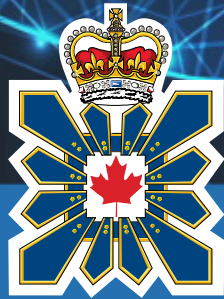




Canadian Security
Intelligence Service

Service canadien du
renseignement de sécurité

UNCLASSIFIED



FOREIGN INTERFERENCE THREATS TO CANADIAN DEMOCRATIC PR

Aussi disponible en français sous le titre : *Menaces d'ingérence étrangère visant les processus démocratiques au Canada*

www.canada.ca

Published July 2021

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Public Safety and Emergency Preparedness, 2021.

Cat. No. PS74-17/2021E-PDF

ISBN: 978-0-660-39625-5

EXECUTIVE SUMMARY

- 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, constitute foreign interference. Examples of foreign interference include attempts to covertly influence, intimidate, manipulate, interfere, corrupt or discredit individuals, organizations and governments to further the interests of a foreign state.
- The Canadian Security Intelligence Service (CSIS) continues to observe steady, and in some cases increasing, foreign interference activity by state actors. Foreign interference directed at our democratic institutions and processes can be effective ways for foreign states to achieve their immediate, medium or long-term strategic objectives. These activities can pose serious threats to Canadians both inside and outside Canada, and threaten Canada's prosperity, strategic interests, social fabric, and national security. Given the nature of today's geopolitical environment, these activities will almost certainly intensify.
- While foreign interference activities can target a range of strategically important political, economic, defence, security, foreign policy and community issues, this report will focus specifically on the foreign interference threat to Canada's democratic process. This report also focuses on CSIS's efforts to counter this threat, although other Government of Canada partners are actively involved in this work.
- Although Canada's electoral system is strong, foreign interference can erode trust and threaten the integrity of our democratic institutions, political system, fundamental rights and freedoms, and ultimately, our sovereignty.
- Foreign interference threats affect all levels of government (federal, provincial, municipal) and target all facets of Canadian society, including civil society, communities, media, voters, political parties, candidates, elected officials and their staff, and elections themselves.
- Foreign states and their proxies use a range of common techniques to further their objectives. This includes human intelligence operations, leveraging state-sponsored or community media, sophisticated cyber tools, and social media. While these techniques are varied and can be difficult to detect, there are indicators that can help increase individual awareness of these threats to avoid becoming a target.
- CSIS is mandated to protect Canada and Canadians against foreign interference, among other threats. To respond to this threat, CSIS works in collaboration with other partners, including the Royal Canadian Mounted Police (RCMP). In addition, CSIS is a core member of the Security and Intelligence Threats to Elections (SITE) Task Force, which coordinates efforts to protect federal elections.
- The nature of foreign interference threats, however, means that all Canadians have a role to play in protecting Canada's democracy and national security, both outside of, and during an election. By raising awareness of these issues, CSIS aims to sensitize Canadians to the threat and help build resilience to protect all that we stand for as a democratic and free Canada.

UNCLASSIFIED



INTRODUCTION

Canada is an open and free democracy with a reputation of being a friendly and welcoming country. Not everyone, however, shares these values. Some foreign states, or their proxies, use deceptive, clandestine or coercive means to advance their strategic interests at the expense of Canada's. This is foreign interference and it is a threat to Canada's national security.

CSIS continues to observe steady, and in some cases increasing, foreign interference by state actors against Canada. Foreign interference targets all facets of Canadian society. One of the key sectors targeted by this activity is Canada's democratic institutions and processes. The purpose of this report is to sensitize Canadians to the nature of foreign interference in this sector and its impact on our democracy. Although Canada's electoral system is strong, foreign interference is a significant threat to the integrity of our democratic institutions, political system, and fundamental rights and freedoms. For instance, certain foreign states and their proxies may use foreign interference to undermine Canada's electoral process, both outside of, and during an election. Such activities may target the Canadian public, media, voters, political parties, candidates, elected officials and their staff, and elections themselves.

As part of its mandate under the *CSIS Act*, CSIS investigates activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. CSIS collects and analyzes information to provide advice to the Government of Canada. It may also take reasonable and proportionate measures to reduce the threats it detects. The threats to national security that CSIS is mandated to investigate include espionage, sabotage, foreign influenced activities, terrorism, and subversion.

Foreign interference activities are persistent, multi-faceted, and target all areas of Canadian society. While CSIS is mandated to investigate this threat, everyone has a role to play in protecting Canada's democracy and national security. Together, we can build resilience to ensure that our communities and institutions are not exploited by foreign state actors, and collectively safeguard our democratic values.

UNCLASSIFIED



WHAT IS FOREIGN INTERFERENCE

“Foreign interference” is a commonly used expression which is also referred to as “foreign influenced activities”. The *CS/SA* Act defines foreign influenced activities 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”. Broadly speaking, foreign interference includes attempts to covertly influence, intimidate, manipulate, interfere, corrupt or discredit individuals, organizations and governments to further the interests of a foreign country. These activities, carried out by both state and non-state actors, are directed at Canadian entities both inside and outside of Canada, and directly threaten national security.

Foreign interference involves foreign states, or persons/entities operating on their behalf, attempting to covertly influence decisions, events or outcomes to better suit their strategic interests. In many cases, clandestine influence operations are meant to deceptively influence Government of Canada policies, officials or democratic processes in support of foreign political agendas.

This activity can include cultivating influential people to sway decision-making, spreading disinformation on social media, and seeking to covertly influence the outcome of elections. These threats can target all levels of government (federal, provincial, municipal) across Canada.

Foreign interference differs from normal diplomatic conduct or acceptable foreign-state actor lobbying. For instance, lawful advocacy is a healthy part of diplomatic relations. Clandestine or deceptive interference by a foreign state to advance its interests are not. States cross a line anytime they, or their representatives in Canada, go beyond diplomacy to conduct activities that attempt to clandestinely or deceptively manipulate Canada’s open democracy and society, including by threats of any kind.

The scale, speed, range, and impact of foreign interference activities in Canada has grown as a result of globalization, technology, and the current geopolitical climate. The changes in how we live our lives in the 21st century have provided foreign states with more opportunities to target individuals in Canada through cyber means, including monitoring and harassment.

WHY CANADA A TARGET?

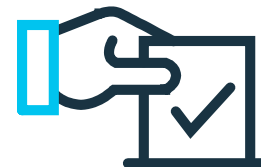
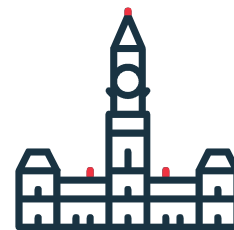
As an open and free democracy with an advanced economy, Canada has long been targeted by foreign states seeking to gain information, covertly influence or leverage individuals and communities to advance their own national interests.



Canada's abundance of natural resources, advanced technology, human talent, and expertise makes it a world leader in many sectors. Canada's close relationship with the United States, its status as a founding member of the North Atlantic Treaty Organization and its participation in a number of multilateral and bilateral defence and trade agreements, as well as the Five Eyes community, has also made it an attractive target for foreign interference. In addition, certain foreign powers are known to leverage Canada's multiculturalism for their own benefit by subjecting Canadian communities to clandestine and deceptive manipulation or threats.



Elections, at any level of government, provide further opportunity for a foreign state to advance its national interests. CSIS has observed persistent and sophisticated state-sponsored threat activity targeting elections for many years now and continues to see a rise in its frequency and sophistication. For instance, CSIS observes 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.



UNCLASSIFIED

WHY DO STATES GAIN FOREIGN INTERFERENCE INFLUENCE THE DEMOCRATIC PROCESSES IN FOREIGN COUNTRIES?

Foreign interference directed at Canada's democratic institutions and processes can be an effective way for a foreign state to achieve its immediate, medium and long-term strategic objectives. The choices that the Government of Canada makes, for example, about military deployments, trade and investment agreements, diplomatic engagements, foreign aid, or immigration policy are of interest to other states. The decisions and policies of provincial and municipal governments are equally important as they determine investments in the economy, infrastructure, resources and the environment, as well as the health and education of citizens and residents. But for some foreign states, the decisions and policy stances of the federal, provincial and municipal governments may negatively affect their core interests. As the world has become ever smaller and more competitive, foreign states seek to leverage all elements of state power to advance their national interests and position themselves in a rapidly evolving geopolitical environment.

Immediate Goals

- Shape narratives around strategic interests (e.g., artificially create perception of support or divisiveness, gain political favour, etc.)
- Covertly influence election outcomes in favour of their preferred candidate or party
- Suppress voter participation
- Reduce public confidence in the outcome of an electoral process

Mid-Term Goals

- Advance strategic priorities that align with their national interests
- Undermine strategic interests of their adversaries
- Discredit democratic institutions
- Erode confidence in democracy

Long-Term Goals

- Achieve economic, intelligence, military, and geopolitical strategic advantage
- Preserve authoritarian regime
- Disrupt the rules-based international order

UNCLASSIFIED

WHERE ARE THE ARGUMENTS FOR FOREIGN INTERFERENCE IN CANADA'S DEMOCRATIC PROCESS?



Canadian Public and Voters

The Canadian public and voters are targeted by foreign interference as they are generally viewed by state actors as vulnerable targets. In particular, elections provide valuable opportunities for state actors to conduct disinformation and interference campaigns; however, such activities are ongoing and are not only observed in the lead-up to, or during, an election.

The targeting and manipulation of diverse Canadian communities are one of the primary means through which states carry out foreign interference activities and undermine Canada's democracy. The impact of this is that communities may fear or resent state-backed or state-linked retribution targeting both individuals in Canada and their loved ones abroad. By exploiting and coercing Canada's communities, foreign states attempt to control messaging that is supportive of Canada's values, policies, or practices; silence dissenting views or opinions of the foreign state or issues that do not support their strategic objectives; and amplify their own favourable messaging. By monitoring and harassing Canada's communities, state actors try to influence public opinion and sow discord. In a democracy where public opinion informs policy development and government decision-making, such influence can alter outcomes and weaken our democratic institutions in the long-term.

State actors may use threats, bribery or blackmail to affect the voting behaviour of individuals inside or outside of communities. Individuals may be threatened or fear reprisal for themselves or their loved ones in Canada or abroad if they fail to comply with publicly supporting a particular candidate or contributing funds to the foreign state's preferred party. While state actors may use coercive techniques to achieve their objectives, they may also use flattery, promise compensation, or appeal to an individual's sense of pride towards another country to elicit the desired behaviour.

Attempts to influence the public are also increasingly observed online, where threat actors have refined their ability to conduct disinformation and foreign interference campaigns. 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

UNCLASSIFIED

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.

When communities in Canada are subjected to threats, harassment, intimidation, or other deceptive means by foreign states that are either seeking to gather support or mute criticism of their policies, these activities constitute a threat to the safety of Canadians and to Canada's security. By aggressively conducting such activities, state actors show disregard for Canadian democratic values and open society.



Elected and Public Officials

Elected and public officials across all levels of government, representing all political parties, are targeted, including: members of Parliament, members of provincial legislatures, municipal officials and representatives of Indigenous governments. Public servants, ministerial and political staff, and others with input into, or influence over, the public policy decision-making process are also targeted by foreign states. State actors may use deceptive means to cultivate a relationship with electoral candidates or their staff in order to covertly obtain information to be used later to their advantage through, for example, threats and blackmail. Alternatively, a state actor may decide to recruit the individual over time in the hopes of greater gains if the individual is elected. After a long period of cultivation there are more opportunities to gain leverage over the official which can be used to pressure the individual into influencing debate and decision-making within government. The individual may also be able to hinder or delay initiatives that are contrary to the foreign state's interest.



Donors, Interest/Lobby Groups and Community Organizations

State actors may also attempt to covertly mobilize others involved in the democratic process. Donors, interest or lobby groups, or community organizations may be used, wittingly or unwittingly, to carry out interference activities that support a foreign state's preferred candidate, or discredit or attack candidates that threaten their interests. For donors, some may have connections to foreign states or be pressured or coerced into making donations to specific candidates. For the candidate receiving the donations, there may be "strings attached" and an expectation that the candidate will act in the state's best interests.

UNCLASSIFIED



Media

Foreign states also threaten Canada's democratic process when they attempt to manipulate Canadian 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. Considering Canada's rich multicultural makeup, foreign states may try to leverage or coerce individuals within communities to help influence to their benefit what is being reported by Canadian media outlets. These individuals may be knowingly or unknowingly acting on behalf or at the behest of a foreign state.

Another way to influence Canada's media outlets is through funding and advertisements. Foreign states may attempt to invest money, pay for advertisements, or sponsor investigative journalism or interviews that help promote their interests. Such activities could result in content advancing a foreign state's interest being communicated to the Canadian public under the guise of independent media. In addition, foreign states may also acquire media outlets in Canada.

Just as damaging is when foreign states attempt to propagate disinformation, promote divisive and inflammatory content, or discredit credible news sources. These activities undermine legitimate public discourse and erode the public's trust in the media, which is a direct attack on democracy.

UNCLASSIFIED

WHAT TECHNIQUES ARE STATES USE TO CONDUCT FOREIGN INTERFERENCE?



Elicitation

- Elicitation results when a targeted person 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, thereby providing the information the threat actor was actually looking for.
- 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.



Cultivation

- Effective threat actors seek to build long-lasting, deep, and even romantic relationships with targeted persons. These relationships enable the manipulation of targets when required, for example, through requests for inappropriate and special “favours”.
- To establish a relationship, the threat actor whose affiliation to a foreign state is not readily known, must first cultivate a target. Cultivation begins with a simple introduction with the end goal of recruitment over time. Shared interests and innocuous social gatherings are often leveraged for cultivation.

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.

UNCLASSIFIED



Coercion

- 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.



Illicit and Corrupt Financing

- Threat actors can use someone as a proxy to conduct illicit financing activities on their behalf.
- Inducements 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: Use strong passwords, enable two-factor authentication, and don't click on links or open attachments unless you are certain of who sent them and why.

UNCLASSIFIED



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.

UNCLASSIFIED

WHAT ARE THE GOVERNMENT OF CANADA AND CSIS DOING TO PROTECT AGAINST FOREIGN INTERFERENCE?

The Government of Canada has a fundamental responsibility to protect Canada's national security and the security of Canadians. It has measures in place to ensure the integrity of our political system, both during and outside of an election. Canada's electoral process is paper-based and there are procedural mechanisms in place to protect against voter fraud, such as having to prove identity and address prior to voting in a federal election. In addition to these safeguards, Elections Canada has a number of other legal, procedural, and IT measures in place that provide very robust protections for Canadian federal elections. The Communications Security Establishment (CSE) also takes measures to prevent cyber threats. At the provincial and territorial level, the Canadian Centre for Cyber Security (Cyber Centre) also provides advice and guidance to election bodies.

CSIS contributes to a whole-of-government approach to protect Canadians from national security threats, including foreign interference. CSIS has longstanding investigations into specific threat actors who are believed to be targeting Canada and Canadians through clandestine, deceptive or threatening means. CSIS advises the Government of Canada of these threats, and is able to take lawful measures under its threat reduction mandate to mitigate threats to the security of Canada.

Foreign interference can manifest through various means, including cyber means. The increasing interconnectedness of the world presents cyber actors with more opportunities than ever to conduct malicious activity. CSIS actively investigates cyber threats and works in collaboration with key partners. While CSIS, CSE, the Cyber Center, the RCMP and other key government partners have distinct and

separate mandates, they share a common goal of keeping Canada, Canadians, and Canadian interests safe and secure online.

In the lead up to the 2019 Federal Election, the SITE Task Force was created to protect Canada's federal election. As an active partner in SITE, CSIS works closely with CSE, the RCMP and Global Affairs Canada to share information on election security and inform decision-making when there are incidents of foreign interference in elections. Now seen as a model for our allies on how different departments can work together to ensure free and fair elections, SITE's efforts continue today.

Canada's democratic institutions and processes are strong and the Government of Canada actively works to ensure their continued protection. However, keeping Canada's democratic institutions, political system, and democracy safe requires a national security-aware population. This means that all citizens need to know about the threats to Canada's democracy and be equipped to protect themselves from foreign interference. We all have a role to play in protecting Canada's democracy.

UNCLASSIFIED



HOW TO REPORT FOREIGN INTERFERENCE

The Government of Canada has mechanisms in place to report foreign interference.

Information related to espionage or foreign interference may be reported to CSIS by contacting 613-993-9620 or 1-800-267-7685, or by completing the web form at www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html.

In addition to their local police, any individual in Canada who is concerned that they are being targeted by state or non-state actors for the purposes of foreign interference should contact the RCMP's National Security Information Network at 1-800-420-5805, or by email at RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca

UNCLASSIFIED



ANNEX E TERMS AND DEFINITIONS

Clandestine or Covert: Activities that are conducted in secret or not out in the open.

Censorship: The suppression of speech, public communication, or information. This may be done on the basis that the information is harmful, obscene, or politically inconvenient depending on perspective.

Coercion: The use of threats, force, or manipulation to compel individuals to act in ways that further their objectives.

Covert Influence: Foreign states who use deception or power to secretly affect, control or manipulate their adversaries to further their own state's objectives.

Cultivation: As part of a long-term recruitment plan, individuals who are in a position of influence, or have knowledge or access to information, are actively sought after. In a process known as cultivation, the individual is groomed for an eventual request or "favour".

Deception: When threat actors cause an individual to believe something that is not true in order to further their objectives.

Discredit: Threat actors may cause others to question or refuse to believe in an individual or something that the individual said or did in order to further their objectives.

Disinformation: The deliberate spread of false or manipulated information with the intent to mislead others.

Interference: Foreign states who use deception or power to secretly hinder or impede their adversaries to further their own state's objectives.


Manipulation: A form of coercion where individuals or information are controlled to shape behaviour, outcomes or decision-making processes.

Misinformation: The spread of false information without the intent to deceive or mislead. This is communication between people that contains incorrect facts.

Propaganda: An organized program of publicity using selective information to propagate a doctrine of belief, often in a misleading or dishonest way.

Proxy: An individual or entity that is not directly linked to a foreign state, but acts on its behalf.

UNCLASSIFIED



Recruitment: Typically after a process of successful cultivation, individuals will be asked to complete a “favour” for a threat actor. Some individuals may be compensated with money, assets, or career progression for assisting the threat actor, while others may not be aware that they have been recruited.

Subversion: Activities that attempt to undermine, overthrow, or destroy the power and authority of an established system or institution.

Threats: A form of coercion where threat actors express their intention to damage an individual's reputation or property, or inflict injury upon an individual, or their loved ones, if they fail to act in ways that further their objectives.