NON-CLASSIFIÉ

Service canadien du renseignement de sécurité

Canadian Security Intelligence Service

L'INGÉRENCE ÉTRANGÈRE ET VOUS

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

Canada

/// QU'EST-CE QUE L'INGÉRENCE ÉTRANGÈRE

Il s'agit d'activités menées délibérément et clandestinement par un État étranger dans le but de servir ses intérêts, souvent au détriment de ceux du Canada. Dans la *Loi sur le SCRS*, les activités influencées par l'étranger (autre terme signifiant ingérence étrangère) sont définies comme étant 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 ».

L'ingérence étrangère est distincte des activités diplomatiques normales ou des pressions politiques acceptables exercées par un État étranger. Elle est intentionnellement clandestine, pernicieuse et trompeuse. Les États franchissent la limite chaque fois qu'ils vont au-delà de la diplomatie pour mener des activités qui visent à menacer des citoyens, des résidents ou des institutions, ou à compromettre notre mode de vie, à fragiliser nos processus démocratiques ou à nuire à notre prospérité économique.

/// LES OBJECTIFS DE L'INGÉRENCE ÉTRANGÈRE

Des gouvernements étrangers mènent des activités d'ingérence au Canada et prennent des Canadiens pour cible afin de servir leurs intérêts, parfois à nos dépens, dans le but d'acquérir un avantage géopolitique, économique, militaire ou stratégique. Ils cherchent à semer la discorde, à perturber notre économie, à influer sur l'élaboration des politiques et les processus décisionnels et à influencer l'opinion publique. Dans de nombreux cas, les opérations d'ingérence clandestine visent à soutenir des programmes politiques étrangers ou à influencer de façon trompeuse des politiques, des centres de recherche, des processus démocratiques ou des représentants du Canada.

/// LA MENACE POUR LA SÉCURITÉ NATIONALE

L'ingérence étrangère est une menace complexe pour la sécurité nationale. Elle constitue une menace importante pour l'intégrité des systèmes politiques, les processus démocratiques, la cohésion sociale, la liberté universitaire et la prospérité économique du Canada et remet en cause les droits et libertés des Canadiens. Bref, comme l'a écrit le Comité des parlementaires sur la sécurité nationale et le renseignement, l'ingérence étrangère menace les valeurs fondamentales de notre pays et notre sécurité nationale.

Le SCRS fait enquête sur les multiples cas qu'il observe où des États étrangers prennent pour cible le Canada et des intérêts canadiens en menant des opérations de renseignement humain, en faisant appel à des médias parrainés par l'État ou influencés par l'étranger et en appliquant des cybertechniques complexes. Les activités traditionnelles d'ingérence menées dans le cadre d'opérations de renseignement humain demeurent le plus grand danger, quoique les cyberopérations d'ingérence suscitent des préoccupations croissantes.

/// LE CANADA EST UNE CIBLE PROPICE

En tant que démocratie libre et ouverte jouissant d'une économie développée, le Canada est depuis longtemps pris pour cible par des États adverses qui cherchent à acquérir des informations et des renseignements ou à exercer une influence afin de servir leurs propres intérêts. Ces activités représentent des menaces stratégiques à long terme pour les intérêts du Canada, nuisent à notre prospérité future et ont un effet nocif sur nos processus démocratiques et nos institutions.

Le Comité estime que ces États ciblent le Canada pour diverses raisons, mais qu'ils cherchent tous à tirer profit de l'ouverture de notre société et à s'immiscer au sein de nos institutions fondamentales pour atteindre leurs objectifs. Ils ciblent les communautés ethnoculturelles, cherchent à corrompre le processus politique, manipulent les médias et tentent de manipuler des débats sur les campus postsecondaires. Chacune de ces activités pose un risque important pour les droits et les libertés des Canadiens et la souveraineté du pays : ils constituent une menace manifeste pour la sécurité du Canada. (Source : Comité des parlementaires sur la sécurité nationale et le renseignement, Rapport annuel 2019, p. 88.)

/// QUELLES SONT LES CIBLES?

Les institutions fondamentales du Canada (p. ex. les universités, la presse libre, les institutions démocratiques), les processus de gouvernance et diverses communautés canadiennes sont tous des cibles d'activités d'ingérence étrangère.

Sur les campus universitaires, des États étrangers peuvent chercher à exercer une influence indue, clandestinement et par l'entremise d'intermédiaires, c'est-à-dire harceler des dissidents et supprimer la liberté d'expression et les libertés universitaires qui ne cadrent pas avec leurs intérêts politiques. De même, ils peuvent tenter d'influencer l'opinion et le débat publics au Canada en s'immisçant dans la presse et les médias en ligne.

Les élus et les représentants officiels de tous les ordres du gouvernement, tous partis politiques confondus, sont pris pour cible : les députés fédéraux et provinciaux, les élus municipaux et les représentants des gouvernements autochtones. Les fonctionnaires, le personnel ministériel et politique et tous ceux qui contribuent au processus décisionnel de la politique publique ou l'influencent sont aussi des cibles intéressantes.

Des acteurs étatiques hostiles s'attaquent également à la structure même de la société multiculturelle du Canada lorsqu'ils cherchent à influencer les communautés canadiennes, notamment par la menace, la manipulation ou la coercition. Certaines de ces communautés sont des cibles vulnérables aux activités d'ingérence étrangère d'États qui tentent de les exploiter de diverses façons afin de servir leurs propres intérêts, parfois au détriment des libertés et des valeurs canadiennes.

L'INGÉRENCE ÉTRANGÈRE DANS LES UNIVERSITÉS ET LE MILIEU DE LA RECHERCHE

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

- influencer clandestinement des programmes de recherche ou des processus d'examen par les pairs;
- exercer des pressions économiques pour obtenir les résultats souhaités;
- introduire ou dissimuler des conflits d'intérêts ou des liens avec l'armée;
- recruter des chercheurs et des membres du personnel pour mener des activités d'ingérence ou des programmes de recrutement de talents;
- réaliser des investissements directs étrangers ou conclure d'autres ententes de financement légales dont les objectifs ou les détails sont délibérément cachés ou présentés sous un faux jour.

Pour essayer d'influencer le débat public dans les établissements d'enseignement, des États étrangers peuvent parrainer certains événements afin d'orienter la discussion au lieu de participer à un débat et un dialogue libres. Ils peuvent aussi tenter directement ou indirectement de perturber des événements publics ou d'autres activités tenues sur les campus qu'ils considèrent comme remettant en cause leurs positions politiques et propager de la désinformation, de façon à miner la confiance dans l'expertise et le discours universitaires.

LES TECHNIQUES COURANTES

Les techniques ou activités d'ingérence étrangère peuvent notamment comprendre : la subtilisation de renseignements, l'établissement de relations, la coercition, le financement illicite, les cyberattaques, l'intimidation et la désinformation.

- Il y a subtilisation de renseignements lorsqu'une personne ciblée est amenée à fournir de précieuses informations au cours d'une conversation anodine.
- L'établissement de relations est une technique visant à cultiver les personnes ciblées sur de longues périodes afin de les manipuler et de faciliter des activités liées à la menace.
- Le chantage et les menaces sont les formes de recrutement et de coercition les plus agressives. L'intimidation est aussi couramment utilisée pour museler les dissidents, notamment sur les campus universitaires, et pour faire suffisamment peur aux diverses communautés canadiennes pour qu'elles en viennent à se conformer.
- Les auteurs de menace peuvent avoir recours à des intermédiaires pour mener des activités de financement illicite ou pour faire des dons à des candidats ou à des partis politiques.
- Les cyberattaques comme le harponnage peuvent faciliter l'introduction de maliciels dans vos systèmes comme moyen de recueillir des informations à l'appui d'activités d'ingérence étrangère.

- Enfin, des acteurs étrangers peuvent employer la désinformation pour influencer des opinions publiques, des perceptions, des décisions et des comportements. Un nombre croissant d'États ont élaboré et mis en place des programmes visant expressément à exercer une influence en ligne dans le cadre de leurs activités courantes. Des adversaires mènent des campagnes d'influence en ligne pour essayer de modifier le discours public, les choix des décideurs, les relations gouvernementales et la réputation de politiciens et de pays à l'échelle nationale et internationale.

INFLUENCE ÉTRANGÈRE EN LIGNE

Un nombre croissant d'États ont élaboré et déployé des programmes visant à mener une activité d'influence en ligne dans le cadre de leurs pratiques quotidiennes. Des adversaires ont recours à des campagnes d'influence pour tenter de changer le discours public, les choix des décideurs politiques, les relations gouvernementales et la réputation des politiciens et des pays, tant à l'échelle nationale qu'internationale. Ils tentent de délégitimiser le concept de la démocratie ainsi que d'autres valeurs, comme les droits de la personne et ceux touchant aux libertés, qui peuvent aller à l'encontre de leurs propres positions idéologiques. Ils cherchent également à aggraver la friction actuelle dans les sociétés démocratiques en ce qui concerne diverses questions controversées d'ordre social, politique et économique. Bien que les activités d'influence en ligne aient tendance à augmenter en périodes électorales, la portée de ces campagnes continues s'est élargie depuis 2018, de façon à réagir et à s'adapter aux événements actuels, et à changer les stratégies en fonction des nouvelles qui font l'actualité et des enjeux politiques populaires. (Source : Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2020)

/// CE QUE VOUS POUVEZ FAIRE

Particuliers

- Soyez conscient de la menace. Le renforcement de notre résilience collective contre l'ingérence étrangère est une responsabilité partagée.
- Faites preuve de vigilance avant de communiquer des informations ou de conclure des ententes. Assurez-vous de connaître vos partenaires et évaluez à l'avance les risques de tout partenariat.
- Pensez cybersécurité.
- N'oubliez pas de toujours vérifier la crédibilité de vos sources d'information afin de vous assurer de recevoir des données exactes.
- Signalez toute activité suspecte et tout incident d'intimidation, de harcèlement, de coercition ou de menace au SCRS ou à votre service de police local.

Organisations

- Ne soyez pas une cible propice à l'ingérence étrangère. Protégez-vous et protégez votre organisation, votre réputation et votre travail en étant conscient de la menace et en faisant preuve de vigilance.
- Élaborez des politiques, des procédures et des processus pour faire face aux cas d'ingérence étrangère. Rendez ces documents publics afin de vous assurer que d'éventuels auteurs de menace sauront que vous ne tolérez pas les activités d'ingérence étrangère.
- Offrez à tous vos employés des documents de sensibilisation ou une formation sur les politiques et les procédures connexes.
- Informez tout partenaire, employé ou investisseur potentiel de votre position et de vos politiques.
- Protégez votre réputation en affirmant publiquement vos valeurs et votre éthique et en décrivant les mesures et les politiques que vous avez mises en place pour les défendre.

NOTES

CONTACTEZ-NOUS

Le SCRS prend au sérieux toutes les allégations d'ingérence étrangère. Ces activités représentent une menace pour la sécurité nationale et la souveraineté du Canada ainsi que pour la sécurité de la population canadienne. Si vous avez été pris pour cible ou si vous avez des inquiétudes ou d'autres informations à signaler, n'hésitez pas à communiquer avec le SCRS par téléphone (au 1-800-267-7685) ou en visitant notre site Web. Canada.ca https://www.canada.ca/en/security-intelligence-service/corporate/contact-us.html