Service canadien du renseignement de sécurité
Canadian Security Intelligence Service

PROTÉGEZ VOS RECHERCHES

TERRE-NEUVE-ET-LABRADOR

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 du produit intérieur brut canadien attribuable à Terre-Neuve-et-Labrador s'élevait à 32 milliards de dollars. La province dispose d'installations et d'établissements d'enseignement réputés dans le domaine de la recherche et du développement et son secteur de la technologie et de l'innovation est en plein essor. En matière de recherche et de développement, les universités de la province n'accusent aucun retard par rapport aux autres universités du pays. Le secteur de la technologie et de l'innovation, qui injecte chaque année plus de 1,6 milliard dans l'économie, représente maintenant un important moteur de croissance économique pour la province. Cette dernière investit des ressources pour diversifier son économie, attirer des talents et du capital d'investissement et améliorer ses infrastructures d'innovation : il est donc important qu'elle protège ces investissements dans son avenir.

En plus des industries importantes comme le pétrole et le gaz (notamment l'équipement et la technologie connexes), l'exploitation minière, l'aquaculture, la fabrication de pointe ainsi que des secteurs liés au savoir comme les technologies de l'information et des communications, l'aérospatiale et les technologies propres représentent aussi des secteurs prometteurs pour la croissance et l'innovation dans la province.

La technologie et l'innovation liées à l'Arctique et aux océans constituent un exemple des domaines de recherche en plein essor dans la province. Parmi toutes les universités canadiennes, l'Université Memorial est celle qui détient l'expertise la plus vaste en lien avec l'Arctique et les eaux océaniques froides. Grâce au Cold-Ocean Deep-Sea Research Facility (installation de recherche sur les eaux océaniques froides et profondes) du Ocean Sciences Centre (Centre des sciences océaniques), les chercheurs ont accès à une infrastructure et à de l'équipement qui sont à la fine pointe de la technologie. De plus, l'innovation et l'expérience du secteur privé viennent renforcer ces atouts du monde universitaire. La province de Terre-Neuve-et-Labrador s'apprête à devenir un chef de file mondial grâce à des solutions technologiques prometteuses dans le domaine de la recherche et de la technologie glaciaires et océaniques : capteurs et imagerie, technologie des satellites, informatisation, systèmes autonomes, recherche dans les eaux froides et technologie sous-marine.

Canada

Malheureusement, ce succès fait aussi de Terre-Neuve-et-Labrador une cible : les secteurs de l'économie du savoir sont tout particulièrement vulnérables, parce que les milieux de travail qui favorisent la créativité et l'innovation sont les milieux ouverts et collaboratifs, dans lesquels l'information et les connaissances technologiques circulent beaucoup, aussi bien au pays qu'à l'étranger. Au Canada, les toutes nouvelles technologies des domaines de la santé, de la biopharmaceutique, de l'intelligence artificielle, de l'informatique quantique, des technologies marines et de l'aérospatiale font face aux plus grandes menaces.

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 : 978-0-660-39448-0
N° de cat. : PS74-14/9-2021F-PDF
Aussi disponible en anglais et en inuktitut.
Also available in English and Inuktitut.