Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Direction de la Liaison-recherche et de la Collaboration avec les intervenants

Guide pour les entités répondant à la COVID-19

13 mai 2020

Introduction

- Le SCRS poursuit son travail pendant la pandémie, ce qui comprend la lutte contre la menace d'ingérence étrangère et d'espionnage. Nous travaillons en étroite collaboration avec des partenaires, à l'intérieur et à l'extérieur du Canada, pour aider à sauvegarder la contribution du Canada aux efforts mondiaux visant à protéger l'humanité contre le COVID-19 et à faire face aux menaces qui pèsent sur les intérêts et la prospérité du Canada.
- Vos efforts et vos recherches sur les questions liées à COVID-19 peuvent faire de vous une cible pour ce type d'activités d'acteurs étrangers hostiles.
- Le Canada possède une abondance de ressources naturelles, de technologies de pointe, de talents humains et d'expertises. Nous sommes des leaders mondiaux dans de nombreux secteurs. Nous avons de puissants alliés avec lesquels nous entretenons des relations économiques, de sécurité et de défense étroites. Nous sommes une nation riche et très développée. Tout cela fait de nous une cible.
- Les services de renseignement étrangers hostiles ou les personnes qui travaillent avec le soutien tacite ou explicite d'États étrangers recueillent des informations politiques, économiques, commerciales ou militaires par des moyens clandestins ici au Canada.

> ***« Bien que les menaces d'espionnage et d'ingérence étrangère ne soient pas nouvelles, un certain nombre de facteurs se sont combinés pendant cette période pour accroître les risques pour les intérêts canadiens. Du côté canadien, cela comprend une augmentation de la recherche et du développement innovateurs au Canada (dont une part importante est financée par des fonds publics); une utilisation accrue des arrangements de télétravail; et l'expansion des partenariats internationaux. Du côté des acteurs étrangers, le SCRS observe une évolution rapide de la nature et du volume des activités menaçantes et leur concentration sur de nouvelles cibles au Canada. »***

- Le SCRS mène des activités de sensibilisation afin d'aider les entités canadiennes à protéger leur recherche et développement, leur propriété intellectuelle ou leurs intérêts commerciaux en augmentant leur sensibilisation à cette menace, et aux mesures qu'elles peuvent prendre pour se protéger.

- N'hésitez pas à contacter le SCRS à tout moment pour toute préoccupation ou question que vous pourriez avoir. Vous pouvez trouver nos coordonnées ici : https://www.canada.ca/fr/service-renseignement-securite/organisation/contactez-nous.html

- Si vous avez des questions liées spécifiquement à un cyberincident ou à la cybersécurité, nous vous invitons à communiquer avec nos partenaires du Centre canadien pour la cybersécurité. Vous pouvez trouver ses coordonnées ici: https://cyber.gc.ca/fr/contactez-nous

Secteurs ciblés pour l'espionnage étranger

- À l'heure actuelle, aucun secteur n'est plus important à l'échelle mondiale que ceux de la santé et de la biopharmaceutique. De nombreux pays ont accéléré leurs activités de recherche et de développement liées à la COVID-19 afin de soutenir les mesures prises pour lutter contre la pandémie.

- Alors que de nombreux chercheurs et équipes de développement sont investis dans un travail transparent et collaboratif à travers les frontières vers un objectif commun, il y a ceux qui, malheureusement, cherchent à exploiter ce partage pour leur propre avantage stratégique ou économique.

- Il est important de savoir cependant que ce ne sont pas les seuls secteurs de l'économie ciblés en ce moment.

> ***«D'autres secteurs tels que l'intelligence artificielle, l'informatique quantique, la nanotechnologie, l'analyse des données massives, la prochaine génération et la fabrication sont également fortement impliqués dans l'effort de réponse COVID-19 et constituent une cible très attrayante pour l'espionnage étranger. »***

- Le SCRS est particulièrement préoccupé par cette menace liée aux activités parrainées par d'États hostiles qui cherchent secrètement un avantage stratégique ou concurrentiel.

- Certains gouvernements sont prêts à utiliser des moyens à la fois licites et illicites pour obtenir des biens et des technologies afin de promouvoir leurs propres intérêts. Les moyens licites peuvent

inclure les achats et les investissements étrangers. Les moyens illicites peuvent comprendre le vol de biens et de technologies par divers moyens tels que les exportations non autorisées, le transfert de technologie immatériel, les cyberattaques et l'utilisation de sources et d'atouts humains.

Quatre portes

- Le SCRS a élaboré le concept des « quatre portes » de la sécurité économique pour comprendre et expliquer ces menaces.

- Il existe quatre moyens d'avoir accès aux biens, aux savoir-faire et aux technologies sensibles : les exportations, les investissements, les connaissances et les licences.

Attaques contre la connaissance

- L'exposition de connaissances canadiennes sensibles - comme la recherche, la propriété intellectuelle, ainsi que des données personnelles et d'entreprise - peut se produire de plusieurs façons, notamment le cyberespionnage, l'utilisation de menaces internes (compromettant un réseau interne ou transférant une technologie exclusive) et le transfert de technologie intangible grâce, par exemple, à la collaboration en matière de recherche.

- Les «cyberespions» et les acteurs des menaces internes ont reçu beaucoup d'attention du public dans le passé pour leur implication dans des attaques contre le savoir, mais un autre type d'acteur moins connu est ce que le Service appelle le collecteur non-traditionnel de renseignements.

- En termes simples, cela se réfère à des personnes sans formation formelle en matière de renseignement, mais avec une expertise particulière, comme des gens d'affaires, des scientifiques, des chercheurs et même des étudiants. Ces personnes savent ce qui est précieux et sont capables d'opérer dans des environnements commerciaux et de recherche sans éveiller de soupçons.

- Les collecteurs non traditionnels de renseignements peuvent ne pas avoir l'intention préméditée de nuire à votre organisation ou au Canada, mais sont extrêmement vulnérables aux demandes des États s'ils retournent dans un pays autoritaire qui ne tient pas compte des droits de propriété intellectuelle et des brevets. Si cet État étranger apprend que ces personnes ont accès à vos informations précieuses, il peut les obliger à remettre votre propriété intellectuelle avec un soutien juridique complet pour forcer leur assistance.

«Outre la recherche et la propriété intellectuelle, les informations financières et médicales des Canadiens peuvent également être ciblées par des acteurs de la menace.»

- Ce type d'informations contient des détails intimes sur une personne ou une organisation, y compris leurs vulnérabilités potentielles, qu'un gouvernement étranger peut exploiter à l'appui d'activités hostiles telles que l'espionnage, le sabotage ou la perturbation.

- Vous pouvez involontairement inviter ces collecteurs non traditionnels dans votre porte d'entrée, alors que vous poursuivez des accords commerciaux ou des collaborations de R&D.

Investissements

- La stabilité économique du Canada et son solide système financier en font un endroit favorable aux investissements étrangers. Une faible proportion de ces investissements représente une menace pour la sécurité nationale et la prospérité du Canada.

- Dans le contexte actuel, les gouvernements étrangers peuvent chercher à investir pour accéder et contrôler les technologies et le savoir-faire sensibles. L'investissement peut également fournir aux acteurs de la menace l'accès aux infrastructures essentielles du Canada ou leur contrôle, y compris les chaînes d'approvisionnement essentielles.

«Cette pandémie a mis en évidence l'importance de sécuriser les chaînes d'approvisionnement pour les biens de santé publique vitaux. Le SCRS veut s'assurer que les investissements étrangers ne facilitent pas les efforts parrainés par l'État pour obtenir l'accès et le contrôle des biens qui sont essentiels à l'intervention mondiale en matière de santé publique. »

- En investissant dans votre entreprise, les acteurs de la menace peuvent avoir accès à tout ce que vous savez et à tout ce que vous possédez.

- Les risques de l'investissement étranger visant l'acquisition de biens, de technologies et de propriété intellectuelle canadiens stratégiques sont réels. Si vous recevez des offres inattendues dans les jours et les semaines à venir, merci de bien vouloir en tenir compte et de faire part au SCRS de vos préoccupations.

«Il est important que vous sachiez que ce qui semble être un investissement étranger lucratif peut avoir des chaînes cachées - et des conséquences – attachées.»

Importations et exportations

- L'achat et l'exportation de technologies avancées, qui peuvent ensuite être copiées ou reconstituées, est un problème de sécurité nationale bien connu. Cependant, dans le contexte actuel de COVID-19, le risque d'attaques ciblées contre les chaînes d'approvisionnement aurait une incidence croissante sur la capacité du gouvernement à assurer la sûreté et la sécurité des Canadiens et sur la capacité du Canada à contribuer à l'innovation en santé mondiale.

- Les ingrédients médicinaux, l'équipement de protection individuelle et d'autres fournitures médicales sont des exemples d'articles essentiels qui, s'ils sont refusés au Canada en raison de chaînes d'approvisionnement compromises, pourraient avoir un impact négatif sur la réponse COVID-19 du Canada.

- Le SCRS est également préoccupé par l'importation de marchandises étrangères qui sont de qualité inférieure et / ou frauduleuses. S'il s'agit de produits de santé, cela met la vie des Canadiens en danger. La GRC qui peut vous conseiller et vous aider à répondre à ces préoccupations.

Licences

- Certaines licences peuvent conférer des droits privilégiés ou l'accès à des espaces physiques ou à des données sensibles, qui peuvent être exploitées pour nuire au Canada et aux canadiens. Des exemples typiques de telles licences comprennent les visas, les brevets, les certifications industrielles et les accords de distribution.

- Souvent, les licences ne sont pas l'objectif elles-mêmes, mais plutôt un moyen d'atteindre l'objectif ultime de l'acteur de la menace, comme l'accès aux données canadiennes, l'infrastructure critique ou le droit d'entrer au Canada.

- Dans le contexte de COVID-19, des exemples de licences pouvant être ciblées comprennent les brevets pharmaceutiques, les brevets biotechnologiques, les autorisations d'utiliser des médicaments ou des procédures spécifiques.

«Votre propriété intellectuelle peut être exposée au vol si vous concluez des accords de licence ou d'autres accords contractuels avec des partenaires étrangers, dans l'espoir qu'ils respectent les lois et normes canadiennes. »

La menace est réelle, mais vous n'êtes pas seul

- Pourquoi devriez-vous vous soucier de ces menaces?
    - Premièrement, cet espionnage menace le gagne-pain même de votre entreprise ou institution et met en péril les intérêts et la prospérité du Canada. Pour le milieu de la recherche, cela peut signifier que des percées scientifiques importantes peuvent être transférées à des pays qui ne souhaitent pas partager les avantages, ou que la contribution du Canada aux efforts mondiaux de santé publique est compromise.

«L'espionnage peut anéantir les perspectives de n'importe quelle entreprise - dans l'ensemble, il peut poser des défis à des secteurs entiers, plaçant le Canada dans une situation désavantageuse à long terme qui érodera notre prospérité. »

    - Pire encore, dans le contexte de la pandémie de COVID-19, une partie de cette activité de menace peut créer de nouveaux risques qui mettent en danger la santé et la sécurité des Canadiens.

- Le SCRS est là pour entendre vos préoccupations et offrir votre soutien. Sachez que:
    - Les acteurs de la menace peuvent essayer les quatre portes, mais ils n'ont besoin que d'une seule pour réussir à nuire considérablement à vous et aux intérêts canadiens;
    - La nationalité n'est pas un indicateur précis de savoir si un individu ou une organisation sera un bon partenaire ou employé ou peut constituer une menace;
    - Lors de la conclusion de partenariats, il est essentiel que vous compreniez qui contrôle votre partenaire potentiel et les biens ou technologies que vous créez, et qui bénéficiera de vos activités;
    - Si vous recevez un financement du gouvernement du Canada, vérifiez s'il existe des limites ou des exigences particulières en matière de propriété intellectuelle ou d'intégrité de la recherche qui doivent être respectées; et,
    - Les menaces sont de toutes tailles et valeurs en dollars. Même si vous êtes petit, votre travail peut être d'un grand intérêt. Votre travail peut être une pièce critique d'un plus grand puzzle.

- Le SCRS a une présence pancanadienne. En cas de situation, veuillez contacter l'un de nos bureaux régionaux pour discuter de toute activité de menace potentielle: https://www.canada.ca/fr/service-renseignement-securite/organisation/contactez-nous.html

«Le SCRS travaille de concert avec ses partenaires du gouvernement du Canada sur cet effort. Nous travaillons ensemble pour détecter, dissuader et répondre à ces menaces au quotidien pour assurer la sécurité et la prospérité du Canada. »