

Information is subject to the provisions of the Access to Information Act and the Privacy Act.



Foreign Interference in Canada - DEATH

CANADA IS A TARGET. It is a significant threat to the integrity of our political system, democratic institutions, economy and fundamental rights and freedoms.



The Canadian Security Intelligence Service Act describes **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.”

Foreign-Influenced Activities, or 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 and lobbying are healthy parts of democracy. **Clandestine or deceptive** foreign interference is not

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

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

PERSON-TO-PERSON FOREIGN INTERFERENCE REMAINS COMMON PRACTICE, PERPETRATED BY:

- Foreign government officials, intelligence officers, proxies and individuals purposefully selected (both willing and unwilling) - commonly members, office staff

TARGETS OF FOREIGN STATES INCLUDE:

- The general population and specific communities, political parties, candidates, parliamentarians and their paid and volunteer staff
- Government and elected officials at a targeted level 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
- You are in a position to influence government policy

FI HAS BEEN OBSERVED AT ALL LEVELS OF GOVERNMENT IN CANADA: MUNICIPAL, PROVINCIAL AND FEDERAL

YOU AND YOUR STAFF HAVE A KEY ROLE TO PLAY IN PROTECTING CANADA'S DEMOCRACY AND INSTITUTIONS.

Common FI Techniques: HOW CAN YOU PROTECT YOURSELF?

Sharon Callahan 604-931-5333

IDENTIFICATION

Electronic records were a targeted person or organization. The sharing of sensitive information through a social conversation.

For example, a friend actor could knowingly seek to provide you with sensitive information, at the hope that you will contact them, thereby producing information they were already looking for.

CONTACTING

Electronic trace actors seek to build long-lasting deep relationships with targeted persons. These relationships occur through the manipulation of large-scale requests for information and social network.

To establish a sophisticated target, most first contacters (Canadian agents) will establish contact with the end goal of recruitment over time. Various financial and production social game plays are often leveraged for recruitment.

DISSEMINATING

The use of electronic and/or printed information, often in the most aggressive forms of recruitment and conversion.

If a threat actor becomes aware of compromising or otherwise embarrassing details regarding your life, they can seek to blackmail you.

Sometimes, blackmail or threats may occur after a long period of communication and relationship-building. A threat actor may also seek to make you in a compromising situation in an effort to blackmail you later.

LIGHT ACTIVITIES

Threat actors may seek to use proxies prior to conduct illicit financing of their behalf.

Indebtedness may occur involuntarily by way of a simple request for a favour. For example, a friend actor may ask you to pay someone back or return money to a third party at their request.

Political parties and candidates may also receive funds, seemingly from a Canadian, though this may have originated from a foreign threat actor.

EVENT TRAILS

Your electronic devices can be compromised through a variety of techniques. A proxy actor may attempt to gain access to your data by using a specific link and creating details about your devices, or compromising accounts, email, calendar, and other systems.

These cyber tools are able to collect records in order to identify specific information that can be used to target individuals through a proxy actor, compromising information about a candidate.

SOCIAL MEDIA INTERVENTION

Threat actors can manipulate social media to spread disinformation, amplify a particular message, or "steal" posts, which is dangerous.

By using specific manipulation tactics, threat actors can identify or track your contacts and create the appearance of being an ally.

Threat actors may attempt to gain access to your data by using a specific link and creating details about your devices, or compromising accounts, email, calendar, and other systems.



Canadian Security Intelligence Service
1-833-998-8188
604-931-5333
1-833-228-7622
POB 613-990-0000

IF YOU FEEL YOU HAVE BEEN TARGETED, HAVE CONCERNS ABOUT ANYTHING YOU WANT TO DISCUSS
You can talk to your local security director or contact any of the following depending on the nature of your concern:
CSS
(national security issues)
613-993-0620
Canadian Centre for Cyber Security
1-833-998-8188
RCMP
(criminal activity)
914 (toll-free number)
1-833-228-7622
POB 613-990-0000

Continental Security
Sécurité Internationale
Sécurité Services

L'ingérence étrangère au Canada — SOYVÀ L'AMPOÛ

Le CANADA ET LE OML : les institutions démocratiques du Canada, ainsi que pour les droits et libertés des Canadiens.



Salon la Loi sur le Service canadien du renseignement de sécurité, les activités influencées par l'étranger s'entendent des activités « qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque ».

Des États étrangers mènent généralement clandestinement, de vastes et ambitieuses des activités d'ingérence contre les Canadiens et les institutions canadiennes au profit de leurs intérêts stratégiques et au détriment du Canada.

- L'ingérence étrangère fait de la conduite diplomatique normale ou des pressions politiques acceptables qu'exercent les acteurs étrangers.
 - La diplomatie active officielle et les groupes de pression ont leur place dans une démocratie saine, mais pas l'ingérence étrangère, trompeuse ou clandestine.
- Les États recourent à l'ingérence étrangère pour atteindre leurs propres intérêts stratégiques nationaux :
- faire des gains sur les plans stratégique, militaire, économique et du renseignement;
 - protéger leur régime;
 - discrediter les institutions libérales et démocratiques.

L'INGÉRENCE ÉTRANGÈRE EN PERSONNE DEMEURE RÉPANDUE; ELLE EST GÉNÉRALEMENT LE FAIT :

- Des représentants de gouvernements étrangers, d'agents de renseignement, d'intermédiaires de personnes collaborant étroitement (à leur insu ou non), de membres de la communauté et d'employés.

LES ÉTATS ÉTRANGERS VISENT, ENTRE AUTRES :

- La population de certains communautés, les parties politiques, les candidats ainsi que les parlementaires et
- Les membres de leur personnel dévoués à leur cause; les fonctionnaires et les élus. Car ils ont accès à des informations privilégiées, à des personnes ressources et à des décideurs.

LES ÉTATS ÉTRANGERS OU LEURS INTERMÉDIAIRES PEUVENT VOUS VISER, DIRECTEMENT OU INDIRECTEMENT, CAR :

- Vous détenez des informations qui les intéressent;
- Vous avez accès à des informations que les intéressés;
- Vous êtes un membre d'influence sur les décisions du gouvernement.

AU CANADA, L'INGÉRENCE ÉTRANGÈRE A ÉTÉ OBSERVÉE AUPRÈS D'ÉLUS FÉDÉRAUX ET PROVINCIAUX ET DANS LES ADMINISTRATIONS MUNICIPALES.

VOTRE PERSONNEL ET VOUS AVEZ UN RÔLE ESSENTIEL À JOUER DANS LA PROTECTION DE LA DÉMOCRATIE ET DES INSTITUTIONS DU CANADA.

Méthodes d'ingérence courantes : COMMENT SE PROTÉGER ?

INGÉRENCE ÉTRANGÈRE

Il y a plusieurs façons de protéger votre mandat à l'égard des renseignements personnels, au cours d'une conversation anonyme.

Par exemple, un acteur de menace d'espionnage international veut savoir des renseignements personnels dans l'espoir que vous le divulguiez et que vous le donnez à un autre individu étranger.

RECRUTEMENT

Un acteur étranger recrute des personnes à l'extérieur du Canada, par exemple, en recrutant un « service » d'espionnage ou d'information.

Pour recruter une personne, il faut d'abord établir la cible. Cela comprend une recherche minutieuse, dans le but de trouver à quel point la personne est liée à la fois au Canada et aux activités étrangères, ainsi que d'établir un contact avec elle.

INTÉGRITÉ

Le processus de recrutement est souvent basé sur l'observation et la collecte de renseignements sur le comportement et le caractère de la personne.

Si un acteur étranger dispose d'informations compromettantes ou malveillantes concernant votre vie, il peut chercher à vous faire croire.

Parfois, la création de fausses informations peut être utilisée pour influencer votre comportement. Un acteur étranger peut aussi utiliser des informations personnelles pour vous faire croire que vous êtes en danger.

INGÉRENCE ÉTRANGÈRE

Un acteur étranger peut chercher à vous influencer comme intermédiaire pour mener des activités de renseignement clandestin pour un autre.

Il peut vous y amener de manière directe, en vous demandant de servir un service à l'étranger, ou indirectement, en vous faisant croire que vous êtes un agent d'un autre service.

Des gains de réputation politique peuvent aussi servir de motivation, ainsi que le fait de travailler avec un autre service pour gagner un meilleur salaire.

ÉTATS ÉTRANGERS

Des États étrangers peuvent recruter des personnes à l'extérieur du Canada, par exemple, en recrutant un « service » d'espionnage ou d'information.

Les États étrangers peuvent recruter des personnes à l'extérieur du Canada, par exemple, en recrutant un « service » d'espionnage ou d'information.

ADMINISTRATION DES ÉTATS ÉTRANGERS

Un acteur étranger peut recruter des personnes à l'extérieur du Canada, par exemple, en recrutant un « service » d'espionnage ou d'information.

Les États étrangers peuvent recruter des personnes à l'extérieur du Canada, par exemple, en recrutant un « service » d'espionnage ou d'information.

Canada

Non classifié

Si vous croyez avoir été pris pour cible, contactez-nous immédiatement.

Si vous avez des préoccupations, contactez-nous immédiatement.

1-855-997-0000

1-855-997-0000

1-855-997-0000

Foreign Interference
Foreign Interference
Foreign Interference

Foreign Interference

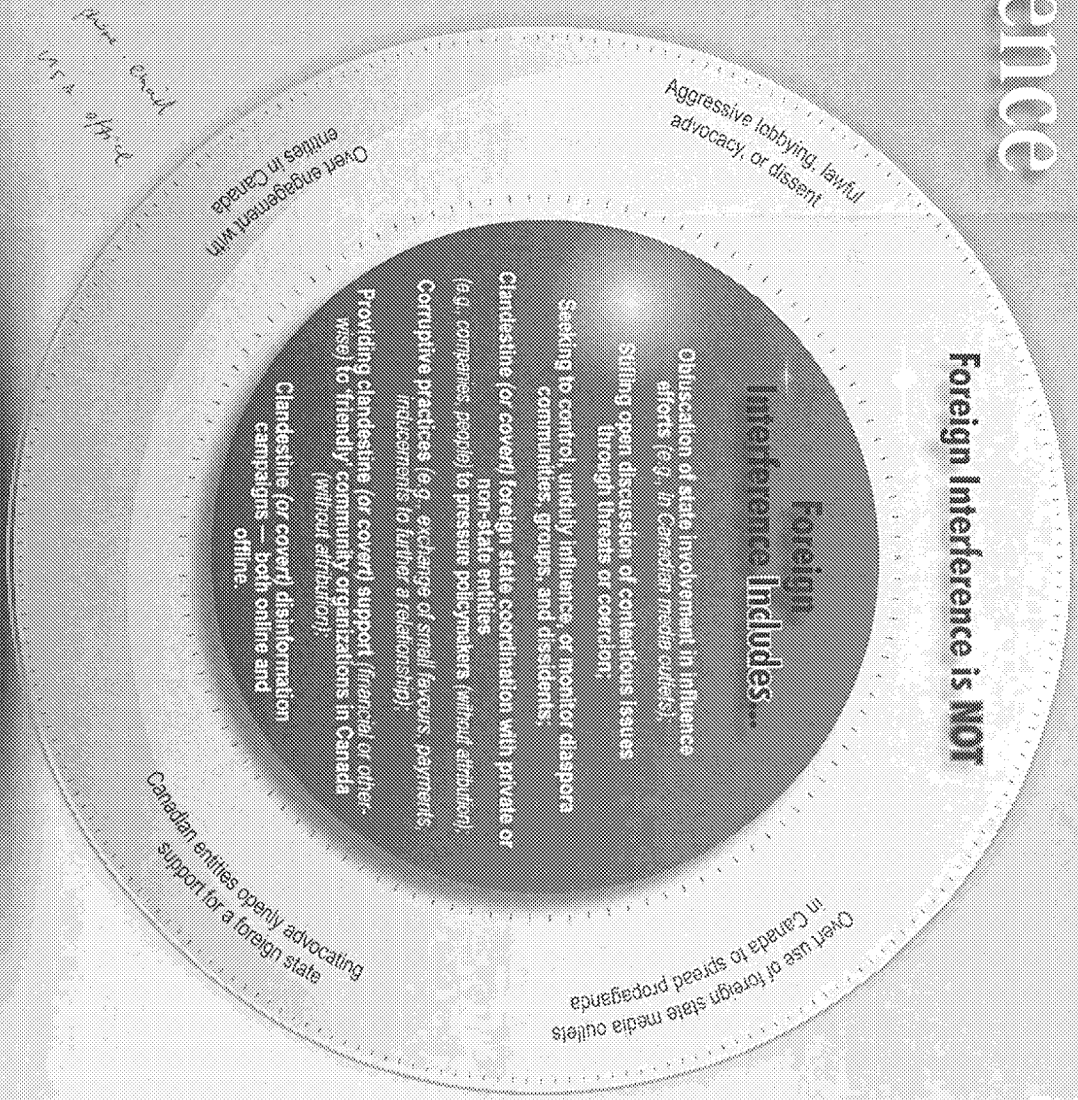


According to Section 2(b) of the CSIS Act, foreign influenced activities are actions within or relating to Canada, that are detrimental to the interests of Canada, and are clandestine or deceptive, or involve a threat to any person.

Foreign influenced activities, also known as foreign interference (FI), poses a significant threat to the integrity of our political system, democratic institutions, social cohesion, economy, long-term prosperity, and fundamental rights and freedoms.

While FI can be a single act, it is more often characterized by a series of activities and behaviours that may occur over a period of time.

FI is a national threat. It targets all levels of government — federal, provincial, territorial, and municipal, as well as Canadian communities.

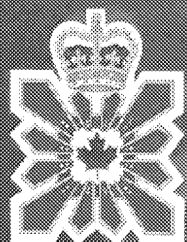


UNCLASSIFIED



Canadian Security
Intelligence Service

Service canadien de
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.

Aussi disponible en français sous le titre : L'ingérence étrangère et vous



UNCLASSIFIED

FOREIGN INTERFERENCE AND YOU

UNCLASSIFIED

FOREIGN INTERFERENCE AND YOU

UNCLASSIFIED

/// 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.



/// 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.

UNCLASSIFIED

FOREIGN INTERFERENCE AND YOU

FOREIGN INTERFERENCE AND YOU

UNCLASSIFIED

FOREIGN INTERFERENCE IN ACADEMIA AND RESEARCH

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

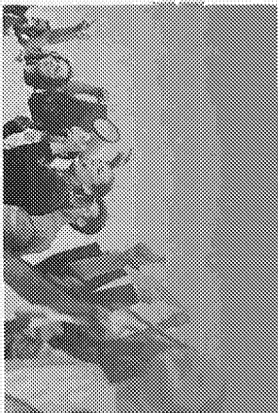
- covertly influencing research agendas or peer review processes
- exerting economic pressure to achieve desired outcomes
- introducing or obscuring conflicts of interest or military ties
- recruiting researchers and staff for interference activities or talent programs, and
- direct foreign investment or other legal funding arrangements where the objectives of the investment or debate 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 their 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 opinion, 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 voter discourse, policymakers' choices, government relationships, and the reputation of politicians and countries both nationally and globally.



/// 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 partner's 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.

ONLINE INFLUENCE

A growing number of states have built and deployed programs dedicated to undertaking online influence as part of their intelligence or adversary 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 seek another leading nation in democratic societies around various domestic social, political, and economic issues. While official foreign influence activities tend to increase around elections, these ongoing campaigns have broadened in scope from 2018, expanding to reach and target its current events, shifting their content strategies around funding news stories and popular political issues (Source: 2023 National Cyber Threat Assessment, Canadian Centre for Cyber Security).

UNCLASSIFIED

FOREIGN INTERFERENCE AND YOU

FOREIGN INTERFERENCE AND YOU

UNCLASSIFIED

NOTES

NOTES

FOR THE CONFERENCE RECORDS

FOR THE CONFERENCE RECORDS

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>