Service canadien du renseignement de sécurité
Canadian Security Intelligence Service

PROTÉGEZ VOS RECHERCHES

MANITOBA

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 contribution du Manitoba au produit intérieur brut du Canada s'est élevée à environ 63 milliards de dollars. Les principaux moteurs de l'économie manitobaine sont les sciences biologiques, la biotechnologie, les technologies de l'information et de la communication (TIC), l'aérospatiale, l'extraction et l'exploration minières, les services financiers, l'agriculture industrielle, la fabrication de pointe, l'énergie et l'environnement ainsi que les services de transport et de distribution.

Le Manitoba possède un solide écosystème de recherche et d'innovation centré sur l'Université du Manitoba et d'autres établissements postsecondaires ainsi que plus de trente centres de recherche et de développement, dont le Centre scientifique canadien de santé humaine et animale et le Centre canadien de recherches agroalimentaires en santé et médecine. Un autre centre de recherche bien connu, Bioscience Association Manitoba, se spécialise dans la prévention des maladies infectieuses, la durabilité agroalimentaire et le développement de biocarburants. Le secteur des biosciences est vaste et diversifié dans la province et compte des entreprises des sous-secteurs de la biotechnologie de la santé, de l'agro-biotechnologie et de la biotechnologie propre. Winnipeg est le plus important centre de fabrication pharmaceutique de l'Ouest canadien. Elle héberge en outre de grands organismes de recherche en informatique qui appuient activement la télésanté et l'analyse de données.

De plus, la province possède un secteur des technologies en pleine croissance. À Winnipeg seulement, on compte quelque 1 300 entreprises de TIC spécialisées dans des domaines comme la gestion des données, le développement logiciel, la cybersécurité et les médias numériques interactifs. Alors que le gouvernement provincial continue d'investir dans l'innovation, il est primordial de protéger les investissements dans l'avenir de la province. Malheureusement, les secteurs de l'économie du savoir sont particulièrement vulnérables à l'ingérence d'acteurs étrangers hostiles, car la créativité et l'innovation sont particulièrement stimulées dans un environnement de collaboration ouvert. Dans un tel environnement, les informations et les connaissances technologiques sont régulièrement échangées à l'intérieur et à l'extérieur des frontières nationales.

Canada

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 : 978-0-660-39428-2
N° de cat. : PS74-14/4-2021F-PDF
Also available in English under the title: *Protect your research - Manitoba*