NON CLASSIFIÉ – RÉSERVÉ À DES FINS OFFICIELLES

RCMP·GRC

ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

ÉVALUATION NATIONALE DES INFRASTRUCTURES ESSENTIELLES

Activités d'ingérence étrangère
Menées par des États

À l'appui de la stratégie adoptée par le gouvernement du Canada pour assurer la résilience des infrastructures essentielles (IE), la GRC évalue et signale l'information relative aux menaces et à la criminalité dirigées contre les IE canadiennes. Cette information peut servir à protéger les IE du Canada. L'information contenue dans le présent bulletin est à jour en date du 2019-12-20.

PRINCIPALES CONSTATATIONS

- Les activités d'ingérence étrangère (AIE) représentent une menace importante pour la recherche et l'innovation au Canada dans les entreprises privées, les institutions gouvernementales et les universités. La perte, le vol ou la reproduction de la recherche et de la propriété intellectuelle (PI) peut causer des torts irréparables à long terme aux grandes industries canadiennes.

- Pour mettre à exécution leurs plans, plus particulièrement ceux liés aux sciences, à la technologie et à l'innovation, des États étrangers sont soupçonnés de se livrer à des AIE. Ces activités sont utilisées de manière stratégique et illégale pour obtenir des renseignements exclusifs ou protégés.

- Dresser la liste des actifs de valeur, adopter des pratiques rigoureuses en matière de cybersécurité et de sécurité matérielle, signaler les comportements suspects et sensibiliser à la sécurité les entreprises, le gouvernement et les universités constituent des mesures pouvant aider à détecter et à atténuer la menace que représentent les AIE.

CONTEXTE

Une AIE est une activité menée par un acteur étranger qui cible des intérêts ou des actifs canadiens. En outre, il s'agit d'efforts secrets, coercitifs ou clandestins de la part d'un acteur étranger pour servir ses propres intérêts stratégiques au détriment de ceux du Canada. Ces

activités sont menées par des représentants de l'État (c.-à-d. des personnes travaillant dans des organismes du renseignement ou recrutées par des agents du renseignement qui recueillent de l'information par des méthodes traditionnelles), ou par des mandataires (c.-à-d. des personnes qui recueillent de l'information par des méthodes non traditionnelles, ce qui comprend des étudiants, des chercheurs universitaires, des professionnels de l'industrie, des réseaux criminels ou quiconque pouvant consulter et obtenir de l'information utile).

À l'article 2 de la *Loi sur le Service canadien du renseignement de sécurité*, font partie des AIE les activités suivantes : *a) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage; b) les activités influencées par l'étranger 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.*[1]

Parmi la vaste gamme d'AIE, on trouve les activités suivantes : piratage et cyberattaques; intimidation de diasporas; manipulation des médias traditionnels et sociaux; efforts secrets de prolifération; recrutement de sources et de personnes influentes; ingérence dans les processus démocratiques d'un État; investissements ciblés permettant d'obtenir de la propriété intellectuelle ou de dominer des secteurs stratégiques de l'économie.

Étude de cas au Canada : chercheur ciblé

Dans les années 1990, Klaus Nielsen, Ph. D., chercheur à l'Agence canadienne d'inspection des aliments (ACIA) et scientifique de DIACHEMIX, a mis au point un antigène utilisé dans des trousses de tests de polarisation de fluorescence pour la brucellose. Cet antigène a fait l'objet d'un brevet américain en 1999, et de nouveau, en 2003.

En 2001, Weiling Yu a commencé à travailler à l'ACIA sous la supervision de M. Nielsen. M^me^ Yu était une technicienne subalterne d'une puissance étrangère suspecte, placée près de M. Nielsen.

En avril 2010, DIACHEMIX a signalé à l'ACIA que M. Nielsen et M^me^ Yu fabriquaient des trousses de dépistage de brucellose par l'intermédiaire d'une entreprise appelée Peace River Biotechnology Company (PRBTC), contrevenant ainsi à un accord de recherche concertée.

En 2012, M. Nielsen a été arrêté par la GRC alors qu'il se rendait à l'aéroport d'Ottawa. Il avait en sa possession 17 fioles cachées dans un thermos rempli de glaçons. Des tests ont confirmé la présence de bactéries Brucella vivantes qui peuvent infecter les humains et le bétail. M. Nielsen a été accusé d'abus de confiance pour avoir essayé de commercialiser la propriété intellectuelle de l'ACIA et de transport dangereux d'un agent pathogène humain.

L'information ci-dessus est tirée en partie de dossiers d'enquête de la GRC et de reportages dans les médias sur une affaire d'espionnage industriel au Canada.

ACQUISITION D'UN AVANTAGE CONCURRENTIEL

Ces dernières années, plusieurs pays, dont le Canada, ont remarqué la persistance de certains acteurs à vouloir obtenir de l'information classifiée et exclusive auprès d'entreprises et d'institutions étrangères. Pour demeurer concurrentiels, certains pays encouragent la collaboration avec des universités, des entreprises privées et des institutions gouvernementales municipales, provinciales et fédérales à l'étranger dans le cadre de projets de recherche conjoints et d'échanges académiques. Le Canada est vu comme étant un pays d'intérêt pour mener des projets conjoints et il est la troisième destination mondiale en importance en ce qui concerne la recherche scientifique et technologique.[2]

La collaboration, largement acceptée et encouragée dans le domaine de la recherche, favorise l'innovation, mais ce qui suscite des inquiétudes, c'est l'obtention ou la distribution illégale d'information classifiée ou exclusive par des moyens détournés ou secrets. Les centres de recherche canadiens signalent des cas de vol ou de reproduction d'information par des personnes utilisant des méthodes de collecte traditionnelles et non traditionnelles, dont quelques-unes pourraient travailler pour des États étrangers.[3]

La stratégie employée par des États-nations pour atteindre leurs objectifs de développement économique repose en grande partie sur le transfert de technologie.[4] Le transfert illégal de technologie et d'expertise offre un avantage à ces nations; il leur permet de faire avancer leurs projets de recherche plus rapidement que ceux du Canada, ce qui finit par être au détriment de l'innovation canadienne et se solde par des pertes économiques pour les entreprises et les institutions canadiennes.[5]

À titre d'exemple, la République populaire de Chine (RPC) ne cache pas son intention d'être un chef de file mondial en matière de sciences et de technologie. Dirigée actuellement par le Parti communiste chinois (PCC) dont le chef est Xi Jinping, la RPC a ouvertement fait part de ses aspirations à exercer un pouvoir et une influence à l'échelle internationale.[6] Pour concrétiser ces aspirations, la RPC se protège contre les menaces perçues, au pays et à l'étranger,[7] et s'en remet dans une large mesure à sa diaspora et à ses citoyens (dont bon nombre vivent selon le principe que chacun travaille pour le bien de l'État) pour réaliser ses objectifs économiques et stratégiques.[8]

Plusieurs compagnies chinoises font preuve d'excellence dans le domaine de la recherche et de l'innovation.[9] Au cours des dix prochaines années, on s'attend à ce que la Chine poursuive ses efforts en vue de devenir un chef de file mondial en matière de sciences et de technologie, ce qui augmentera encore davantage son influence internationale dans ces domaines.[10] Dans le cadre de cette stratégie, la RPC a élaboré « *Made in China 2025* », une politique industrielle visant à améliorer les industries de pointe et du secteur manufacturier,[11] en vue de remplacer les technologies importées par des technologies produites au pays.[12]

Le plan quinquennal présentant les projets de développement scientifiques et technologiques prévus d'ici 2030[13] devrait réduire la dépendance de la Chine à l'égard de la technologie étrangère et accroître l'importance et la pertinence des fabricants de technologie de pointe chinois dans le marché mondial[14]. D'ici 2025, la Chine a l'intention de produire 70 % des composantes de base et des matériaux nécessaires à ces projets.[15]

En 2008, la RPC a mis sur pied le programme de recrutement des experts mondiaux (*Recruitment Program of Global Experts)*, mieux connu sous le nom de *Thousand Talents Program*.[16] Celui-ci visait à recruter des talents (p. ex. des universitaires et des chercheurs) de l'étranger. Depuis sa création, le programme a attiré plus de 7000 participants et a aidé la RPC à établir sa pertinence et sa supériorité dans le domaine des sciences et de la technologie. On soupçonne que le *Thousand Talents Program* est utilisé à mauvais escient et qu'il constitue l'une des méthodes employées par la RPC pour faciliter le vol et la reproduction de technologies et de travaux de recherche importants provenant de pays occidentaux.[17]

Plan quinquennal de la Chine pour l'innovation en matière de sciences et de technologie d'ici 2030

Moteurs d'avion et turbines à gaz	Innovation dans le domaine des semences
Station en eau profonde	Science du cerveau et intelligence artificielle
Communications par satellite, à large bande et mobiles	Technologie de réseau intelligent
Médecine de précision et sécurité de la santé	Systèmes de fabrication intelligents et robotique
Communication et informatique quantique	Cybersécurité nationale
Exploitation de l'espace lointain	Nouveaux matériaux
Gouvernance environnementale	Charbon propre
Réseaux intégrés d'information spatiale et terrestre	Mégadonnées

Central Committee of the Communist Party of China, "The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China", http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765213498.pdf

D'ailleurs, en 2018, les organismes de renseignement américains ont indiqué que la Chine, en recrutant des scientifiques étrangers, et en volant de la propriété intellectuelle aux États-Unis (É.-U.) en faisant des acquisitions ciblées d'entreprises américaines, constitue une menace sans précédent à l'industrie.[18] Les scientifiques, les professionnels, les employés du gouvernement et autres recrutés peuvent fournir à la Chine de l'information exclusive de secteurs industriels clés obtenue illégalement.[19] Les industries canadiennes sont aussi vulnérables. Les secteurs suivants ont été ciblés dans le cadre du *Thousand Talents Program* : l'aérospatiale et la défense, la biotechnologie, les produits chimiques, les communications, les technologies de l'information, l'exploitation minière et la métallurgie, l'agriculture, l'énergie nucléaire, le pétrole et le gaz, ainsi que les sciences de l'environnement.[20]

Étude de cas : vols de secrets commerciaux

En août 2018, Xiaoqing Zheng, un ingénieur sino-américain qui travaillait à General Electric Co. depuis 2008 et avait été recruté par l'entremise du *Thousand Talents Program* en 2012, a été arrêté aux États-Unis et accusé d'avoir volé des secrets commerciaux sur les technologies liées aux turbines. Selon les médias, Zheng, qui voyageait fréquemment entre les É.-U. et la Chine, avait fondé en Chine deux entreprises spécialisées dans les technologies liées aux turbines.

D'autres cas semblables risquent de se produire au Canada; compte tenu de son expertise dans nombre de secteurs, il ne faut pas s'étonner que la Chine s'attende à ce que le Canada recrute des ressortissants chinois vivant et travaillant à l'étranger.

[1] Innovation, « Former GE engineer indicted on federal charges », https://www.timesunion.com/news/article/former-GE-engineer-indicted-on-federal-charges-13788690.php

Des employés d'entreprises, d'organismes gouvernementaux ou d'établissements d'enseignement au Canada qui sont reconnus pour leurs connaissances spécialisées ou leur expertise peuvent être vulnérables aux efforts de recrutement d'États étrangers. Les personnes qui sont ciblées sont souvent des victimes peu méfiantes, manipulées par des acteurs parrainés par l'État qui travaillent diligemment au fil du temps afin de gagner la confiance de celles-ci, les persuadant que la communication d'information classifiée ou exclusive est pour le bien de l'État.

L'insinuation, c'est-à-dire l'attitude amicale manifestée envers une cible afin d'exercer une influence sur elle, est une tactique viable qui peut être utilisée pour manipuler. Le professeur Steven H. Appelbaum, de l'Université Concordia, l'explique ainsi [Traduction] « *Il s'agit d'une tactique dans la mesure où la cible est souvent bien disposée à l'égard de la*

source, même si la tentative d'insinuation est grossière et évidente. La personne qui pratique l'insinuation fait des gestes positifs envers la cible pour que celle-ci se sente obligée de lui renvoyer l'ascenseur. »[21] Si ces efforts ne fonctionnent pas, ils peuvent changer de tactique et recourir aux menaces et à l'intimidation.

EXERCER SON POUVOIR À L'ÉTRANGER

Pour certains États-nations, il est essentiel de faire front commun pour assurer sa pertinence politique et exercer son pouvoir et son influence à l'échelle mondiale. Conformément à ce principe, ces États-nations exercent un contrôle serré sur leurs citoyens, et ceux qui vivent à l'étranger sont censés travailler pour le bien de l'État.[22] Ils s'attendent souvent à ce que les membres de leurs diasporas recueillent des renseignements d'autres pays.

Afin de démontrer que leur contrôle et leur influence s'étendent au-delà de leurs frontières, certains États-nations suivent de près ce qui se passe dans leurs diasporas à l'étranger. L'objectif est de recueillir de l'information et des renseignements, mais aussi d'empêcher les dissidents de dénoncer leurs gouvernements. Selon les médias, certains États-nations tentent d'empêcher toute forme de dissidence tant à l'intérieur qu'à l'extérieur de leurs frontières[23], ce qui revient dans les faits à interdire toute critique.[24]

À titre d'exemple, en 2012, la RPC a intensifié ses efforts pour lutter contre la corruption en faisant appel à sa Commission centrale de contrôle de la discipline *(Central Commission for Discipline Inspection* [CCDI]) pour cibler des représentants du gouvernement accusés de corruption. Dans le cadre de cette campagne anti-corruption, la RPC a élaboré *Project Fox Hunt* et *Sky Net 2017*. Ces projets visaient à localiser et à obtenir l'extradition de fonctionnaires présumés corrompus ayant fui la RPC avant que des poursuites puissent être intentées contre eux.[25] Selon des renseignements de sources ouvertes, depuis le lancement de cette campagne, plus de 4000 personnes ont été arrêtées[26] et rapatriées de plus de 120 pays et quelque 2,4 milliards de $ US ont été récupérés.[27]

Cependant, au fil du temps, la portée de cette initiative semble s'être élargie pour cibler les personnes poursuivies par la CCDI en raison de dissidence politique ou d'autres activités qui s'opposent au gouvernement chinois.[28] Selon certains rapports, les agents gouvernementaux chinois utilisent des tactiques d'intimidation agressives pour réprimer ce qu'ils considèrent comme étant des messages de dissidence et de propagande qui jettent le discrédit sur la RPC.[29] D'autres rapports indiquent que la seule raison d'être de la CCDI est d'éliminer les adversaires politiques.[30]

Pour trouver ces personnes, les États-nations peuvent dans un premier temps utiliser des méthodes policières traditionnelles, notamment en délivrant des mandats d'arrestation internationaux à leur encontre.[31] Cependant, on observe une intensification des méthodes de rapatriement. Les services de sécurité de certains États-nations auraient envoyé des agents à l'étranger pour contraindre les suspects à rentrer au pays pour faire face à des accusations criminelles,[32] ce qui inquiète les organismes d'application de la loi et du renseignement et les organisations non gouvernementales (ONG) en Occident. Les agents ou mandataires de ces services de sécurité se rendent parfois à l'étranger en utilisant un visa touristique ou de visiteur,[33] afin de faire pression, par la menace ou l'intimidation, sur les ressortissants recherchés pour qu'ils rentrent au pays; ils vont jusqu'à détenir ou menacer des membres de leurs familles et utilisent stratégiquement la diaspora pour parvenir à leurs fins.[34]

Human Rights Watch, une ONG qui fait de la recherche et défend les droits de la personne[35], s'oppose fortement aux méthodes utilisées par la CCDI, et affirme qu'il est notoire que celle-ci viole la loi et a recours à la torture et à des moyens coercitifs.[36] Une technique controversée utilisée parfois par la CCDI consiste à rendre publics les noms et adresses d'individus vivant à l'étranger, y compris au Canada,[37] qui sont réputés être des criminels et faire partie des personnes les plus recherchées en Chine. Selon le CCDI, la RPC publie ces noms et adresses dans le but de gêner et de faire honte publiquement à ces personnes et ainsi les convaincre de rentrer en Chine pour faire face à des accusations criminelles.[38]

Des activités comparables aux AIE ciblant des membres de la diaspora peuvent être menées par des représentants de l'État ou des mandataires : intercepter illégalement des communications privées; suivre ou surveiller une personne; menacer d'avoir recours à la violence ou utiliser des tactiques d'intimidation, dans certains cas, afin d'obliger une personne à commettre un acte pour soutenir l'État. Il arrive que des membres des diasporas signalent aux services de police les cas d'intimidation et de harcèlement à leur endroit ou à l'endroit de proches. Cependant, l'un des grands défis pour les organismes d'application de la loi qui cherchent à déposer des accusations criminelles contre les personnes qui emploient ces techniques réside dans la réticence des victimes à signaler les incidents, celles-ci craignant bien souvent des représailles à leur égard ou à l'égard de membres de leur famille.[39]

CRÉER UN DISCOURS

En cette époque caractérisée par les « fausses nouvelles », on observe un regain d'intérêt pour les médias, la propagande et les campagnes de désinformation. Il est devenu de plus en plus difficile de déterminer la légitimité de l'information diffusée aux masses. Internet et les médias sociaux ont la capacité à la fois d'aider et d'entraver certaines plateformes, y compris politiques. La désinformation, c'est-à-dire « *l'information fausse et délibérément produite pour nuire à une personne, un groupe social, une organisation ou un pays* »[40] peut créer des divisions, déformer les nouvelles, diffuser de la propagande, susciter la méfiance et affaiblir la crédibilité des démocraties libérales.[41] La mauvaise information, c'est-à-dire « *l'information qui est fausse, mais qui n'a pas été créée dans l'intention de causer du tort* »[42] peut nuire malgré tout. Des journalistes, des réseaux d'information, des diplomates et des membres de diasporas peuvent être ciblés si on juge qu'ils ont la capacité d'influencer diverses plateformes politiques ou qu'ils appuient certains intérêts de l'État.[43] Le paysage médiatique canadien est réputé pour valoriser et promouvoir la liberté d'expression et toute tentative de porter atteinte à son impartialité peut être assimilé à une forme d'ingérence.

À titre d'exemple, on soupçonne la Russie de cibler des réseaux d'information, notamment en Amérique du Nord, afin de dissuader toute couverture médiatique négative à son sujet, et d'inciter des journalistes à utiliser un discours positif pour dépeindre la Russie.[44] Par ailleurs, le gouvernement russe cible la diaspora ukrainienne au Canada, surtout depuis que ce pays et d'autres alliés ont imposé des sanctions à la Russie après l'annexion de la Crimée en 2014.[45] La Russie a tout particulièrement ciblé les Ukraino-Canadiens accusés d'être à l'origine des politiques antirusses du gouvernement canadien.[46]

Par ailleurs, des diplomates nord-américains en poste dans plusieurs villes européennes ont signalé avoir été agressivement ciblés par des acteurs étatiques étrangers, dont certains travailleraient pour les services de sécurité et de renseignement russes. De multiples cas d'intimidation et de harcèlement ont été signalés, dont les plus graves ciblaient des diplomates

qui ont tenté de dénoncer aux autorités les activités malveillantes de la Russie.[47] Les campagnes de désinformation et les tactiques de harcèlement et d'intimidation utilisées par des acteurs étatiques contre des diasporas et des corps diplomatiques sont utilisées pour manipuler le discours sur certains États.

Parallèlement, on soupçonne des États étrangers d'être à l'origine de cyberespionnage et d'intrusions,[48] d'employer des agents partout dans le monde afin de recueillir des renseignements, d'infiltrer les réseaux industriels et de prépositionner des outils informatiques.[49] L'industrie privée, les institutions gouvernementales et les universités sont vulnérables à ces actions. Plus préoccupant encore, ces tactiques peuvent être utilisées pour entraver des processus démocratiques.[50] On soupçonne ainsi la Russie d'avoir tenté de miner le processus démocratique en Amérique du Nord en s'ingérant dans l'élection présidentielle de 2016 aux É.-U.[51] Au Canada, des organismes du renseignement ont observé à « plusieurs reprises des États étrangers cibler des communautés, tant en personne et que par des campagnes en ligne. »[52] Des informations de source ouverte indiquent également que des campagnes de piratage commanditées par des États ont ciblé des partis politiques canadiens.[53] Étant donné leur hostilité à l'égard de l'Occident et leur capacité à infiltrer des médias et divers secteurs à l'étranger, certains États étrangers pourraient lancer des campagnes de désinformation ou des cyberintrusions afin de compromettre le déroulement de futures élections dans le monde.[54]

ÉVALUATION

Les entreprises, les universités et les organismes gouvernementaux canadiens sont susceptibles d'être victimes d'AIE menées par des États étrangers pour atteindre des objectifs stratégiques et économiques.[55] En raison de son développement industriel et technologique, le Canada constitue une cible attrayante pour l'espionnage économique et l'AIE. Si leurs motivations peuvent différer, les États étrangers continuent de chercher des moyens d'exercer leur pouvoir et de recueillir des renseignements, préservant certaines capacités pour le moment qu'ils jugeront opportun. Les AIE constituent pour la société canadienne une menace importante qui souvent n'est pas détectée et est rarement signalée. Sans stratégies d'atténuation, sensibilisation et pratiques rigoureuses en matière de sécurité matérielle et cybersécurité, ces activités se poursuivront probablement de façon continue dans des secteurs-clés. Il est essentiel de dresser la liste des biens de valeur et des renseignements utiles, et de signaler toute activité suspecte.

Les invitations à des expositions, à des séminaires, à des congrès internationaux ou à participer à des projets de recherche, aussi anodines qu'elles puissent paraître, peuvent en fait cacher une volonté de se rapprocher du personnel ciblé afin de lui soutirer de l'information sensible. Les visites ciblées et bien préparées de diplomates, de clients potentiels ou de chercheurs étrangers dans des entreprises canadiennes peuvent mener au vol ou à la perte d'information essentielle. Les entrepreneurs ou les sous-traitants peuvent aussi être bien placés pour obtenir illégalement de l'information exclusive ou classifiée. Les demandes spontanées d'information exclusive ou sensible par des personnes non identifiées, ainsi que la surveillance et les entrées subreptices sont des moyens efficaces de recueillir des renseignements. Les tactiques utilisées pour recueillir de l'information sont souvent subtiles, mais elles peuvent devenir plus audacieuses et malicieuses au fil du temps.

Indices d'activité suspecte

- Être présent au travail de façon répétée ou sans justification en dehors des heures normales.
- Tenter d'accéder à des renseignements classifiés en se portant volontaire à maintes reprises pour des affectations ou des tâches qui ne relèvent pas de ses responsabilités normales.
- Tenter de pénétrer dans des zones à accès restreint ou de se brancher au réseau de l'entreprise sans autorisation ou sans l'habilitation sécuritaire voulue.
- Occuper un emploi à temps partiel ou effectuer des activités externes (consultation, p. ex.) qui risquent de créer un conflit d'intérêts avec son obligation de protéger des renseignements classifiés et sensibles.
- Utiliser de façon excessive les photocopieurs, les télécopieurs ou les systèmes informatiques pour reproduire ou transmettre des renseignements classifiés, sensibles ou exclusifs qui ne cadrent pas avec les exigences de son poste.
- Apporter des caméras ou des dispositifs d'enregistrement, sans autorisation, dans des zones où sont rangés des renseignements classifiés ou protégés.
- Faire de courts séjours inexpliqués ou inusités à l'étranger ou tenter de cacher ses voyages à l'étranger.
- Adopter soudainement un nouveau style de vie qui ne cadre pas avec son salaire (vivre au-dessus de ses moyens).

Indices de cyberintrusion

- Appareil dont le fonctionnement continue de ralentir, qui gèle constamment ou plante fréquemment.
- Hausse importante de la consommation de données sans que l'utilisation de l'appareil n'ait changé.
- Les pages Web et les vidéos prennent plus de temps à se charger qu'à l'habitude.
- L'utilisateur ne se souvient pas d'avoir effectué certaines des activités du compte (p. ex. des courriels qu'il ne se souvient pas d'avoir envoyés).
- Des logiciels ou des programmes complémentaires que l'utilisateur ne reconnaît pas ou qu'il n'a pas installés s'affichent dans son système.
- Des fenêtres non sollicitées s'affichent et demandent aux utilisateurs de changer les paramètres de leur système ou d'accorder des permissions à un programme particulier.
- Le logiciel de sécurité se désactive de lui-même ou ne fonctionne pas normalement (p. ex. il refuse d'effectuer une vérification du système).

Certains comportements, signes ou indices, pris dans leur ensemble et en contexte, peuvent révéler une menace d'AIE dans des entreprises privées, des institutions gouvernementales ou des universités. À lui seul, un comportement ou un indicateur ne constitue pas nécessairement la preuve d'une AIE; par contre, un faisceau d'indices, comportementaux et autres, peut révéler une activité suspecte justifiant une enquête.[56] En voici quelques exemples : personnes insatisfaites ou mécontentes de leur rôle professionnel (qui cherchent à se venger); rétention d'information exclusive ou de nature délicate sans autorisation ou à l'insu de l'employeur; entreposage de documents classifiés à la maison ou dans d'autres lieux non autorisés; ou exagération de son statut ou de ses relations professionnelles.

De nombreuses AIE ne sont découvertes qu'après coup. De plus, une entreprise n'essuiera pas que des pertes financières; sa réputation pourrait également en pâtir (embarras d'avoir manqué à ses obligations, ne plus être considérée à l'avant-garde de l'innovation), de même que la confiance des clients ou des actionnaires, sans compter le temps consacré en pure perte à la recherche. C'est pourquoi certaines organisations peuvent être réticentes à signaler de possibles AIE, de peur que leurs clients ou leurs concurrents n'y voient une vulnérabilité. De plus, même lorsqu'un incident se produit ou une intrusion est découverte, l'étendue des dommages ou de la perte peut ne pas être connue.

Pour atténuer le risque, il est essentiel de signaler aux autorités toute intrusion ou AIE potentielle. Les services de police et d'autres organismes de sécurité peuvent fournir à l'industrie des conseils sur le processus officiel de plainte, les mesures à prendre, la protection de l'information, et le mandat et la compétence territoriale de l'organisme.

Afin d'enquêter de façon exhaustive sur un possible cas d'AIE, les autorités policières doivent pouvoir compter sur la coopération de l'entreprise touchée qui doit fournir de l'information sur l'incident ou l'intrusion, ainsi que son ampleur (en termes d'impact et d'étendue des dommages ou de perte si celle-ci est quantifiable).

RECOMMANDATIONS

Il est important que tous les partenaires, y compris les organismes d'application de la loi et le personnel de sécurité du secteur privé, demeurent vigilants et signalent tout ce qui leur semble suspect. Le personnel de première ligne est le mieux placé pour observer les comportements suspects. Il connaît ce qui l'entoure et sait ce qui est normal d'y trouver au quotidien.

Un incident particulier peut sembler insignifiant, mais s'il fait suite à plusieurs autres incidents documentés, il pourrait signaler une menace sérieuse. Pour signaler une activité suspecte, un cas d'extrémisme criminel ou toute autre activité susceptible de menacer la sécurité nationale du Canada, communiquez avec :

L'ENIE encourage les destinataires du présent document à signaler tout renseignement concernant des activités criminelles ou suspectes aux organismes d'application de la loi de leur région.
Pour signaler une activité suspecte, un cas d'extrémisme criminel ou toute autre activité susceptible de menacer la sécurité nationale du Canada, communiquez avec :

le Réseau infosécurité nationale, au 1-800-420-5805
le Service canadien du renseignement de sécurité (SCRS), au 613-993-9620

Rédigé par :

Équipe nationale des infrastructures essentielles
Sécurité nationale de la Police fédérale
Courriel : SIR-SIS@rcmp-grc.gc.ca

Pour une assistance immédiate, veuillez composer le 9-1-1 ou communiquer avec le service de police local.

[1] Site Web de la législation (Justice) du gouvernement du Canada. https://laws-lois.justice.gc.ca/fra/lois/c-23/TexteComplet.html
[2] Australian Strategic Policy Institute, « Picking flowers, making honey », https://www.aspi.org.au/report/picking-flowers-making-honey
[3] *The Globe and Mail*, « China' military scientists target Canadian universities », https://www.theglobeandmail.com/world/article-chinas-military-scientists-target-canadian-universities/
[4] Département de la Justice des É.-U, « CHINA : The Risk to Corporate America » https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf
[5] *The Globe and Mail*, « China' military scientists target Canadian universities », https://www.theglobeandmail.com/world/article-chinas-military-scientists-target-canadian-universities/
[6] BBC News, « The thoughts of Chairman Xi », https://www.bbc.co.uk/news/resources/idt-sh/Thoughts_Chairman_Xi
[7] Australian Strategic Policy Institute: The Strategist, "Spying beyond the façade," 2013-11-13, https://www.aspistrategist.org.au/spying-beyond-the-facade/
[8] Texas National Security Review: War on the Rocks, "Beijing's Influence Operations Target Chinese Diaspora," 2018-03-01 https://warontherocks.com/2018/03/beijings-influence-operations-target-chinese-diaspora/
[9] Forbes, « China is Innovating Faster than you Imagine », https://www.forbes.com/sites/michaelcwenderoth/2018/04/11/china-is-innovating-faster-than-you-imagine/#43cfbe68273d
[10] Bureau du secrétaire américain à la Défense, « Annual Report to Congress: Military and Security Developments Involving the People's Republic of China »
[11] Council on Foreign Relations, « Is 'Made in China 2025' a Threat to Global Trade? », https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
[12] Bureau du secrétaire américain à la Défense, « Annual Report to Congress: Military and Security Developments Involving the People's Republic of China »
[13] Département de la Justice des É.-U, « CHINA : The Risk to Corporate America », https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf
[14] Council on Foreign Relations, « Is 'Made in China 2025' a Threat to Global Trade? », https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
[15] Council on Foreign Relations, « Is 'Made in China 2025' a Threat to Global Trade? », https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
[16] Bloomberg, « China's Thousand Talents called key in seizing U.S. expertise », https://www.bnnbloomberg.ca/china-s-thousand-talents-called-key-in-seizing-u-s-expertise-1.1097112
[17] United States Senate Permanent Subcommittee on Investigations, "Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans," 2019-11-18 https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans.pdf
[18] Council on Foreign Relations, « Is 'Made in China 2025' a Threat to Global Trade? », https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
[19] Département de la Justice des É.-U, « CHINA : The Risk to Corporate America », https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf
[20] CBC News, « Canada among targets of alleged Chinese hacking campaign », https://www.cbc.ca/news/politics/canada-among-china-hacking-victims-1.4954608
[21] Semantics Scholar, « Ingratiation as a political tactic: effects within the organization », https://pdfs.semanticscholar.org/366c/51a13570c3f520da1f0333760ac9cbd65010.pdf
[22] Axios, « How China became a global power of espionage », 2018-03-23, https://www.axios.com/china-chinese-spies-intelligence-xi-cia-bc4b9c3f-67c3-4a93-bc54-c7a38d975bd6.html
[23] Hudson Institute, « The Chinese Communist Party's Foreign Interference Operations: How the U.S. and Other Democracies Should Respond », 2018-06-20, https://www.hudson.org/research/14409-the-chinese-communist-party-s-foreign-interference-operations-how-the-u-s-and-other-democracies-should-respond
[24] *Business Insider*, « Barging into your home, threatening your family, or making you disappear: Here's what China does to people who speak out against them », https://www.businessinsider.com/how-china-deals-with-dissent-threats-family-arrests-2018-8
[25] *Financial Times*, « China steps up 'fox hunt' campaign », https://www.ft.com/content/f6a1c75c-c573-11e5-808f-8231cd71622e
[26] Ecns.cn, « China's Sky Net campaign nabs more than 4,000 fugitives since 2015 », https://www.ecns.cn/2018/04-25/300303.shtml
[27] China.org.cn, « Fox Hunt film launched in Beijing », http://www.china.org.cn/arts/2019-05/28/content_74830220.htm
[28] Human Rights Watch, « China : Secretive Detention System Mars Anti-Corruption Campaign », https://www.hrw.org/news/2016/12/06/china-secretive-detention-system-mars-anti-corruption-campaign
[29] *The New Yorker*, « China's bizarre program to keep activists in check », https://www.newyorker.com/magazine/2018/12/24/chinas-bizarre-program-to-keep-activists-in-check
[30] Human Rights Watch, « China : Secretive Detention System Mars Anti-Corruption Campaign », 2016-12-06, https://www.hrw.org/news/2016/12/06/china-secretive-detention-system-mars-anti-corruption-campaign
[31] *Huffington Post*, « China's "Fox Hunt" makes great achievements », https://www.huffingtonpost.com/entry/chinas-fox-hunt-makes-great-achievements_us_58f61286e4b0156697225299
[32] *National Post*, « Chinese police run secret operations in B.C. to hunt allegedly corrupt officials and laundered money », https://nationalpost.com/news/canada/chinese-police-run-secret-operations-in-b-c-to-hunt-allegedly-corrupt-officials-and-laundered-money
[33] *The Globe and Mail*, « Chinese agents enter Canada on tourist visas to coerce return of fugitive expats », https://www.theglobeandmail.com/news/politics/chinese-agents-enter-canada-on-tourist-visas-to-coerce-return-of-fugitive-expats/article31981251/
[34] Global News, 2019-08-25 "Chinese influence in Canada 'alive and well,' says student leader threatened by trolls," https://globalnews.ca/news/5804742/chinese-influence-canada/
[35] Human Rights Watch, « Frequently Asked Questions », https://www.hrw.org/frequently-asked-questions
[36] CBC News, « 5 from B.C. on China's 'most wanted' list of 22 alleged criminals », 2017-04-29, https://www.cbc.ca/news/canada/british-columbia/china-graft-corruption-bc-michael-ching-mo-yeung-ching-trudeau-liberals-canada-1.4091272
[37] CBC News, « 5 from B.C. on China's 'most wanted' list of 22 alleged criminals », 2017-04-29, https://www.cbc.ca/news/canada/british-columbia/china-graft-corruption-bc-michael-ching-mo-yeung-ching-trudeau-liberals-canada-1.4091272
[38] Reuters, « Shame on you! China uses public billboards to expose runaway debtors », https://www.reuters.com/article/us-china-debt-shaming/shame-on-you-china-uses-public-billboards-to-expose-runaway-debtors-idUSKCN0ZZ0BS
[39] Global News, 2019-08-25 "Chinese influence in Canada 'alive and well,' says student leader threatened by trolls," https://globalnews.ca/news/5804742/chinese-influence-canada/
[40] Organisation des Nations Unies pour l'éducation, la science et la culture, « Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training », https://en.unesco.org/fightfakenews
[41] Service canadien du renseignement de sécurité, « Qui dit quoi? Défis sécuritaires découlant de la désinformation aujourd'hui », https://www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_fra.pdf
[42] [47] Organisation des Nations Unies pour l'éducation, la science et la culture, « Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training », https://en.unesco.org/fightfakenews

[43] *The New York Times*, « What Does Putin Really Want? », https://www.nytimes.com/2019/06/25/magazine/russia-united-states-world-politics.html
[44] Service canadien du renseignement de sécurité, « Qui dit quoi? Défis sécuritaires découlant de la désinformation aujourd'hui », https://www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_fra.pdf
[45] CBC News, « Top Russian news host takes aim at Ukrainian Canadians », https://www.cbc.ca/news/world/top-russian-news-host-takes-aim-at-ukrainian-canadians-1.4980859
[46] CBC News, « Top Russian news host takes aim at Ukrainian Canadians », https://www.cbc.ca/news/world/top-russian-news-host-takes-aim-at-ukrainian-canadians-1.4980859
[47] *Washington Post*, « Russia is harassing U.S. diplomats all over Europe », https://www.washingtonpost.com/opinions/global-opinions/russia-is-harassing-us-diplomats-all-over-europe/2016/06/26/968d1a5a-3bdf-11e6-84e8-1580c7db5275_story.html
[48] DW.COM, « Full-scope cyber actor: US intelligence officials testify on Russia's cyber activities », 2017-05-01, https://www.dw.com/en/full-scope-cyber-actor-us-intelligence-officials-testify-on-russias-cyber-activities/a-37026281
[49] National Counterintelligence and Security Center, « Foreign Economic Espionage in Cyberspace », https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf
[50] PBS News Hour, « Inside the Mueller report, a sophisticated Russian interference campaign », https://www.pbs.org/newshour/show/inside-the-mueller-report-a-sophisticated-russian-interference-campaign
[51] Reuters, « Russia's Putin says he sympathized with Trump before U.S. election », https://www.reuters.com/article/us-putin-trump-vote/russias-putin-says-he-sympathized-with-trump-before-u-s-election-idUSKCN1UE2HZ
[52] *The Star*, « Canadians are being targeted by foreign influence campaigns, CSIS says », https://www.thestar.com/politics/federal/2019/07/02/canadas-voters-being-targeted-by-foreign-influence-campaigns-spy-agency-says.html
[53] *The Star*, « Canadians are being targeted by foreign influence campaigns, CSIS says », https://www.thestar.com/politics/federal/2019/07/02/canadas-voters-being-targeted-by-foreign-influence-campaigns-spy-agency-says.html
[54] *The Star*, « Countering the growing threat of Russian disinformation in Canada », https://www.thestar.com/opinion/contributors/2018/01/11/countering-the-growing-threat-of-russian-disinformation-in-canada.html
[55] *The Star*, « Canada turfed out more spies to the U.S. than elsewhere », 2015/03/03, https://www.thestar.com/news/canada/2015/03/03/canada-turfed-out-more-spies-to-the-us-than-elsewhere.html
[56] Département de la Sécurité intérieure des É.-U., National Cybersecurity and Communications Integration Center, « Combating the Insider Threat », 2014/05/02, https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf