Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

UNCLASSIFIED

Foreign Interference in Canada – BE ALERT

CANADA IS A TARGET: FI 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 witting and unwitting) - community 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 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;
- 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?

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 you with incorrect information, in the hope that you will correct them, thereby providing information they were actually looking for.

Be discrete, avoid 'over-sharing', and assume public conversations are monitored.

CULTIVATION

Effective threat actors seek to build long-lasting, deep 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, targets must first be cultivated. 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.

Be aware and keep track of odd social interactions, frequent requests to meet privately, and out-of-place introductions or engagements.

BLACKMAIL/ THREATS

The use of blackmail and/or threats represents one of the most aggressive forms of recruitment and coercion.

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 cultivation and relationship-building. A threat actor may also seek to place you in a compromising situation in an effort to blackmail you later.

Avoid sharing compromising details about your life with untrusted individuals, both in-person and online. Avoid placing yourself in compromising situations.

ILLICIT FINANCING

Threat actors may seek to use you as a proxy to conduct illicit financing on their behalf.

Inducements may occur innocuously via a simple request for a favour. For example, a threat actor may ask you to 'pay someone back' or relay money to a third party on their behalf.

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

Be aware of inappropriate requests which involve money, and question the source of strange donations or 'gifts'.

CYBER TOOLS

Your electronic devices can be compromised through a range of tradecraft.
Socially-engineered e-mails (i.e., 'spear-phishing' emails) can trick you into a clicking a specific link and sharing details about your devices, or can potentially introduce harmful malware into your systems.

These cyber tools enable threat actors to collect potentially useful information that can be used in a foreign influence operation (e.g. voter data, compromising information about a candidate).

Use strong passwords, enable two-factor authentication, and do not click on links/open attachments unless you are certain of who sent them and why.

SOCIAL MEDIA MANIPULATION

Threat actors can manipulate social media to spread disinformation, amplify a particular message, or 'troll' users, when appropriate.

By using specific manipulation tactics, threat actors can potentially impact voter opinions and degrade the reputations of elected officials.

Be careful in what you share on-line (or re-post from others), take note of odd online interactions and content.

IF YOU FEEL YOU HAVE BEEN TARGETED, – OR – HAVE CONCERNS ABOUT ANYTHING YOU WANT TO DISCUSS

you can talk to your Chief Security Officer or contact any of the following depending on the nature of your concern:

CSIS
(national security threats)
613-993-9620

Canadian Centre for Cyber Security
1-833-CYBER-88

RCMP
(criminal activity) 911
(non-imminent threat)
1 833-226-7622

PCO 613-960-4000

Canada

Service canadien du renseignement de sécurité | Canadian Security Intelligence Service

Ingérence étrangère au Canada – SOYEZ À L'AFFÛT

NON CLASSIFIÉ

LE CANADA EST UNE CIBLE : L'ingérence étrangère représente une menace importante pour l'intégrité du système politique, pour l'économie et pour les institutions démocratiques du Canada, ainsi que pour les droits et libertés des Canadiens.

Selon 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 influencées par l'étranger ou 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 diffère 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;
- discréditer les institutions libérales et démocratiques.

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

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

LES ÉTATS ÉTRANGERS VISENT, ENTRE AUTRES :

- La population et certaines communautés, les partis politiques, les candidats ainsi que les parlementaires et
- Les membres de leur personnel (rémunérés et bénévoles), 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 qui les intéressent;
- Vous êtes en mesure d'influer sur les décisions du gouvernement.

AU CANADA, L'INGÉRENCE ÉTRANGÈRE A ÉTÉ OBSERVÉE AUX ÉCHELONS FÉDÉRAL ET PROVINCIAL 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?

SUBTILISATION

Il y a subtilisation lorsqu'une cible est amenée à fournir des informations précieuses au cours d'une conversation anodine.

Par exemple, un auteur de menace pourra sciemment vous fournir des informations erronées dans l'espoir que vous le corrigiez et que vous lui donniez ainsi ce qui l'intéresse vraiment.

Soyez discret, évitez de trop en dire et partez du principe que les conversations publiques sont surveillées.

RELATIONS

Un auteur de menace efficace cherche à établir des relations étroites durables avec sa cible. Il peut ainsi la manipuler au besoin, par exemple, en lui demandant un « service » inapproprié ou particulier.

Pour nouer une relation, il faut d'abord cultiver la cible. Cela commence par une simple présentation, dans le but de nouer la cible au fil du temps. Des intérêts communs et des activités sociales anodines sont souvent utilisés à cette fin.

Be aware and keep track of odd social interactions, frequent requests to meet privately, and out-of-place introductions or engagements.

CHANTAGE ET MENACES

Le chantage et les menaces représentent les formes les plus agressives de recrutement et de coercition.

Si un auteur de menace dispose d'informations compromettantes ou autrement embarrassantes sur votre vie, il peut chercher à vous faire chanter.

Parfois, le chantage ou les menaces surviennent alors que la relation est entretenue depuis longtemps. Un auteur de menace peut aussi vous mettre dans une situation compromettante pour vous faire chanter par la suite.

Évitez de confier des informations compromettantes sur votre vie à des gens peu fiables, en personne ou en ligne. Évitez de vous retrouver dans des situations compromettantes.

FINANCEMENT ILLICITE

Un auteur de menace peut chercher à vous utiliser comme intermédiaire pour mener des activités de financement illicites pour son compte.

Il peut vous y inciter de manière anodine, en vous demandant un simple service. Il peut par exemple vous demander de « rembourser quelqu'un » ou de remettre de l'argent à un tiers en son nom.

Des partis et des candidats politiques peuvent aussi recevoir des fonds venant, semble-t-il, d'un Canadien, alors qu'ils ont peut-être pour origine un auteur de menace étranger.

Faites attention aux demandes inappropriées où il est question d'argent et mettez en doute l'origine des dons ou des « cadeaux » curieux.

OUTILS INFORMATIQUES

Diverses techniques peuvent servir à compromettre vos appareils électroniques. Les courriels de hameçonnage peuvent vous amener à cliquer sur un lien et à donner des détails sur vos appareils ou alors infecter vos systèmes avec un malware.

Ces outils informatiques permettent à un auteur de menace de recueillir des informations (ou des données sur des électeurs, informations compromettantes sur un candidat).

Utilisez de bons mots de passe, activez l'authentification à deux facteurs et évitez de cliquer sur des liens ou d'ouvrir des pièces jointes si vous ne savez pas qui les a envoyés ni pourquoi.

MANIPULATION DES MÉDIAS SOCIAUX

Un auteur de menace peut manipuler les médias sociaux pour diffuser de fausses informations, amplifier un message ou « troller » des utilisateurs, s'il y a lieu.

Selon les moyens de manipulation employés, un auteur de menace pourrait influer sur l'opinion des électeurs ou porter atteinte à la réputation d'élus.

Prenez garde à ce que vous affichez en ligne (ou à ce que vous republiez) et prenez en note les interactions étranges en ligne.

SI VOUS CROYEZ AVOIR ÉTÉ PRIS POUR CIBLE, – OU – SI VOUS AVEZ DES PRÉOCCUPATIONS DONT VOUS SOUHAITEZ PARLER

communiquez avec l'agent de sécurité ministériel ou l'un ou l'autre des organismes suivants, selon la nature du problème.

SCRS
(menaces pour la sécurité nationale) 613-993-9620

Centre canadien pour la cybersécurité
1 833 CYBER 88

GRC
(activité criminelle) 911
(menace non imminente)
1 833 226 7622

BCP 613-960-4000

Canada