UNCLASSIFIED

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

FOREIGN INTERFERENCE AND YOU

A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.
DES RENSEIGNEMENTS ET DES CONSEILS FIABLES POUR UN CANADA SÛR ET PROSPÈRE.

Canada

/// WHAT IS FOREIGN INTERFERENCE?

Foreign interference is deliberate and covert activity undertaken by a foreign state to advance its interests, often to the detriment of Canada's. The CSIS Act describes Foreign-Influenced Activities, which is another term for 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 is distinct from normal diplomatic conduct or acceptable foreign state lobbying; it is purposely covert, malign, and deceptive. States cross a line anytime they go beyond diplomacy to conduct activities that attempt to threaten our citizens, residents and institutions, or to compromise our way of life, undermine our democratic processes, or damage our economic prosperity.

/// FOREIGN INTERFERENCE AIMS

Foreign governments engage in foreign interference activities in Canada and target Canadians to advance their interests, sometimes at our expense, in an effort to achieve geopolitical, economic, military and strategic advantage. They seek to sow discord, disrupt our economy, bias policy development and decision-making, and to influence public opinion. In many cases, clandestine influence operations are meant to support foreign political agendas or to deceptively influence the targeted country's policies, officials, research institutions or democratic processes.

/// THE NATIONAL SECURITY THREAT

Foreign interference is a complex national security threat. It poses a significant threat to the integrity of our political systems, democratic processes, social cohesion, academic freedom, economic prosperity and challenges Canadians' rights and freedoms. In short, and as described by the National Security and Intelligence Committee of Parliamentarians, foreign interference threatens the fundamental values of our country and our national security.

CSIS has observed and investigated multiple instances of foreign states targeting Canada and Canadian interests through the use of human intelligence operations, state-sponsored or foreign influenced media, and sophisticated cyber techniques. Traditional interference through human intelligence operations remains the greatest danger, but interference through hostile cyber activity is a growing concern.

/// CANADA AS PERMISSIVE TARGET

As an advanced economy and an open and free democracy, Canada has long been targeted by hostile states seeking to acquire information, intelligence and influence to advance their own interests. These activities pose strategic, long-term threats to Canada's interests, jeopardize our future prosperity, and have a corrosive effect on our democratic processes and institutions.

The Committee believes that these states target Canada for a variety of reasons, but all seek to exploit the openness of our society and penetrate our fundamental institutions to meet their objectives. They target ethnocultural communities, seek to corrupt the political process, manipulate the media, and attempt to curate debate on postsecondary campuses. Each of these activities poses a significant risk to the rights and freedoms of Canadians and to the country's sovereignty: they are a clear threat to the security of Canada. (Source: Annual Report 2019, National Security and Intelligence Committee of Parliamentarians, p. 77.)

/// WHO AND WHAT IS TARGETED?

Canada's fundamental institutions (e.g. academia, free press, democratic institutions), governance processes, and diverse Canadian communities are all active targets of foreign interference activities.

On university campuses, foreign states may seek to exert undue influence, covertly and through proxies, by harassing dissidents and suppressing academic freedoms and free speech that are not aligned with their political interests. Similarly, these actors may attempt to influence public opinion and debate in Canada through interference in our press or online media.

Elected and public officials across all levels of government, representing all political parties, are targeted: 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 attractive targets.

Hostile foreign actors also target the fabric of Canada's multicultural society, seeking to influence Canadian communities, including through threats, manipulation and coercion. Some of these communities are vulnerable targets of foreign interference from states seeking to exploit them in various ways to advance the foreign state's interests, sometimes to the detriment of Canadian values and freedoms.

FOREIGN INTERFERENCE IN ACADEMIA AND RESEARCH

Foreign actors may seek to interfere in academia through a range of actions, such as:

- covertly influencing research agendas or peer review processes
- exerting economic pressure to achieve desired outcomes
- introducing or obscuring conflicts of interest or military ties
- recruiting researchers and staff for interference activities or talent programs, and
- direct foreign investment or other legal funding arrangements where the objectives of the investment or details about the funding are deliberately obscured or misrepresented.

In trying to influence public debate at academic institutions, foreign states may sponsor specific events to shape discussion rather than engage in free debate and dialogue. They may also directly or indirectly attempt to disrupt public events or other on-campus activities they perceive as challenging their political positions and spread disinformation, undermining confidence in academic discourse and expertise.

COMMON TECHNIQUES

Foreign interference techniques or activities can include (but are not limited to): elicitation, cultivation, coercion, illicit financing, cyber attacks, intimidation and disinformation.

- Elicitation results when a targeted person is manipulated into sharing valuable information through a casual conversation.
- Cultivation is a technique of building long-lasting relationships with targeted persons to enable manipulation and facilitate threat activities.
- Blackmail and threats are two of the most aggressive types of recruitment and coercion. Intimidation is also commonly used to silence dissent, including on university campuses, and to instill fear and compliance among various Canadian communities.
- Threat actors can use individuals as a proxy to conduct illicit financing activities or to make a donation to a political party or candidate.
- Cyber attacks such as spear-phishing can be used to introduce malware into your system as a means of collecting information to support foreign interference activities.
- Disinformation can be used by foreign actors to influence public opinions, perceptions, decisions and behaviours. A growing number of states have built and deployed programs dedicated to undertaking online influence as part of their daily business. Adversaries use online influence campaigns to attempt to change civil discourse, policymakers' choices, government relationships, and the reputation of politicians and countries both nationally and globally.

ONLINE INFLUENCE

A growing number of states have built and deployed programs dedicated to undertaking online influence as part of their daily business. Adversaries use online influence campaigns to attempt to change civil discourse, policymakers' choices, government relationships, and the reputation of politicians and countries both nationally and globally. They try to delegitimize the concept of democracy and other values such as human rights and liberty, which may run contrary to their own ideological views. They also try to exacerbate existing friction in democratic societies around various divisive social, political, and economic issues. While online foreign influence activities tend to increase around elections, these ongoing campaigns have broadened in scope since 2018, expanding to react and adapt to current events, shifting their content strategies around trending news stories and popular political issues (Source: 2020 National Cyber Threat Assessment, Canadian Centre for Cyber Security).

/// WHAT CAN YOU DO?

Individuals:

- Be aware of the threat; increasing our collective resilience against foreign interference is a shared responsibility.
- Do your due diligence before sharing information or entering into arrangements, know your partners and assess the risks of any partnership in advance.
- Be cyber safe.
- Remember to always verify the credibility of your information sources to ensure that you are receiving accurate information.
- Report suspicious activities and any incidents of intimidation, harassment, coercion, or threats to CSIS or to your local law enforcement authorities.

Organizations:

- Don't be a permissive target for foreign interference. Protect yourself, your organization, your reputation and your work by being aware of the threat and doing your due diligence.
- Develop policies, procedures and processes for dealing with instances of foreign interference. Make these public to ensure that potential threat actors are aware that you will not tolerate foreign interference activities.
- Provide awareness materials or training on associated policies and procedures to all employees.
- Inform any prospective partners, employees, and investors of your position and policies.
- Protect your reputation by publicly affirming your values and ethics and describing measures and policies that you are taking to advance and protect them.

NOTES

NOTES

CONTACT US

CSIS takes all allegations of foreign interference seriously. These activities constitute a threat to our national security and sovereignty, and the safety of Canadians. If you have been targeted or have concerns or other information to report, please contact CSIS by telephone (1-800-267-7685) or through our website. Canada.ca https://www.canada.ca/en/security-intelligence-service/corporate/contact-us.html