIS has observed social media being leveraged to spread disinformation or run foreign influenced campaigns designed to confuse or divide public opinion, or interfere in healthy public debate.

- Foreign states attempt to manipulate social media to amplify societal differences, sow discord, and undermine confidence in fundamental government institutions or electoral processes.

- They may use a coordinated approach to amplify a single narrative while also promoting inflammatory content. Foreign states may also use cyber-enabled tracking or surveillance of dissidents, those who challenge their rhetoric, or do not support their interests in Canada.

- Such behaviour can lead to threats or blackmail if the individual fails to cooperate.

- In fulfilling our crucial mandate, CSIS developed publicly available resources on foreign interference, which were published in a range of foreign languages in order to ensure that vulnerable communities can access threat information in their language of choice.

- CSIS continues to engage with Canadian communities, advocacy groups, businesses, industry associations, academic institutions, and all levels of government (federal, provincial/territorial, municipal, and Indigenous) to ensure they are aware of the national security threats facing our country and give them the information they need to protect their interests.

- These efforts are aimed at listening, better understanding the communities that we serve, establishing trusted relationships, and conveying threat-related information to increase awareness and resilience to foreign interference in particular.

Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

Hotlines

- As is common in large, multicultural countries, Canadian communities are subject to clandestine and deceptive manipulation by foreign states. This is foreign interference. CSIS and the RCMP actively investigate this threat to our national security.

- Both the RCMP and CSIS have phone numbers and online reporting mechanisms that are monitored 24/7 for anyone who would like to report a threat to national security, including foreign interference.

- Should individuals ever be concerned for their personal safety and security, it is essential that they contact their local police for immediate action.

- CSIS' tip line is 613-993-9620, toll-free at 1-800-267-7685. The TTY/TDD number is 613-991-9228. The online reporting mechanism is on CSIS' web page under "Reporting National Security Information."

Date:	2023 04 19
Classification:	Unclassified
Agency:	CSIS

Freedom Convoy protests and funding

- During the protests in Ottawa and across Canada last year, CSIS remained committed to continue assessing threats to Canada's national security during the important operational activities underway by law enforcement partners.

- While the right to freedom of expression and peaceful assembly is an important part of our democracy, individuals are not justified in breaking the law or engaging in violence. CSIS supported the City of Ottawa and the enforcement actions being taken by the Ottawa Police Service, and their law enforcement partners.

- On financial reporting, CSIS continued to work within the parameters of the *CSIS Act* to support the Government of Canada in implementing measures that were in effect under the *Emergencies Act*.

- The *Emergencies Act* did not expand CSIS' powers to investigate or take threat reduction measures. CSIS continued to work within the existing authorities of the *CSIS Act*.

- Under the *Emergencies Act*, other designated entities had expanded requirements to report to CSIS certain activities linked to designated persons. CSIS engaged with its financial partners to ensure that disclosures specifically related to its national security mandate.

- With respect to foreign sources of funding, CSIS' mandate is engaged when funds are provided at the direction of or with the support of a foreign state or when those donating the money are doing so to support an act of serious violence or terrorism.

- CSIS did not observe that this had occurred in the context of the Convoy.