Service canadien du renseignement de sécurité | Canadian Security Intelligence Service

PROTÉGEZ VOS RECHERCHES

TERRITOIRES DU NORD-OUEST

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

/ Aux termes de son mandat, le Service canadien du renseignement de sécurité (SCRS) mène des enquêtes sur les menaces que font peser les activités d'espionnage et d'ingérence étrangère, puis conseille le gouvernement du Canada à ce sujet. Dans un monde où la concurrence s'intensifie, les États cherchent à se donner tous les avantages possibles. Aussi, pour atteindre leurs objectifs dans les secteurs économiques, sécuritaires et militaires, des États étrangers se livrent à l'espionnage, ce qui entraîne d'importantes répercussions sur le Canada : pertes d'emplois, pertes de revenu pour les entreprises et le gouvernement, diminution des avantages nationaux et concurrentiels, etc.

En 2019, la part des Territoires du Nord-Ouest (T.N.-O.) au produit intérieur brut du Canada s'élevait à environ 4,4 G$, un total principalement attribuable à ses secteurs économiques traditionnels, c'est-à-dire l'exploitation minière, l'exploitation de carrières, le pétrole et le gaz, la construction et les services. Les T.N.-O., qui cherchent à réaliser leur potentiel économique, reconnaissent que les projets de recherche et de développement pourraient aussi être d'importants moteurs économiques. Ils sont les hôtes d'une communauté de recherche motivée comprenant des organismes territoriaux, des organismes communautaires, des partenaires œuvrant dans des projets nationaux et des universités au sud ainsi que des réseaux de recherches nordiques canadiens et circumpolaires. Le Collège Aurora et les centres de recherche qui y sont associés (Western Arctic, North Slave et South Slave) ainsi que l'Institut de recherche sur la santé circumpolaire font partie des organismes notables à cet égard.

Aussi, les investissements récents de la Fondation canadienne pour l'innovation dans ce collège et les centres associés assureront la poursuite de recherches importantes dans la communauté, notamment sur les changements climatiques, un phénomène préoccupant. Des chercheurs aux T.N.-O. mènent d'importantes recherches dans les domaines de la géoscience, des ressources minérales et pétrolières, des agrotechnologies, de la biomasse et des énergies de substitution. Selon la stratégie sur les possibilités économiques du gouvernement des T.N.-O., de nouveaux domaines de recherche excitants pourraient renforcer l'économie des T.N.-O., comme la recherche dans l'espace. En outre, les programmes d'innovation des techniques de fabrication et de contribution technologique serviront aussi à souligner des projets novateurs réalisés dans les T.N.-O.

Cela dit, le SCRS a déterminé que, malheureusement, des organisations étrangères hostiles ont un grand intérêt pour plusieurs de ces secteurs prometteurs. Les domaines liés à l'économie du savoir sont particulièrement vulnérables aux opérations d'espionnage et d'ingérence parrainés par des États hostiles qui cherchent à exploiter l'ouverture et l'esprit de collaboration qui permettent aux Canadiens d'innover. Aussi, le SCRS s'est engagé à aider ses partenaires à protéger leurs investissements de base dans l'infrastructure économique, le développement sectoriel

Canada

et la capacité de la population des T.N.-O. à tirer profit de l'économie canadienne fondée sur l'innovation.

Le préjudice à la prospérité collective du Canada est difficile à mesurer, mais il n'en est pas moins bien réel. Par conséquent, il est important que les Canadiens soient mieux informés des menaces de manière à ce qu'ils puissent continuer d'innover, de collaborer, d'établir des partenariats et de prospérer avec une bonne compréhension des risques et de la façon de s'en protéger. Le SCRS communique avec des parties des secteurs touchés pour améliorer la connaissance de la situation sécuritaire des différentes provinces et de l'ensemble du Canada. Il fournit des informations à des représentants de l'industrie, des organismes gouvernementaux et non gouvernementaux et des universités pour que toutes ces parties prennent les mesures nécessaires pour protéger leurs informations, les fruits de leurs recherches, leurs propriétés intellectuelles et leurs investissements. L'appareil de sécurité nationale du gouvernement du Canada et les communautés d'affaires et universitaires ont un intérêt commun : améliorer leurs connaissances des menaces d'espionnage d'origine étatique visant le Canada pour atténuer leurs répercussions sur la croissance de l'économie et leur capacité à innover. En d'autres mots, le SCRS vous offre son aide pour protéger les biens de votre organisme, son personnel et sa réputation.

/ QUELS SONT LES SECTEURS VISÉS?

- Les technologies
- La biopharmaceutique
- La santé
- Les transports aérospatiaux, ferroviaires et maritimes (y compris les véhicules verts, l'équipement maritime et les chaînes d'approvisionnement)
- Les universités
- L'énergie
- Les manufactures

/ QUELLES SONT LES CIBLES?

- L'équipement et les travaux de recherche avancés se rapportant aux technologies, aux sciences, au génie et aux mathématiques
- Les propriétés intellectuelles
- Les composantes des infrastructures essentielles
- Les données permettant l'identification (comme les dossiers financiers et médicaux)
- Les informations du gouvernement
- Les capacités de communication

Voici des exemples plus précis : des documents de conception, des plans de fabrication, des plans de mise en marché, des résultats de tests, des formules, des procédés, des renseignements sur les employés, des informations sur les fabricants et les fournisseurs, des logiciels, des données sur les investissements, des stratégies organisationnelles, des protocoles d'accès et des demandes de brevets ou de financement.

/ QUELLES SONT LES MÉTHODES UTILISÉES?

- Le cyberespionnage
- Le vol et le transfert illicite de connaissances et de technologies
- L'acquisition et l'exploitation de données sensibles canadiennes
- L'accès à des infrastructures essentielles et leur contrôle depuis l'étranger
- Les menaces de l'intérieur
- Les investissements étrangers hostiles
- La rétro-ingénierie
- Le sabotage et la déstabilisation
- L'exploitation de licences abusives
- La subtilisation d'informations (ou élicitation)

Veuillez noter que cette liste n'est pas exhaustive.

/ COMMENT PEUT-ON SE PROTÉGER?

- Déterminer quelles sont les informations les plus précieuses ou utiles et les protéger. Ne les communiquer qu'en cas de nécessité
- Améliorer et mettre à l'épreuve régulièrement ses politiques et pratiques de cybersécurité
- Faire preuve de rigueur

- Effectuer des vérifications sur les fournisseurs, les partenaires, les employés, les visiteurs et les bailleurs de fonds
- Encourager l'établissement d'une culture où la sécurité est importante
- Adopter des mesures de gestion du risque
- Mettre en œuvre des protocoles de sécurité physique rigoureux
- S'assurer que les termes des marchés et des ententes de collaboration sont équitables, réciproques et que les mesures de résolution des conflits sont applicables
- Protéger ses biens
- Se méfier des offres non sollicitées
- Communiquer avec les autorités en cas de préoccupations

/ QU'EST-CE QU'UN INVESTISSEMENT ÉTRANGER HOSTILE?

Au Canada, la plupart des investissements étrangers sont effectués avec ouverture et transparence, mais des sociétés d'État et celles liées à l'État et des entreprises privées étroitement liées à des gouvernements ou des services de renseignement étrangers tentent d'effectuer des acquisitions, entre autres transactions. Ces acquisitions font peser des risques : compromission des infrastructures essentielles, prises de contrôle dans des secteurs stratégiques, espionnage, ingérence étrangère et transferts illégaux de technologie et de savoir-faire. Aussi, la participation des sociétés d'État et celles liées à l'État aux investissements peut être cachée.

/ QU'EST-CE QU'UNE MENACE DE L'INTÉRIEUR?

Une tierce partie peut tenter d'exploiter une personne de confiance (un employé, un entrepreneur, un fournisseur, un partenaire, etc.) pour accéder aux informations les plus précieuses d'un organisme. Cette tierce partie, parfois appelée « agent de collecte non professionnel » peut utiliser différents moyens pour amener la personne de confiance à lui fournir les informations ou l'accès aux informations : coercition, manipulation, chantage et incitatifs. Voici des comportements qui peuvent révéler l'existence d'une menace de l'intérieur : heures de travail irrégulières, tentatives d'intrusion informatique, intérêt inhabituel pour des informations qui ne se rapportent pas aux fonctions de l'intéressé, dissimulation de relations étrangères, absences inexpliquées et train de vie anormalement élevé. Vous connaissez votre organisme. Soyez alerte et méfiez-vous des activités et des comportements suspects.

/ QU'EST-CE QUE LE CYBERESPIONNAGE?

Il est possible d'exploiter les systèmes informatiques, par exemple en employant une technique d'hameçonnage ou en installant un maliciel, pour obtenir clandestinement des informations confidentielles ou voler des propriétés intellectuelles.

/ QU'EST-CE QUE LA SUBTILISATION D'INFORMATIONS?

Une personne pourrait utiliser la flatterie, manifester un intérêt, poser des questions à indice ou feindre l'ignorance pour obtenir des informations. Ces techniques peuvent être employées dans des situations professionnelles comme dans un contexte social.

CONTACTEZ NOUS :

Canada.ca

Demandes d'informations : 613-993-9620

Communication d'informations relatives à la sécurité nationale : 1-800-267-7685

ISBN : 978-0-660-39460-2
N° de cat. : PS74-14/12-2021F-PDF
Aussi disponible en anglais et en inuktitut.
Also available in English and Inuktitut.