FOREIGN INTERFERENCE: THE FUNDAMENTALS

UNCLASSIFIED

Canada

OBJECTIVES

UNCLASSIFIED

1. Raise awareness of foreign interference activities
   - What is it?
   - Related threats

2. Highlight tactics used to carry-out foreign interference activities
   - Common targets and why
   - Techniques of the trade

3. Safeguarding against foreign interference activities
   - Individual responsibilities
   - Government of Canada resources

WHAT IS FOREIGN INTERFERENCE?

UNCLASSIFIED

The *Canadian Security Intelligence Service Act* describes foreign interference as: *"activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person."*

Foreign Interference (FI) is extensive and aggressive activity undertaken by foreign states, typically covert, against Canadians and Canadian institutions, to advance their strategic interests to the detriment of Canada.

- FI differs from normal diplomatic conduct or acceptable foreign state-actor lobbying.
- Active, overt diplomacy/lobbying are a healthy part of democracy. Clandestine or deceptive foreign interference is not.

States conduct FI to further their own strategic national interests, for:

- Strategic, military, intelligence and economic gain;
- regime preservation; or
- discrediting liberal-democratic institutions.

HOW ELSE DO STATES TARGET CANADA?

UNCLASSIFIED

Espionage continues to present a grave threat to Canada's prosperity and national interests.

- Foreign actors seek intellectual property and proprietary information to further their own economic, political or military agendas.
- Sectors including sensitive/emerging technology, energy, and military are targeted.
- Espionage can involve intelligence agents, insiders, direct investment, and cyber tools.

FI poses a threat to the integrity of our political system, Canada's democratic institutions, and the rights and freedoms of Canadians.

- Canada is a target of foreign state efforts to interfere with or undermine our democratic processes and institutions. Methods used by foreign states may include:
  - Leverage foreign language and mainstream media to promote foreign agendas;
  - Influence nomination and campaign outcomes, including with funding; and
  - Manipulate community members to silence dissent or influence election outcomes, including with threats.

WHO DO FOREIGN STATES TARGET?

UNCLASSIFIED

Person-to-person FI remains common practice, perpetrated by:

- Foreign diplomats;
- Intelligence officers; and
- Proxies and individuals purposefully selected (both witting and unwitting).

Targets of foreign states include:

- the general population and specific communities;
- voters;
- political parties;
- candidates;
- parliamentarians and their paid and volunteer staff; and,
- electoral processes.

FI has been observed at all levels of government in Canada: municipal, provincial and federal.

WHAT TECHNIQUES ARE USED?

Techniques employed – both in Canada and overseas – can include:

- Elicitation;
- Cultivation;
- Intrusion;
- Blackmailing/threatening;
- Financing (including contributions not overtly linked to a foreign state);
- The 'Honey Trap‘; and
- Eavesdropping.

Foreign states may also use cyber tools to conduct clandestine interference activities.

- Employing spear phishing and other malicious cyber intrusions to gain access to private information for leverage or to discredit political actors.
- Manipulating online information, often on social media using cyber tools, in order to influence voters’ opinions and behaviour.

WHY ARE PARLIAMENTARIANS AT RISK?

UNCLASSIFIED

Government and parliamentarians are targeted because of their access to privileged information, contacts and decision-makers.

Foreign states or their proxies may target you, directly or indirectly, because:

- You possess information they want;
- You have access to information they want; or
- You are in a position to influence government policy.

Foreign states may also seek to discredit you to further their strategic agendas.

WHAT YOU CAN DO

UNCLASSIFIED

1) Remain vigilant

- Use discretion and assume that conversations in public places may be overheard. Communications on public transportation, and at cafes, restaurants and bars are particularly vulnerable.
- What you share online – e.g. through social media, in comments on other people's posts – can be mined by individuals seeking to target you.
- Exercise caution in the receipt and use of gifts, especially electronic ones that can plug into your computer.
- Be wary of approaches from strangers, particularly when their interest pertains to your work or area of interest. Even seemingly benign information can be of interest to foreign intelligence agencies.
- Be suspicious of unsolicited offers of assistance or information, or excessive flattery that seeks to appeal to your ego.

WHAT YOU CAN DO

UNCLASSIFIED

2) Protect classified and privileged information

- Store sensitive or classified information in appropriately secured cabinets.
- Exercise care in carrying information; classified information should be carried in a secure briefcase.
- Send information through secure channels in advance of travel.
- Travelling with clean electronics minimizes the loss and risk if a device is lost, stolen, hacked or copied.

WHAT YOU CAN DO

3) Protect your devices

- Use strong passwords for devices, enable two-factor authentication, secure mobile devices with passcodes or other identification (fingerprint/face recognition).
- Regularly patch devices and computers, maintaining up-to-date operating systems and applications.
- Never click on links or open attachments unless you are certain who sent them and why.
- Avoid using public wifi and, if you must, set the network location to “Public”.
- Disable features not in use, such as GPS, Bluetooth or Wi-Fi.
- Do not use “Remember Me” features for passwords on websites/mobile applications.

THE BOTTOM LINE

UNCLASSIFIED

- Foreign states continue to engage in aggressive FI in Canada to advance their own strategic interests.
- Canada's democratic system is the principal target of foreign states seeking to advance their political, economic and security agendas by influencing government policies and decisions.
- Individuals with perceived access or influence over decision-making, at the federal, provincial and municipal levels, may be targeted.
- FI may be conducted by individuals in Canada operating on behalf of a foreign state through person-to-person contact.
- Cyber tools provide another powerful means to influence the electorate, political outcomes and even, potentially, the electoral process.
- Knowledge, preparation, vigilance, discretion and robust cyber security are important steps to mitigate against the threat.

RESOURCES

Canadian Centre for Cyber Security

1-833-CYBER-88

www.cyber.gc.ca/democracy - provides practical ways for Parliamentarians, parties and candidates to protect against cyber threats.

CSIS (national security threats)

613-993-9620

RCMP (criminal activity)

Contact your local federal policing operations unit

EXERCISE: SCENARIO #1

UNCLASSIFIED

Scenario:

A volunteer in your riding association office clicks on a phishing link in an email and critical party information (donor database and voter information database) is locked with ransomware. A ransom is demanded from the party to unblock the Party networks. The hacker threatens to publicly release Party-specific donor database information, which includes the personal information of donors. As a sign of his intentions, the hacker releases some sensitive Party emails.

Questions:

- What immediate action do you take?
- What steps should be taken to avoid this from happening in the future?

EXERCISE: SCENARIO #2

UNCLASSIFIED

Scenario:

An incoming foreign delegation presents you with a gift following a productive meeting. The gift includes a plaque and a USB-enabled coffee mug warmer. Your administrative assistant hangs the plaque in your office and plugs the coffee mug warmer into a computer to heat a coffee.

Immediately, your office experiences some network slowdowns. Emails are taking longer to send, and Google Chrome seems to be taking much longer to load. A network scan by House of Commons/Senate IT security discovers that the USB coffee warmer implanted malware on the system and that sensitive documents have been ex-filtrated.

Questions:

- What prevention efforts could have been made to avoid this situation from occurring?
- In this case outline what steps should be taken.

EXERCISE: SCENARIO #3

UNCLASSIFIED

Scenario:

At an embassy cocktail party, you are approached by an official representative from the host country, who suggests that a visit to their country would be an important opportunity to deepen your knowledge of the country and inform your work on the standing committee responsible for international trade. The official indicates that you would be part of a broader Canadian delegation, including representatives from Canadian industry, academia, and other parliamentarians. During the trip, some of the host handlers take a keen interest in your work, asking pointed questions and suggest that there are likely areas where you could work together to advance important mutual priorities.

Questions:

- What concerns are emerging in this scenario?
- How would you respond to the opportunity being presented?

Slide Notes

Slide 4:

Current threat picture:

The Canadian Security Intelligence Service has seen that:
Foreign language and mainstream media in Canada have been used to promote foreign agendas and challenge Canadian interests.
Communities in Canada are targeted by foreign states who try to silence dissent or use them as tools to support their FI activities.
Spear phishing and other malicious cyber intrusions are used to gain access to private information for leverage or to discredit political actors.

Foreign cyber actors use different cyber techniques for interference activities.
Cyber threat actors:
use cyber tools to target the websites, e-mail, social media accounts, and the networks and devices of political parties, candidates, elected officials and their staff in order to extract information for leverage, or to discredit political actors.
could attempt to undermine trust in our elections or suppress voter turnout by altering content on websites, social media accounts, and networks and devices used by Elections Canada.
manipulate online information, often on social media using cyber tools, in order to influence opinions and behaviour.

Slide 9:

The best way to secure information or assets when you travel is to send classified information to your destination via classified email/mail before your departure. Never carry classified documentation.
Using clean electronics ensures that if lost, stolen, hacked, or copied, the loss of information is known, contained, and risk can be accurately assessed.
Pay special attention to security considerations when communicating over non-secure means of communications. Seemingly innocuous details can become intelligence information. Adversaries pay close attention to observables to deduce critical information about your projects, programs, and activities.
Ex: A CBC/Radio Canada investigation was just released regarding the compromise of NDP MP Matthew DUBE' s cellphone, who volunteered for the experiment - discussions and geolocation.
Situational awareness

Slide 10:

The best way to secure information or assets when you travel is to send classified information to your destination via classified email/mail before your departure. Never carry classified documentation.
Using clean electronics ensures that if lost, stolen, hacked, or copied, the loss of information is known, contained, and risk can be accurately assessed.
Pay special attention to security considerations when communicating over non-secure means of communications. Seemingly innocuous details can become intelligence information. Adversaries pay close attention to observables to deduce critical information about your projects, programs, and activities.
Ex: A CBC/Radio Canada investigation was just released regarding the compromise of NDP MP Matthew DUBE' s cellphone, who volunteered for the experiment - discussions and geolocation.
Situational awareness