Cyberincidents géopolitiques au Canada

ÉTAT DES LIEUX 2023

Proposé par l'Observatoire des conflits multidimensionnels

UQÀM

CHAIRE **RAOUL-DANDURAND**
EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

Table des matières

Qui sommes-nous?

L'Observatoire des conflits multidimensionnels (OCM) de la Chaire Raoul-Dandurand a été créé en 2019, grâce à l'appui de la Banque Nationale du Canada. Dirigé par Frédérick Gagnon, professeur de science politique à l'UQAM et titulaire de la Chaire Raoul-Dandurand, l'OCM rassemble des chercheures et chercheurs canadiens et internationaux étudiant la mutation des stratégies de puissance que les acteurs internationaux, surtout étatiques, déploient sur la scène internationale pour déstabiliser des États, fragiliser leurs sociétés, institutions et processus politiques, ou porter atteinte à leurs systèmes et infrastructures critiques. Les manipulations de l'information, les cyberattaques, les offensives géoéconomiques dont l'espionnage économique, et l'ingérence politique et électorale figurent parmi les phénomènes étudiés par l'OCM. Contribuant au développement d'une réflexion canadienne sur ces enjeux au moyen de publications scientifiques et grand public, de conférences et colloques, et d'interventions médiatiques, l'OCM informe et sensibilise sur la manière dont les mutations sécuritaires contemporaines, notamment l'usage malveillant des technologies numériques, affectent des États comme le Canada, leur gouvernement, la société civile, le secteur privé et les citoyennes et citoyens.

Avec les contributions de

Frédérick Gagnon est titulaire de la Chaire Raoul-Dandurand, directeur de l'Observatoire des conflits multidimensionnels (OCM) et professeur de science politique à l'Université du Québec à Montréal (UQAM). Il est un expert reconnu de la vie politique aux États-Unis, de la politique étrangère des États-Unis et des relations canado-américaines. Ses récents travaux à l'OCM ont porté sur l'ingérence russe et les manipulations de l'information lors des élections américaines de 2016, la gestion américaine de la cyberconflictualité, les effets de la compétition géoéconomique sino-américaine sur les relations entre le Canada et les États-Unis, et la politique géoéconomique des États-Unis à l'égard du Canada.

Alexis Rapin est chercheur en résidence à l'Observatoire des conflits multidimensionnels. Il travaille notamment sur les transformations de la conflictualité, tels la cyberdéfense et l'essor des stratégies de désinformation. Il a notamment contribué à plusieurs ouvrages collectifs en français et en anglais portant sur les conflits armés et la cybersécurité. Début 2023, il a témoigné sur les enjeux relatifs à la cyberdéfense du Canada devant le Comité permanent de la défense nationale de la Chambre des communes.

Danny Gagné est candidat au doctorat en science politique à UQAM et chercheur en résidence à l'Observatoire des conflits multidimensionnels. Ses recherches portent sur la stratégie américaine de guerre par drones de combat. Ses récents travaux à l'OCM, portant notamment sur la manipulation de l'information à des fins géopolitiques, ont fait l'objet de plusieurs chroniques des nouvelles conflictualités publiées par la Chaire Raoul-Dandurand.

Fanny Tan est chercheure en résidence à l'Observatoire des conflits multidimensionnels et étudiante en science politique à l'UQAM. Détentrice d'un baccalauréat en médias numériques (UQAM) et d'un certificat en design de jeux vidéo (UQAT), Fanny Tan écrit régulièrement sur les enjeux sociaux des nouvelles technologies dans les médias en tant que journaliste indépendante. Elle est collaboratrice techno à l'émission Moteur de recherche (ICI Première) et membre des collectifs de protection de la vie privée Crypto.Québec et le Lab 2038.

HUIT INCIDENTS MARQUANTS

2022

JANVIER

CYBERINCIDENT À AFFAIRES MONDIALES CANADA

Affaires mondiales Canada est victime d'une cyberattaque, dont des sources gouvernementales envisagent qu'elle provienne de Russie. Certains services en ligne du ministère sont rendus temporairement indisponibles par les mesures de mitigation. L'incident se produit alors que la ministre des Affaires étrangères Mélanie Joly est en visite à Kiev et que la Russie a massé des troupes aux frontières de l'Ukraine.

JUIN

OPÉRATION D'INFLUENCE CONTRE APPIA RARE EARTHS

La firme de cybersécurité Mandiant révèle l'existence d'une opération d'influence ayant visé trois grandes sociétés minières, dont la compagnie canadienne de minage de terres rares Appia Rare Earths & Uranium Corp. Cette opération ferait partie d'une campagne de manipulation de l'information menée par l'entité Dragonbridge et cherchant à propager des narratifs favorables aux intérêts de la République populaire de Chine.

SEPTEMBRE

CAMPAGNE D'EXTORSION MANDATÉE PAR L'IRGC

Des agences de cybersécurité américaines, canadiennes, australiennes et britanniques révèlent l'existence d'une campagne de cyberintrusions attribuée au Corps des Gardiens de la révolution islamique (IRGC). Les pirates iraniens auraient notamment cherché à mener des attaques par rançongiciel contre diverses organisations dans les quatre pays concernés.

DÉCEMBRE

PIRATAGE D'AMNESTY CANADA PAR LA CHINE

Amnesty Canada annonce avoir fait l'objet d'un piratage informatique sophistiqué, qui a forcé l'ONG à mettre ses systèmes hors-ligne pendant près de 3 semaines. D'après la firme de cybersécurité Secureworks, cette cyberattaque serait attribuable à un groupe de pirates affilié à l'État chinois. Ceux-ci semblaient chercher à obtenir des informations confidentielles sur les contacts et les projets de l'organisation.

AVRIL

PIRATAGES D'ENTREPRISES ÉNERGÉTIQUES PAR L'IRAN

Meta annonce avoir sévi contre un groupe basé en Iran, ayant mené des piratages contre diverses entreprises dans une dizaine de pays. Les cibles du groupe incluent notamment une ou plusieurs entreprises énergétiques canadiennes. Un des logiciels malveillants déployés permettait par exemple d'accéder à des fichiers et de les exfiltrer, et de prendre des captures d'écran à l'insu des victimes.

MAI

ATTAQUE PAR RANÇONGICIEL CONTRE CMC ÉLECTRONIQUE

CMC Électronique, entreprise aéronautique canadienne active dans le secteur de la défense, est visée par une attaque par rançongiciel. L'attaque est revendiquée par le groupe cybercriminel russophone ALPHV. CMC vient alors d'être désignée pour participer au programme de modernisation de la flotte d'hélicoptères CH-146 Griffon des Forces canadiennes.

JUILLET

ESPIONNAGE D'ENTREPRISES ÉNERGÉTIQUES PAR LAZARUS GROUP

La firme de cybersécurité Talos (Cisco) révèle que le groupe de pirates nord-coréen Lazarus a mené, entre février et juillet 2022, une campagne de cyberespionnage contre des entreprises énergétiques canadiennes, américaines et japonaises. Selon Talos, cette campagne avait pour objectif le vol de propriété intellectuelle.

OCTOBRE

CYBERINCIDENT AU PARLEMENT CANADIEN

Le *Toronto Star* révèle qu'un cyberincident d'origine non spécifiée a frappé le Parlement canadien. Les membres du Parlement se sont vu demander de changer le mot de passe de leur adresse courriel, et certains services en ligne du Parlement ont été interrompus. Aucun détail n'est alors livré sur les acteurs potentiellement responsables de l'incident.

Le Canada et les cyberincidents géopolitiques à l'horizon 2023

Qu'entend-on par cyberincident ?

Nous définissons comme « cyberincidents » des actions intentionnelles, malveillantes, circonscrites dans le temps, menées au moins en partie dans le cyberespace. Le terme cyberincident inclut donc à la fois les cyberattaques, le vol de données ou encore les actes de manipulation de l'information, entre autres exemples (pour plus de détails, voir la rubrique méthodologique à la fin de ce rapport). Nous nous concentrons ici sur les cyberincidents présentant un caractère géopolitique ou stratégique, le plus souvent orchestrés par des États.

Les incidents discutés ici ont touché le Canada, qu'il s'agisse de ses pouvoirs publics, ses entreprises ou institutions de recherche, ou encore des individus, des organisations internationales ou non gouvernementales basées au Canada. Il s'agit dans certains cas d'incidents ayant visé spécifiquement le Canada, et dans d'autres cas, d'incidents ayant touché une diversité de pays (incluant le Canada). Les incidents recensés remontent jusqu'à 2010.

Marquée par différents séismes géopolitiques, tels l'invasion tous azimuts de l'Ukraine, l'intensification de la rivalité géoéconomique sino-américaine, ou l'essor d'un mouvement de protestation massif en Iran, l'année 2022 a vu plusieurs de ces bouleversements déborder dans l'espace numérique mondial, y compris canadien. Opérations de cyberespionnage, attaques par rançongiciel et campagnes d'influence en ligne ont ainsi occupé et préoccupé le débat public canadien à de multiples reprises en 2022. Et cela vraisemblablement plus que n'importe quelle année précédente : alors que la dernière édition de ce rapport concluait à une moyenne annuelle de 10 cyberincidents géopolitiques au Canada depuis 2017, ce ne sont pas moins de 14 incidents que la présente analyse a permis de comptabiliser en 2022. Au total, le répertoire des cyberincidents canadiens de la Chaire Raoul-Dandurand, dont les données du présent rapport sont issues, recense aujourd'hui 97 cyberincidents géopolitiques ayant touché le Canada depuis 2010.

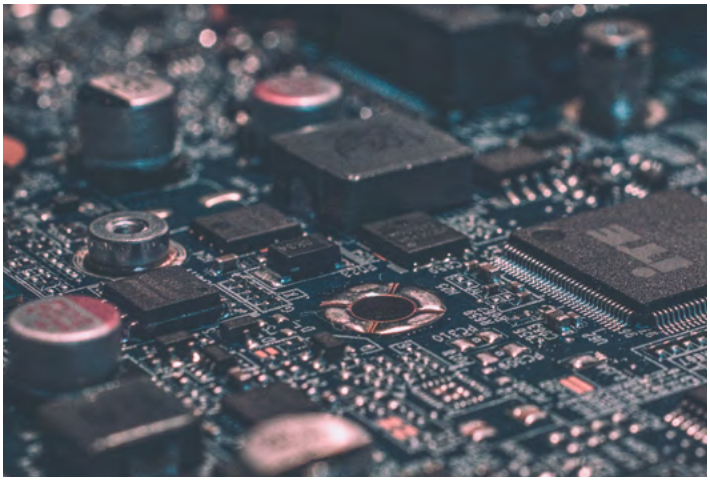
Quelles conclusions majeures pouvons-nous tirer des cyberincidents observés en 2022 ? Bien évidemment, les incidents géopolitiques qui ont lieu dans le cyberespace constituent un objet d'étude complexe : identifier les attaquants, leurs motifs ainsi que les conséquences de leurs actions est souvent un travail de longue haleine, dont les résultats ne sont pas toujours certains. Basé uniquement sur des sources ouvertes, le présent rapport ne livre donc que le fruit d'un travail de veille et de compilation, qui vise à présenter un aperçu des connaissances actuelles au Canada. La présente section met ainsi en évidence quelques données majeures concernant 2022, et illustre en quoi cette année s'est distinguée ou non des précédentes, par exemple sur le plan des types d'incidents, des secteurs visés ou encore des pays et des groupes de pirates informatiques les plus fréquemment impliqués dans les cyberincidents au Canada.

Quelles sont les cibles connues ?

Représentant la moitié des victimes répertoriées, le secteur privé a constitué la cible la plus fréquente des cyberincidents géopolitiques en 2022. Ce sont principalement des entreprises canadiennes qui œuvrent dans des domaines à valeur stratégique qui font les frais de ces attaques : le secteur de l'énergie notamment, mais aussi

l'industrie minière ou encore l'aérospatiale. En juillet 2022, par l'entremise du groupe de pirates informatiques Lazarus, la Corée du Nord s'est infiltrée dans les systèmes d'entreprises énergétiques canadiennes (dont les identités n'ont pas été dévoilées), à des fins de vol de propriété intellectuelle. La Chine, très active sur le marché des minerais stratégiques ces dernières années, s'est par ailleurs intéressée au secteur minier canadien, à travers une campagne d'influence ayant visé la firme Appia Rare Earths & Uranium Corp. en juin 2022. Il apparaît donc que la position du Canada dans le domaine des technologies de pointe attire l'attention de puissances étrangères.

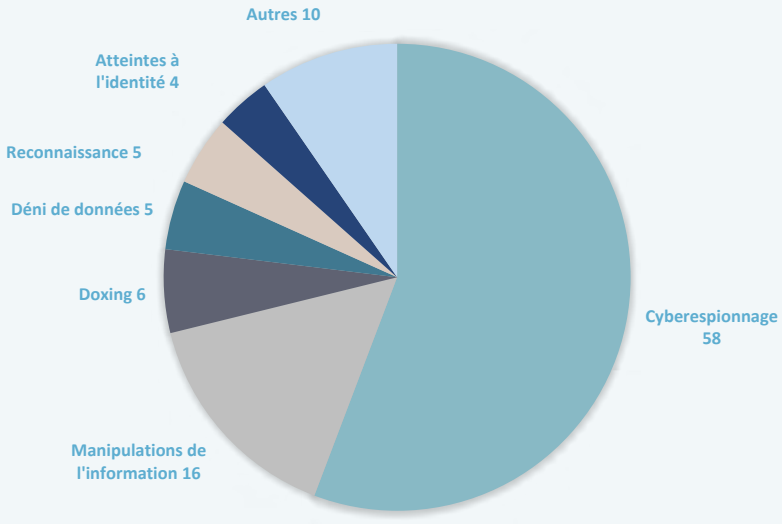
Du côté du secteur public, on remarque que les institutions canadiennes ont subi plus de cyberincidents que d'habitude en 2022. Au cas du Conseil national de recherches cité plus haut s'ajoutent une cyberattaque contre Affaires mondiales Canada, un cyberincident au Parlement canadien, ainsi qu'une campagne



de désinformation pilotée par la Russie ayant visé les Forces armées canadiennes dans le contexte du conflit en Ukraine. Quant aux allégations d'ingérence chinoise dans les élections fédérales de 2021, il importe de noter que l'enquête est encore en cours et que les informations rendues publiques jusqu'ici ne permettent pas de conclure que ces actes aient compris un volet cybernétique à proprement parler.

Quels sont les types de cyberincidents les plus fréquents ?

Types de cyberincidents répertoriés (depuis 2010)



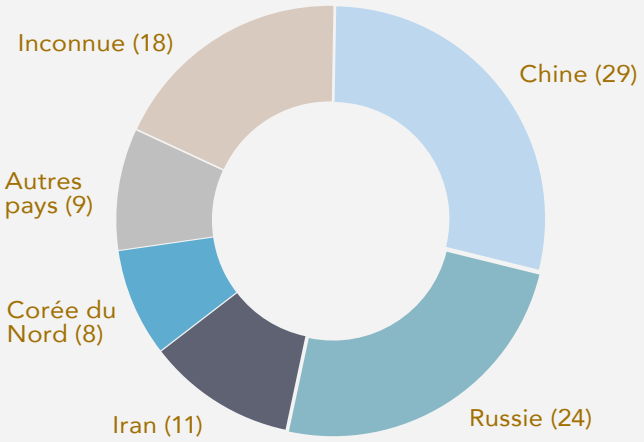
* Des cas peuvent cumuler simultanément plusieurs types d'incidents
Source : Répertoire des cyberincidents canadiens

Entre 2010 et 2022, le type de cyberincident géopolitique le plus fréquent au Canada est toujours le cyberespionnage qui représente environ 60 % des cas répertoriés. 2022 s'inscrit dans la même tendance puisque le cyberespionnage compose 40 % des cas[1]. Parmi les autres types d'incidents répertoriés l'année dernière, on trouve également deux cas de déni de données (ici, des rançongiciels), deux menaces de fuitage de données (doxing), ainsi que deux cas de manipulation de l'information (voir le graphique). Et, bien que la cause n'ait pas encore été publicisée, une intrusion dans les systèmes informatiques du Conseil national de recherche du Canada aurait eu lieu en mars 2022 ; cet organisme est une cible de choix pour des cyberespions désirant épier les activités de recherche scientifique canadiennes.

1 4 cas sur les 10 où il y a un motif clair.

D'où proviennent la plupart de ces actes ?

Origine géographique des cyberincidents (depuis 2010)



Nos données indiquent que, depuis 2010, quatre pays sont à l'origine de la grande majorité des cyberincidents géopolitiques recensés au Canada : la Chine (29 incidents sur 97), la Russie (24), l'Iran (11) et la Corée du Nord (8). Ces données concernent l'origine *géographique* des cyberincidents ayant touché le Canada et n'impliquent pas nécessairement une responsabilité des gouvernements des pays mentionnés (pour plus de détails, voir la rubrique méthodologique à la fin de ce rapport).

La répartition des incidents répertoriés en 2022 est cohérente avec ce portrait global, quoique l'ordre d'importance diffère quelque peu : c'est la Russie qui occupe la tête du classement avec 5 cyberincidents, tandis que la Chine et l'Iran seraient tous deux à l'origine de 3 incidents. Un cas proviendrait par ailleurs de Corée du Nord. Il faut noter que l'Iran semble témoigner d'un regain d'activité à l'encontre du Canada : alors que 8 cyberincidents canadiens lui ont été attribués durant toute la décennie 2011-2021, la République islamique en a cumulé trois en 2022 seulement.

Source : Répertoire des cyberincidents canadiens

Quels groupes de pirates informatiques ont visé le Canada en 2022 ?

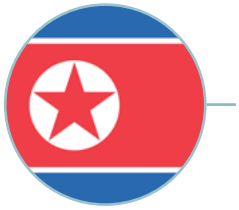
Parmi les cyberincidents géopolitiques répertoriés en 2022, plusieurs ont été attribués à des groupes de pirates informatiques déjà bien connus au Canada, tels Lazarus (groupe nord-coréen en activité depuis 2009) ou le groupe cybercriminel russophone Lockbit (vraisemblablement fondé en 2019). D'autres groupes semblent en revanche avoir visé le Canada pour la première fois l'année dernière. C'est notamment le cas de Dragonbridge, une entité chinoise menant des campagnes d'influence en ligne dans différents pays depuis 2019 et qui serait derrière la récente campagne de manipulation de l'information contre l'entreprise minière Appia Rare Earths. Le groupe de pirates étatiques russe Sandworm, actif depuis le milieu des années 2000 et déjà très connu sur la scène internationale, aurait également mené sa première opération au Canada en 2022.

Quelques groupes de pirates étatiques très actifs contre le Canada

Sur la base des efforts d'attribution déployés par les firmes de cybersécurité ou par les pouvoirs publics, on peut observer qu'un petit nombre de groupes de pirates étatiques est responsable d'une part importante des cyberincidents ayant touché le Canada. L'infographie ci-dessous présente ces différents acteurs, leur affiliation présumée, ainsi que les incidents canadiens leur ayant été formellement attribués.

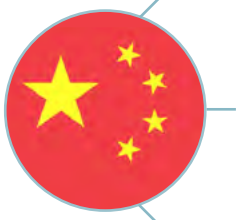
SILENT LIBRARIANS

Affiliation présumée : Mabna Institute (contractant du gouvernement iranien)
Opérations au Canada : Vague d'hameçonnage (2020), vague d'espionnage contre des universités (2019), espionnage contre des universités (2018)



LAZARUS GROUP

Affiliation présumée : Bureau général de reconnaissance (Armée populaire de Corée)
Opérations au Canada : Espionnage d'entreprises énergétiques (2022), vol de cryptomonnaies « AppleJeus » (2021), espionnage de la recherche COVID-19 (2020), campagne GhostSecret (2018), rançongiciel Wannacry (2017)



APT 1

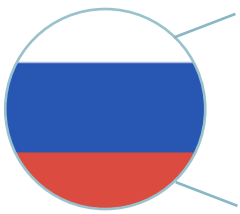
Affiliation présumée : Unité 61398 de l'Armée populaire de libération
Opérations au Canada : Operation OceanSalt (2018), campagne Surtr (2013), piratage de la Commission de l'immigration et du statut de réfugié (2011)

APT 10

Affiliation présumée : Ministère de la Sécurité d'État (bureau de Tianjin)
Opérations au Canada : Opération Cloud Hopper (2018), brèche d'Equifax (2017)

HAFNIUM

Affiliation présumée : Ministère de la Sécurité d'État (département de Hainan)
Opérations au Canada : Exploitation de la faille Microsoft Exchange (2021), campagne Leviathan (2019)



COZY BEAR

Affiliation présumée : Service des renseignements extérieurs (SVR)
Opérations au Canada : Campagne de phishing (2021), compromission de Solar Winds (2020), cyberespionnage de la recherche sur la COVID-19 (2020)

FANCY BEAR

Affiliation présumée : Unité 26165 du GRU (renseignement militaire)
Opérations au Canada : Cyberespionnage de la recherche sur la COVID-19 (2020), piratage de l'Agence mondiale antidopage (2019)

3 TENDANCES À SURVEILLER

Rétrospective : quand 2022 confirme les tendances

Dans la précédente édition de ce rapport, publiée au printemps 2022, nous présentions trois tendances majeures à surveiller de près pour l'année à venir : le cyberespionnage de plus en plus fréquent de membres de la société civile canadienne par des puissances étrangères, l'usage grandissant du cybermercenariat ainsi que l'essor des cyberattaques par rançongiciel au Canada et leurs potentielles retombées géopolitiques.

Un an plus tard, il s'avère que plusieurs cyberincidents répertoriés en 2022 sont malheureusement venus confirmer ces prévisions, et les dangers qu'elles sous-tendent. Alors que ces tendances risquent de perdurer en 2023 et au-delà, il apparaît important de démontrer concrètement comment elles continuent de se manifester et d'affecter la société canadienne.

Activistes, exilés et ONG : cibles privilégiées

Phénomène observé ponctuellement depuis 2013 au moins, les campagnes de cyberespionnage et de surveillance électronique orchestrées par des puissances étrangères contre des membres de la société civile canadienne deviennent de plus en plus fréquentes. Au moins deux cyberincidents de ce type ont pu être observés en 2022.

En novembre 2022, le Service canadien du renseignement de sécurité (SCRS) a annoncé avoir ouvert une enquête sur différentes menaces visant des activistes iraniens établis au Canada. Selon le SCRS, le régime iranien chercherait à surveiller et intimider les membres de la diaspora qui participent au mouvement de contestation secouant la République islamique depuis septembre 2022. Dans sa déclaration, le SCRS indiquait que « les tactiques et les outils utilisés dans ce but incluent le cyberespionnage ». Une enquête de la CBC a parallèlement révélé que certains activistes iraniens de la région de Toronto ont reçu des appels anonymes intimidants sur des numéros privés. Certaines de ces menaces faisaient référence à des publications partagées sur des comptes de réseaux sociaux privés, laissant envisager un recours à des moyens de surveillance électronique.

En décembre 2022, Amnesty International Canada a annoncé avoir fait l'objet d'un piratage informatique sophistiqué, repéré quelques semaines plus tôt. D'après la firme de cybersécurité Secureworks, mandatée par l'ONG, cette cyberattaque serait le fait d'un groupe de pirates affilié à l'État chinois. Ceux-ci

semblaient chercher à obtenir des informations confidentielles sur les contacts et les projets de l'organisation, et sont parvenus à accéder à certains fichiers de travail. La branche canadienne d'Amnesty figure parmi les organisations qui, depuis plusieurs années déjà, dénoncent publiquement le harcèlement d'activistes pour les droits de la personne, déployé par la Chine en sol canadien. La brèche en question aurait par ailleurs forcé l'ONG à mettre certains systèmes hors-ligne pendant près de 3 semaines, affectant significativement ses opérations ainsi que ses efforts de levée de fonds.

> **« Importante terre d'accueil garantissant la liberté d'expression, le Canada compte de grandes diasporas ou communautés d'exilés, dont les États d'origine (...) craignent la faculté de critique et de revendication. »**

Comme le démontrent des publications récentes, les cyberincidents visant les organismes de la société civile sont un phénomène qui ne se limite pas au Canada. Toutefois, différents facteurs font du Canada un pays considérablement à risque en la matière. Importante terre d'accueil garantissant la liberté d'expression, le Canada compte de grandes diasporas ou communautés d'exilés, dont les États d'origine (tels la Chine, l'Iran ou l'Arabie saoudite) craignent la faculté de critique et de revendication. Diplomatiquement très actif dans la promotion des droits de la personne à l'international, le Canada est également perçu comme un important symbole de l'ordre international libéral que plusieurs États souhaitent éroder. De tels facteurs sont importants à prendre en compte pour mieux saisir les enjeux derrière ces campagnes cybernétiques contre la société civile canadienne.

L'essor des cybermercenaires

L'essor de l'industrie du cybermercenariat, un marché gris transnational fournissant des services de piratage sur commande, était également considéré comme une tendance à surveiller en 2022. Alors que des actions malveillantes de cybermercenaires contre des entités canadiennes ont été observées depuis 2020 au moins, un autre cas du genre s'est produit plus récemment (voir également l'encadré ci-dessous).

En février 2023, un consortium de journalistes d'investigation a en effet révélé l'existence d'une mystérieuse firme israélienne, surnommée Team Jorge, commercialisant des services de piratage informatique et d'opérations d'influence. Cette mystérieuse officine entretiendrait notamment un réseau de 30000 faux profils sur différents médias sociaux, servant à la diffusion inauthentique coordonnée de narratifs fallacieux ou orientés. Les investigations entourant Team Jorge ont également révélé que l'entreprise avait mené des campagnes de désinformation en ligne pour influencer des disputes commerciales dans près de 20 pays, dont le Canada.

On ne sait toutefois pas pour l'instant quel(s) dossier(s) d'intérêt pour le Canada la firme aurait eu pour mission d'influencer, et encore moins pour le compte de quel commanditaire. De ce fait, et en vertu de notre méthodologie, le cas n'est pas encore inclus dans notre répertoire.

Rançongiciels : quand la criminalité se mêle à la géopolitique

Enfin, une troisième tendance importante évoquée en 2022 était la prolifération spectaculaire des cyberattaques par rançongiciel, et les potentielles implications géopolitiques de ces activités. Nous soulignions alors que, bien qu'elles soient le plus souvent de nature criminelle et motivées par l'appât du gain, les attaques par rançongiciel pouvaient également présenter des ramifications d'ordre stratégique et touchant aux rivalités entre États. Plusieurs cyberincidents répertoriés en 2022 sont venus mettre en évidence ce phénomène (voir également l'encadré ci-dessous).

En mai 2022, deux firmes canadiennes du secteur de la défense (basées à Montréal) ont été victimes d'attaques par rançongiciel : la firme Top Aces, qui commercialise des services d'entraînements pour pilotes de chasse, entre autres pour l'Aviation royale canadienne, et CMC Électronique, entreprise du domaine aérospatiale, impliquée dans un programme de modernisation d'hélicoptères des Forces armées canadiennes. Dans les deux cas, des observateurs ont fait remarquer que les données compromises pouvaient contenir de l'information à forte valeur stratégique. Il était donc envisageable que les cybercriminels, en marge de leur opération d'extorsion, cherchent à monnayer les données à des puissances étrangères. De fait, le ministère canadien de la Défense a par la suite annoncé entreprendre une analyse poussée des possibles impacts de l'attaque contre CMC Électronique.

> **« Bien qu'elles soient le plus souvent de nature criminelle et motivées par l'appât du gain, les attaques par rançongiciel [peuvent] également présenter des ramifications d'ordre stratégique et touchant aux rivalités entre États. »**

Ces deux cas illustrent les potentielles synergies pouvant exister entre cybercriminels et acteurs étatiques, les premiers étant fréquemment soupçonnés de rendre des services occasionnels aux seconds, dans le but d'« acheter » leur impunité. Alors que bon nombre de gangs opérant des attaques par rançongiciel sont basés en Russie, de nombreuses recherches suggèrent qu'un système de connivence — à tout le moins informel — existe entre le renseignement russe et les groupes cybercriminels. Bien que Top Aces et CMC Électronique aient tous deux été visés par des groupes criminels russophones, il est toutefois impossible de conclure avec certitude que les données compromises aient été offertes à des puissances adverses.

Un cas canadien : une campagne d'extorsion mandatée par l'Iran (septembre 2022)

En septembre 2022, plusieurs agences de cybersécurité américaines, canadiennes, australiennes et britanniques publient un communiqué conjoint : elles disent avoir repéré une importante campagne de cyberintrusions ayant visé des organisations des quatre pays en question. On y apprend entre autres que les pirates auraient exploité les vulnérabilités Fortinet, Microsoft Exchange et Log4j, en vue de mener une campagne de cyberextorsion, notamment par l'entremise de rançongiciels.

De prime abord, cette campagne ressemble en tout point à une opération criminelle, comme l'année 2022 en a connu par dizaines. Toutefois, le Canada et ses trois alliés ont entrepris de communiquer conjointement pour une bonne raison : au terme d'analyses poussées, les agences impliquées concluent que la campagne a été mandatée par le gouvernement iranien. Plus précisément, divers indices pointeraient du doigt le Corps des Gardiens de la révolution islamique (IRGC), organisation paramilitaire au service du régime.

L'IRGC aurait néanmoins pris soin de couvrir ses traces : l'exécution de cette campagne de cyberextorsion aurait été sous-traitée à deux entreprises technologiques iraniennes, Najee Technology Hooshmand Fater LLC et Afkar System Yazd Company. Le but de l'opération reste néanmoins mystérieux. Selon le communiqué, les pirates auraient tenté à la fois de crypter les données de leurs cibles (en vue d'exiger une rançon) et de les exfiltrer (probablement à des fins de collecte de renseignements) lorsque celles-ci semblaient présenter une valeur stratégique. Le nombre et la nature des entités visées, au Canada et ailleurs, ne sont cependant pas précisés.

Quels étaient les termes de l'arrangement entre l'IRGC et ces deux mystérieuses entreprises ? L'histoire ne le dit pas non plus. On peut imaginer que les Gardiens de la révolution cherchaient à espionner des organisations occidentales détenant des données sensibles, et auraient recouru à un acteur privé pour ne pas alerter les services de renseignement adverses ou bénéficier d'un déni plausible s'ils avaient été démasqués. Les deux entreprises, pour leur part, ont probablement récolté quelques bonnes grâces du régime iranien, tout en remplissant impunément leurs coffres grâce aux sommes extorquées. Leur degré de succès, sur le premier comme sur le second aspect, demeure cependant inconnu.

Quoiqu'il en soit, cette campagne de cyberextorsion illustre bien deux des tendances discutées plus haut dans ce rapport. D'une part, elle démontre comment certains États (et particulièrement l'Iran) tentent désormais d'instrumentaliser l'essor des attaques par rançongiciel pour camoufler leurs activités de collecte de renseignements à l'étranger. D'autre part, elle dévoile comment des entités cybermercenaires peuvent contribuer à de tels subterfuges, compliquant d'autant l'identification des véritables commanditaires de cyberattaques et leurs motifs. Ce sont là deux tendances préoccupantes, auxquelles le Canada devra vraisemblablement prêter une attention particulière à l'avenir.

Ukraine et cyberconflictualité : le Canada épargné ?

C'était l'une des grandes craintes énoncées dans les premiers mois de l'invasion tous azimuts de l'Ukraine : que les pays occidentaux qui soutiennent l'Ukraine diplomatiquement ou militairement, tel le Canada, fassent l'objet de cyberattaques « punitives » orchestrées ou encouragées par la Russie. L'usage de rançongiciels, les attaques par déni de service ou les opérations de vol et fuitage de données contre des organisations canadiennes, notamment, étaient jugés comme très probables.

Après plus d'une année de conflit, ces craintes se sont-elles matérialisées au Canada ? Au moins en partie. En avril 2023, par exemple, plusieurs attaques par déni de service menées par des groupes d'hacktivistes pro-Russie ont visé une vingtaine de sites internet appartenant à diverses organisations publiques ou privées canadiennes. Parmi ceux-ci figuraient notamment les sites du premier ministre, du Sénat ou encore de l'Association des industries canadiennes de défense et de sécurité. Là où de telles cyberattaques sont spectaculaires, mais demeurent relativement sans conséquences, les cas ci-après démontrent que d'autres cyberincidents liés au conflit en Ukraine, plus discrets et plus élaborés, ont également touché le Canada au fil de l'année 2022.

Une cible avant tout indirecte

En mars 2022 par exemple, la firme de cybersécurité Trend Micro révélait que le groupe de pirates informatiques Sandworm (affilié au renseignement militaire russe - GRU) avait compromis, au Canada et dans plusieurs autres pays, plus de 150 routeurs et serveurs par l'entremise d'un logiciel malveillant. Selon Trend Micro, les pirates ne ciblaient pas particulièrement les entités canadiennes opérant ces appareils, celles-ci ne présentant qu'un faible intérêt stratégique. L'opération visait plus probablement à établir discrètement un contrôle sur ces infrastructures, en vue de les utiliser comme vecteur d'une future attaque de plus grande ampleur — potentiellement contre des systèmes ukrainiens. De fait, Sandworm est connu comme l'un des groupes russes les plus actifs en Ukraine : c'est à ses membres que sont attribués les cybersabotages de 2015 et 2016 contre le réseau électrique ukrainien, ainsi que la cyberattaque du rançongiciel NotPetya en 2017. Le Canada aurait donc fait figure de cible intermédiaire.

C'est aussi sur le terrain informationnel que le conflit en Ukraine vient discrètement affecter le Canada. En avril 2022, le Centre de la sécurité des télécommunications (CST) a notamment annoncé avoir observé plusieurs opérations de désinformation menées par la Russie, certaines concernant le Canada. Dans un effort de diffusion coordonné, différents agents d'influence russes disséminaient des contenus fallacieux affirmant par exemple que des soldats canadiens étaient déployés dans le Donbass, et que certains s'étaient rendus coupables de crimes de guerre[1]. Ces fausses nouvelles étaient illustrées par des images trafiquées censées montrer des soldats des Forces armées canadiennes déployés sur la ligne de front. Elles étaient entre autres diffusées par des sites web frauduleux cherchant à imiter visuellement des médias occidentaux établis. Ici aussi, le Canada constituait plutôt une cible indirecte : ces contenus ne visaient pas une audience canadienne, mais avaient manifestement vocation à porter atteinte à l'image du Canada à l'étranger.

Organes gouvernementaux potentiellement visés

En marge de ces deux cyberincidents relativement bien documentés, deux autres cas plus ambigus ont également été répertoriés et laissent à penser qu'ils pourraient être liés au conflit en Ukraine : le piratage d'Affaires mondiales Canada fin janvier 2022 (voir ci-contre) et un cyberincident ayant touché le Parlement canadien en octobre de la même année. Si ni l'un ni l'autre n'a fait l'objet d'une attribution officielle jusqu'ici, la Russie fait partie des suspects potentiels.

« Le Canada constituait plutôt une cible indirecte : ces contenus ne visaient pas une audience canadienne, mais avaient manifestement vocation à porter atteinte à l'image du Canada à l'étranger. »

De fait, en juin 2022, un rapport publié par Microsoft révélait que 128 organisations dans 42 pays avaient fait l'objet d'opérations de cyberespionnage russes en marge du conflit. Alors que le Canada figurait dans les cibles identifiées par Microsoft, il n'est pour l'heure pas clair quelles étaient la ou les entités canadiennes visées, et si Affaires mondiales était l'une d'elles. Survenu plus tard, le cyberincident d'octobre 2022 ayant touché le Parlement reste entouré de mystère. On peut toutefois noter qu'à la période où l'incident s'est produit, la Chambre des communes se penchait sur différents rapports relatifs aux inventaires de véhicules des Forces armées canadiennes susceptibles d'être livrés à l'Ukraine.

Les facteurs de risque à surveiller

Reste qu'en termes comparatifs, le Canada est loin d'avoir été une cible prioritaire des activités cybernétiques russes jusqu'ici. Selon un nouveau rapport de Microsoft publié en mars 2023, ce sont les États-Unis, la Pologne, le Royaume-Uni et les États baltes qui ont été les plus visés par les opérations de cyberespionnage imputées à la Russie depuis février 2022. Dans un autre rapport, publié début 2023 par

[1] Des fausses rumeurs similaires avaient déjà été disséminées par des acteurs russes à plusieurs reprises par le passé, notamment en 2017 et en 2018.

le CyberPeace Institute, le Canada ne figurait qu'au 14e rang des pays les plus touchés par les diverses cyberattaques russes entourant le conflit russo-ukrainien.

Si le Canada ne peut se prévaloir d'avoir été totalement épargné par la cyberconflictualité découlant de la guerre en Ukraine, il est néanmoins loin d'être le pays occidental le plus affecté. Pour autant, alors que le conflit ne semble pas près de s'arrêter, au moins trois facteurs pourraient contribuer à modifier cet état de fait à court ou moyen terme :

- D'abord, des livraisons de matériel militaire importantes ou fortement médiatisées pourraient susciter l'attention des acteurs cyber pro-Russie et motiver des actions cybernétiques ponctuelles. C'est ce que démontrent par exemple les attaques par déni de service qui ont visé l'Allemagne en janvier 2023, à la suite de l'annonce de livraisons de chars d'assaut Leopard 2. Il faut d'ailleurs noter que les attaques par déni de service ayant visé des sites canadiens en avril 2023 faisaient suite à l'annonce d'une nouvelle livraison de munitions canadiennes à l'Ukraine. Bien qu'assez probables, de tels incidents sont le plus souvent peu élaborés et engendrent des dégâts très limités.

- Ensuite, alors que le conflit présente le risque de s'enliser, l'aide militaire étrangère est considérée par un nombre grandissant d'experts comme le principal talon d'Achille de l'Ukraine. Ce faisant, la Russie déploie des efforts informationnels croissants pour tenter d'éroder le soutien des opinions publiques occidentales à l'Ukraine. Or, la position du Canada dans le top-5 des plus gros fournisseurs d'aide militaire le désigne comme une cible de choix pour les campagnes d'influence russes. Tandis que des opérations russes ont récemment cherché à exacerber les craintes entourant l'accueil de réfugiés ukrainiens dans différents pays d'Europe, il est envisageable que de telles campagnes visent prochainement à influencer le public canadien.

- Enfin, les sanctions technologiques frappant la Russie commencent à peser sévèrement sur certaines de ses industries. À mesure que ces contraintes s'accentuent, Moscou pourrait redoubler ses efforts de cyberespionnage industriel, afin d'acquérir les connaissances susceptibles de lui conférer une plus grande autosuffisance technologique. Le secteur aéronautique, par exemple, est un de ceux où la Russie subit actuellement de grandes difficultés, et dans lequel le savoir-faire avancé détenu par le Canada pourrait susciter les convoitises des cyberespions russes.

Un cas canadien : le cyberincident à Affaires mondiales Canada (janvier 2022)

Le 24 janvier 2022, les médias nationaux canadiens s'agitent : on vient d'apprendre qu'Affaires mondiales Canada a été victime d'un cyberincident, que des sources gouvernementales anonymes décrivent comme « une cyberattaque ». On apprend que l'incident aurait été repéré le 19 janvier, et que certains services en ligne du ministère sont momentanément indisponibles, du fait des mesures de remédiation entreprises. Certains médias rapportent que les ambassades canadiennes à l'étranger rencontrent des problèmes avec leurs communications électroniques. Des sources anonymes confient dans la foulée que de forts soupçons sur l'origine de l'incident pèsent sur la Russie.

De fait, le contexte de l'attaque est sensible sur le plan géopolitique : alors que le gouvernement russe a massé plus de 100 000 soldats aux abords des frontières de l'Ukraine au fil de l'année 2021, les diplomaties occidentales s'affairent depuis plusieurs semaines à tenter de raisonner (et plus encore dissuader) Moscou. Le Canada figure parmi les États s'étant fortement impliqués dans ces efforts. La ministre des Affaires étrangères canadiennes Mélanie Joly est d'ailleurs en visite à Kiev lorsque survient le cyberincident. On ne sait évidemment pas encore que la Russie lancera bel et bien, exactement un mois plus tard, une offensive de grande ampleur contre le territoire ukrainien.

Le 15 février, de nouveaux éléments surgissent dans la presse. On apprend notamment que certains services en ligne du ministère ne sont toujours pas rétablis, et que le Centre de la sécurité des télécommunications (l'agence de renseignement fédérale en charge des questions de cybersécurité) assiste Affaires mondiales dans ses efforts de remédiation. Aucun autre commentaire n'est émis quant à la source de la cyberattaque. Entre-temps, le 8 février, la presse internationale a révélé que le ministère des Affaires étrangères britannique a lui aussi subi un cyberincident similaire un peu plus tôt dans l'année.

En juin 2022, un rapport de Microsoft révèle justement que des pirates informatiques affiliés au renseignement russe ont mené des opérations de cyberespionnage dans 42 pays, dont le Canada (et presque tous les autres membres de l'OTAN). Près de la moitié des entités visées étaient des agences gouvernementales, dans le but, selon Microsoft, « d'obtenir de l'information interne des gouvernements qui jouent un rôle essentiel dans la réponse occidentale à la guerre ». En février 2023, un autre rapport, publié par la firme de cybersécurité française Sekoia.IO, révèle quant à lui que le groupe de pirates APT29 (ou Fancy Bear) affilié au renseignement extérieur russe (SVR) aurait manifestement eu pour mission spécifique d'espionner les diplomaties occidentales au fil de 2022. Fancy Bear aurait notamment mené « des opérations clandestines de longue durée contre les réseaux d'ambassades ».

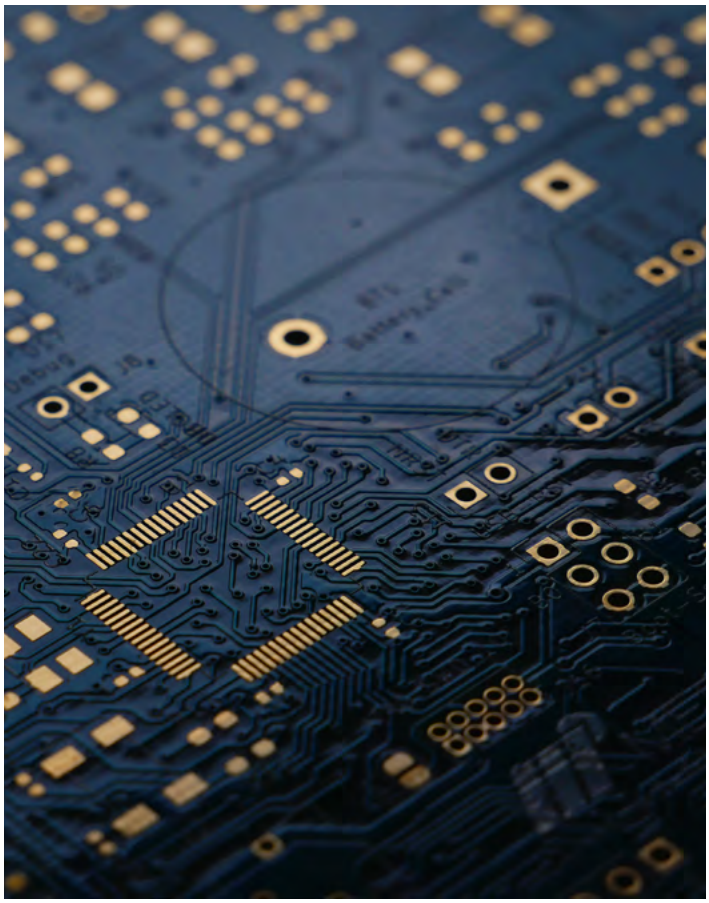
La cyberattaque contre Affaires mondiales pourrait-elle faire partie de cette vaste campagne de cyberespionnage russe ? L'hypothèse est très probable, mais n'est pas encore confirmée. Sans détails supplémentaires (ni attribution officielle) du gouvernement canadien à ce jour, on ne sait pas si l'attaque a été fructueuse et, le cas échéant, quelles informations ont été compromises. Par ailleurs, alors que dans son rapport de juin 2022 Microsoft n'a pas révélé le nombre et la nature des entités canadiennes ciblées, il faut envisager que d'autres organisations stratégiques canadiennes aient été visées par la Russie dans le cadre du conflit ukrainien.

Minéraux critiques et semi-conducteurs : nouvel épicentre de la rivalité avec la Chine ?

La pandémie de COVID-19 a affecté la pensée stratégique canadienne de plusieurs manières. Elle a notamment suscité de vives inquiétudes à Ottawa en perturbant les chaînes d'approvisionnement mondiales dans deux secteurs essentiels pour l'avenir du Canada : les minéraux critiques/terres rares et les semi-conducteurs. Le premier ministre Justin Trudeau et le président Joe Biden ont d'ailleurs fait de cette question l'un des points centraux de leur rencontre à Ottawa en mars 2023, promettant de rapatrier une partie de la production mondiale vers l'Amérique du Nord.

La valeur stratégique des minéraux critiques et des semi-conducteurs pourrait en effet dépasser celle du pétrole dans les décennies à venir. Essentiels à la fabrication d'équipements militaires comme les systèmes de communication ou encore de guidage de missiles, ils sont, en plus, l'une des clés de la transition vers les énergies renouvelables promise par Ottawa, Washington et leurs alliés. Les approvisionnements en lithium, cobalt, cuivre, dysprosium, néodyme et lanthane sont notamment cruciaux pour le développement des batteries et moteurs des voitures électriques, des panneaux solaires ou des aimants nécessaires à la fabrication des éoliennes. Il en va de même pour les semi-conducteurs : on retrouve ces puces et micro-puces dans de nombreux objets qui permettent aux Canadiens de réduire leur empreinte écologique, tels que les véhicules électriques, les ordinateurs et autres appareils électroménagers économes en énergie.

Le Canada, les États-Unis et leurs alliés dépendent toutefois fortement de la Chine et de l'Asie de l'Est dans ces secteurs. La Chine est le premier producteur mondial de terres rares : elle détient 36 % des réserves



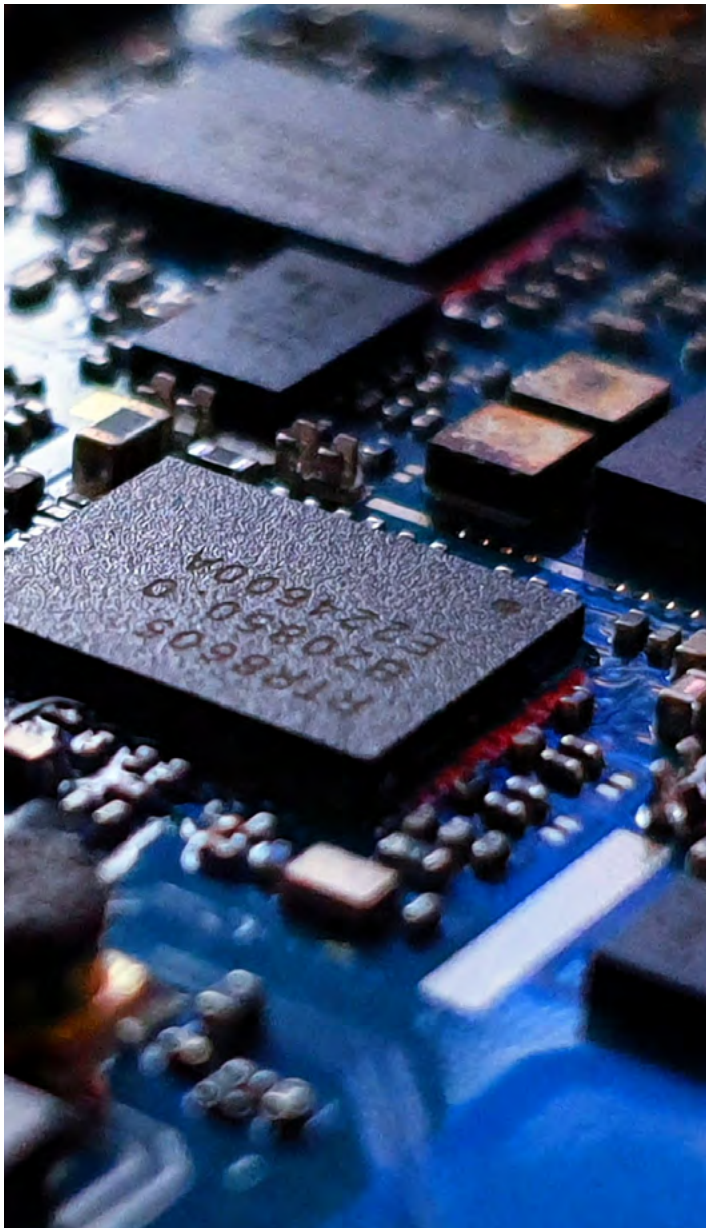
connues et contrôle 70 % de la capacité d'extraction mondiale et 90 % de la capacité de traitement. Dans son ouvrage Chip War : The Fight for the World's Most Critical Technology, le professeur Chris Miller rappelle en outre que la Chine aspire à devenir un chef de file dans la production des semi-conducteurs (elle compte actuellement pour 15 % de la production mondiale). Plus important encore, elle investit massivement dans la recherche et le développement afin d'augmenter sa production de puces et de micro-puces les plus sophistiquées, dont 90 % des approvisionnements mondiaux proviennent actuellement de Taiwan, île voisine que Pékin considère comme sienne et dont elle ne reconnaît pas la souveraineté.

Les menaces constantes d'une intervention militaire chinoise contre Taiwan incitent encore davantage le Canada et les États-Unis à tenter de réduire leur dépendance à l'égard des semi-conducteurs de cette région. Lors de leur rencontre à Ottawa en mars 2023, Trudeau et Biden ont ainsi réitéré l'importance de préserver la stabilité dans le détroit de Taiwan, mais aussi d'augmenter les investissements gouvernementaux pour accélérer la production et l'assemblage de semi-conducteurs essentiels, en Amérique du Nord.

« Les menaces constantes d'une intervention militaire chinoise contre Taiwan incitent encore davantage le Canada et les États-Unis à tenter de réduire leur dépendance à l'égard des semi-conducteurs de cette région. »

Ottawa et Washington recourent en plus aux sanctions et aux barrières économiques pour freiner les avancées chinoises dans ces secteurs. En novembre 2022, Ottawa ordonnait par exemple à trois firmes chinoises « de se départir de leurs investissements dans des entreprises canadiennes actives dans le secteur des minéraux critiques, et ce, pour des raisons de "sécurité nationale" ». Un mois plus tôt, Washington annonçait une série de mesures pour isoler la production chinoise de semi-conducteurs du reste du monde, dont une interdiction aux compagnies américaines de vendre des puces et micropuces hautement sophistiquées à la Chine, pour éviter les copies et le vol de propriété intellectuelle.

Ces développements menacent déjà de faire des minéraux critiques/terres rares et des semi-conducteurs l'épicentre des rivalités entre Ottawa et Pékin, et d'inciter la Chine à s'en prendre au Canada pour nuire à sa réputation internationale, paralyser ses entreprises ou ralentir le rapatriement de chaînes de productions essentielles en sol nord-américain. Notre répertoire des cyberincidents géopolitiques visant le Canada montre déjà que la Chine recourt à divers moyens, dont le cyberespionnage, pour remporter la compétition géoéconomique dans des secteurs névralgiques pour le Canada, Washington et ses alliés. Or, les cas étudiés en 2022 illustrent que Pékin pourrait être de plus en plus tentée à recourir aux campagnes de désinformation pour miner la crédibilité des entreprises canadiennes impliquées dans la rivalité sino-canadienne dans les secteurs des minéraux critiques/terres rares et des semi-conducteurs. L'opération d'influence chinoise de 2022 visant la compagnie torontoise Appia Rare Earths & Uranium Corp. en témoigne.



Un cas canadien : Appia Rare Earths & Uranium Corp. dans le collimateur de Pékin (juin 2022)

En juin 2022, la compagnie canadienne Appia Rare Earths & Uranium Corp. annonçait la découverte d'un nouveau gisement de terres rares dans le bassin d'Athabasca au nord de la Saskatchewan. Selon la firme de cybersécurité américaine Mandiant, elle est ensuite devenue la cible d'une entité chinoise nommée Dragonbridge, qui a mené une campagne de manipulation de l'information consistant à créer des milliers de faux comptes sur les médias sociaux, des sites Internet ou encore des forums de discussion en ligne, pour promouvoir des récits alignés sur les intérêts du gouvernement chinois et discréditant la réputation d'Appia Rare Earths & Uranium Corp., que Pékin voit comme un compétiteur stratégique. Parmi les messages publiés sur Facebook et Twitter, plusieurs soulignent les effets potentiellement néfastes des projets d'Appia Rare Earths & Uranium Corp. sur l'environnement et la santé des travailleurs. Dragonbridge a visé d'autres compagnies œuvrant dans l'extraction de terres rares en sol nord-américain, dont Lynas Rare Earths et USA Rare Earth, qui ont toutes deux annoncé de nouveaux projets aux États-Unis en 2022. Encore là, les publications sur les médias sociaux visaient à ternir la réputation des compagnies en question, en affirmant par exemple que la pollution causée par l'exploitation des terres rares menace la santé des communautés locales.

À l'heure où Joe Biden et Justin Trudeau promettent de soutenir de telles entreprises pour accroître la production de minéraux critiques/terres rares et de semi-conducteurs au Canada et aux États-Unis, des campagnes comme celle menée par Dragonbridge deviendront peut-être la tendance dans les années à venir. Lors de leur rencontre à Ottawa en mars 2023, Biden et Trudeau rappelaient que les États-Unis s'appuient sur le *Defense Production Act* pour prévoir des investissements de 250 millions de dollars US pour des projets canadiens ou américains d'extraction et de traitement de minéraux critiques. De son côté, le Canada promet 1,5 milliard de dollars d'investissement dans ce même secteur. Ottawa et Washington souhaitent également créer un corridor nord-américain de production de semi-conducteurs, en commençant par un investissement du Canada et d'IBM visant à étendre les capacités de testage et d'emballage de l'usine d'IBM à Bromont, au Québec. Le gouvernement du Québec a par ailleurs sa propre stratégie pour contribuer au rapatriement des chaînes d'approvisionnement essentielles en Amérique du Nord, comme en témoigne le Plan québécois pour la valorisation des minéraux critiques et stratégiques 2020-2025.

La Chine a certainement l'œil sur ces développements, qui entrent directement en conflit avec son désir d'être le leader incontesté dans ces domaines stratégiques. Comme le démontre le présent rapport, la Chine est déjà le pays dont provient le plus grand nombre d'incidents géopolitiques touchant le Canada. En alignant ses politiques industrielles et manufacturières, ainsi que sa stratégie pour l'Indo-pacifique, sur celles des États-Unis, le Canada resserre les liens avec son allié traditionnel, mais se place du même coup sur le chemin d'une puissance chinoise qui ne cesse de croître et qui n'hésite pas à recourir à diverses offensives numériques et géoéconomiques (espionnage économique, vol de propriété intellectuelle, cyberattaques, etc.) pour déstabiliser et ralentir ses rivaux.

Conclusion

La menace grandissante des cyberopérations malveillantes propulsées par l'intelligence artificielle

Fin février 2023, un hypertrucage diffusé sur YouTube et mettant en scène Justin Trudeau, apparemment en entrevue avec l'animateur de balado américain Joe Rogan, a été visionné plusieurs centaines de milliers de fois en moins d'une semaine. Bien que la vidéo ait été conçue à des fins humoristiques par une entreprise de divertissement, la ressemblance des voix et la qualité de l'hypertrucage semblent avoir berné un certain nombre d'internautes. Cette anecdote laisse présager du rôle grandissant que les technologies d'intelligence artificielle (IA) pourraient jouer dans les stratégies de désinformation.

Selon le think tank Eurasia Group, l'arsenal de possibilités offert par l'IA et son accessibilité croissante ont le potentiel de transformer celle-ci en une véritable « arme de déstabilisation massive » au service d'agents d'influence étrangers. Des outils d'IA générative permettent maintenant de créer de fausses images et de faux enregistrements audio paraissant vraisemblables, même aux yeux des experts. De plus, les armées d'automates (*bots*) déjà déployées à faible coût sur les réseaux sociaux et aux capacités désormais décuplées par l'IA peuvent accroître la polarisation des masses, ou encore, simuler un soutien encore plus vraisemblable à un candidat ou une cause politique. Des textes générés par l'IA peuvent aussi être utilisés pour créer des contenus médiatiques convaincants semblant provenir de sources d'information légitimes.

En plus de servir de multiplicateur de force pour les États bien versés dans les opérations d'influence, la démocratisation de l'IA pourrait inciter le déploiement de telles campagnes chez de nouveaux acteurs qui n'en avaient auparavant ni les ressources ni les capacités nécessaires. Le Canada, qui semble avoir été passablement épargné par les plus récents efforts de désinformation russe accompagnant l'invasion en Ukraine, pourrait à moyen terme être davantage ciblé par Moscou, ou faire les frais de l'arrivée de nouveaux acteurs étatiques désirant entrer dans l'arène des opérations d'influence.

L'IA pourrait également jouer un rôle grandissant dans la répression transnationale visant des activistes basés au Canada. L'Iran et la Chine, deux pays utilisant déjà plusieurs de ses outils à l'intérieur de leurs frontières à des fins de surveillance, de censure et de désinformation,

pourraient exporter des stratégies d'intimidation propulsées par l'IA pour viser plus extensivement et plus efficacement ses ressortissants exilés au Canada. Fin 2022, les agences de sécurité canadiennes mettaient par exemple en garde les membres de la diaspora iranienne contre des tentatives de surveillance et de harcèlement d'activistes, opérées par le régime iranien. Il est ainsi concevable que des États autoritaires emploient prochainement des outils de reconnaissance faciale dopés à l'IA pour identifier des personnes participant à des manifestations au Canada, entre autres à partir de vidéos publiées sur les réseaux sociaux.

Au-delà de leur rôle dans la désinformation et la répression numérique, les outils d'IA sont également utilisés pour faciliter les cyberattaques. Par exemple, des cybercriminels peuvent désormais créer automatiquement du code destiné à mener des attaques par rançongiciel, tandis que les voix générées par IA peuvent être utilisées pour débloquer l'accès à des portails sécurisés via reconnaissance vocale. Une récente étude publiée dans le journal Applied Artificial Intelligence montre par ailleurs que les individus sont particulièrement vulnérables aux tentatives d'hameçonnage élaborées grâce à l'IA.

À la mi-mars 2023, la firme de recherche OpenAI a mis en ligne la dernière mouture de son fameux modèle de langue de grande taille (Large Language Model), ChatGPT-4. Malgré les précautions prises par ses développeurs, quelques jours ont suffi pour se rendre compte de ses failles éthiques. Les professionnels de la cybersécurité devront donc s'adapter rapidement et faire preuve d'agilité pour protéger les systèmes informatiques et leurs points d'entrée contre des attaques de plus en plus sophistiquées. Sinon, l'année 2023 pourrait consacrer l'avènement de premiers cyberincidents géopolitiques canadiens rendus possibles par l'intelligence artificielle.

Comment ce rapport a-t-il été établi ?

Les données et cas présentés dans le présent rapport sont directement extraits du répertoire des cyberincidents canadiens conçu par l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand. Il s'agit d'une base de données en ligne, inaugurée en 2021 et librement accessible au public. Pour la consulter, rendez-vous sur :

www.dandurand.uqam.ca/cyberincidents

Le répertoire des cyberincidents canadiens a pour objectif de recenser et classer les cyberincidents à caractère géopolitique ayant touché le Canada : sa population, ses pouvoirs publics, ses entreprises, sa société civile, ses infrastructures ou des entités y étant basées. Il se veut une source de référence, régulièrement mise à jour, mais ne prétend pas à l'exhaustivité. Il remonte pour l'heure jusqu'à 2011. Un incident manquant ? Vous pouvez nous le signaler à l'adresse chaire.strat@uqam.ca.

CE QUE CE RAPPORT TRAITE ET NE TRAITE PAS

Fidèle aux missions de la Chaire Raoul-Dandurand, le présent rapport se concentre sur les cyberincidents présentant des implications géopolitiques ou stratégiques pour le Canada. En d'autres termes, les incidents traités ici relèvent essentiellement de rapports de puissance internationaux : ils proviennent le plus souvent de l'extérieur du Canada, sont pour la plupart orchestrés par des gouvernements étrangers, et ce, à des fins militaires, politiques, économiques, et autres.

Ce rapport ne traite donc pas des cyberincidents d'origine strictement domestique et/ou relevant strictement de cybercriminalité (même s'ils proviennent de l'étranger). Du fait que ces caractéristiques peuvent occasionnellement être difficiles à établir, nous privilégions une approche inclusive dans laquelle le répertoire peut comprendre des cas ambigus. Nous encourageons les lectrices et lecteurs à aller consulter le répertoire en ligne pour plus d'informations sur les nuances ou réserves d'usage concernant les cas ambigus.

Typologie des incidents et leurs définitions

Le répertoire des cyberincidents canadiens, sur lequel ce rapport s'appuie, distingue huit catégories de cyberincidents à caractère géopolitique. Cette typologie s'articule davantage autour de la dimension stratégique des incidents (leurs buts) que sur leur dimension technique (leur modus operandi). Elle s'inspire librement de celle du Cyber Operations Tracker entretenu par le think tank américain Council on Foreign Relations. Ci-dessous figurent les définitions propres à chaque type d'incident :

CYBERESPIONNAGE : Fait d'obtenir par des moyens numériques de l'information sans l'accord préalable du détenteur de cette information. Cette catégorie comprend par exemple le vol de secrets d'État, le vol de propriété intellectuelle, la surveillance clandestine d'individus, etc.

RECONNAISSANCE : Fait de s'introduire frauduleusement dans un système informatique dans le but de le cartographier, évaluer ses défenses ou vulnérabilités, par exemple en prévision d'actions futures.

MANIPULATION DE L'INFORMATION : la diffusion intentionnelle, massive et coordonnée de nouvelles fausses ou biaisées dans le cyberespace, à des fins politiques hostiles (voir Jeangène Vilmer et al., 2018)

ATTEINTE À L'IDENTITÉ : Fait d'usurper, prendre le contrôle, ou modifier l'apparence de manière non autorisée d'un site web (defacement), d'un compte ou d'une page à des fins politiques hostiles.

DOXING : « Publication intentionnelle sur internet d'informations personnelles sur un individu par un tiers, souvent dans le but d'humilier, menacer, intimider ou punir l'individu en question » (Douglas, 2016). Nous élargissons cette définition aux organisations (« organizational doxing »). Cette catégorie inclut par exemple les opérations « hack and leak ».

DÉNI DE DONNÉES : Fait de détruire définitivement, ou de priver temporairement, un utilisateur ou une organisation de ses données. Cette catégorie inclut l'utilisation de rançongiciels.

DÉNI DE SERVICE : « Quelconque attaque visant à compromettre la disponibilité de réseaux ou de systèmes […] résultant dans une dégradation de la performance ou une interruption de service » (Verizon, 2019). Ceci comprend notamment les cyberattaques de type DDoS (distributed denial of service).

CYBERSABOTAGE : Fait d'utiliser un virus ou logiciel malicieux pour causer un dommage physique à un ordinateur, une machine, tout ou partie d'une infrastructure ; ou pour interrompre de manière prolongée le fonctionnement d'un système informatisé.

Dates et origine des cyberincidents

Les informations présentées dans ce rapport sont basées sur des sources ouvertes, et les détails de nombreux cyberincidents, ou la manière dont certaines conclusions sont établies par les organes pertinents, demeurent souvent inconnus ou confidentiels.

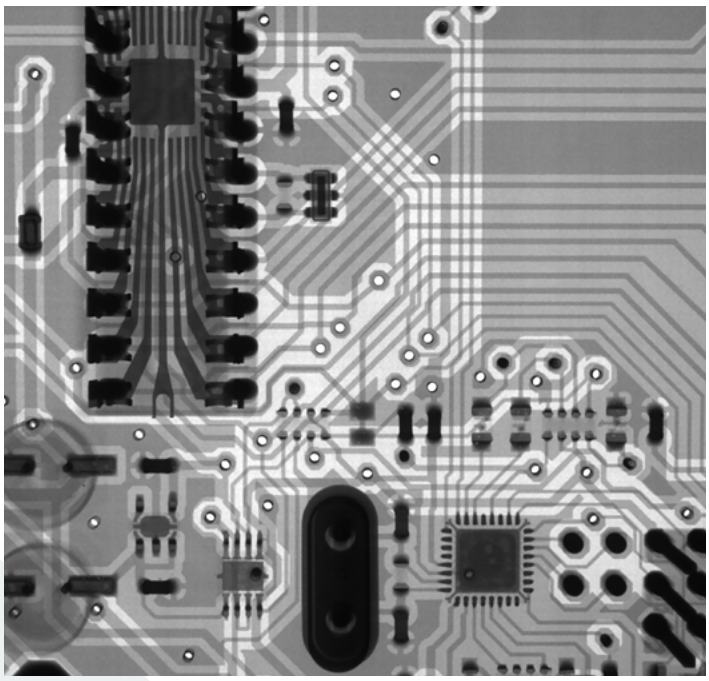
En ce qui a trait à la date que nous attribuons à un cyberincident, il peut s'agir du moment où l'incident a concrètement eu lieu, ou du moment où il a été publicisé. Nous privilégions la première approche, mais il arrive fréquemment que la date exacte du début d'un incident ne puisse être établie. C'est particulièrement vrai de vagues de cyberespionnage, furtives par nature, ou de campagnes de désinformation échelonnées sur de longues périodes. Lorsque c'est le cas, nous prenons alors pour référence la date à laquelle l'incident a été repéré ou publicisé.

En ce qui concerne l'origine, nous opérons une distinction entre la provenance (géographique) et la responsabilité (politique) d'un incident. Nous favorisons dans ce rapport la donnée géographique, du fait qu'elle est techniquement plus facile à établir, et qu'il est assez rare que la responsabilité d'un cyberincident soit publiquement attribuée. Dans un cas comme dans l'autre, les origines citées dans le rapport s'appuient sur les conclusions publiques des organismes ayant investigué un incident donné : rapports de firmes de cybersécurité, communiqués d'agences de sécurité nationale, etc. Nous invitons les lectrices et lecteurs à parcourir le répertoire en ligne pour plus de détails sur l'origine donnée à chaque incident.

Sur quelles sources le répertoire et le rapport s'appuient-ils ?

Les données du répertoire des cyberincidents canadiens, sur lequel ce rapport s'appuie, sont établies à partir des types de sources suivants : contenus produits par des médias professionnels respectant les principes énoncés par la Charte de Munich ; études et rapports d'institutions gouvernementales, universitaires ou privées (entreprises de cybersécurité, think tanks, ONG, etc.) ; communiqués d'organes gouvernementaux canadiens et étrangers ; publications scientifiques et autres bases de données, soumises à une évaluation par les pairs.

Ces sources sont autant que possible soumises à recoupement entre elles. Nous invitons les lectrices et lecteurs à parcourir le répertoire en ligne afin de consulter les sources propres à chaque cas.



Chaire Raoul-Dandurand
en études stratégiques et diplomatiques

Université du Québec à Montréal

dandurand.uqam.ca

Révision :
Yvana Michelant-Pauthex
Louis Collerette

Graphisme :
Françoise Conea

Avec l'appui de :

BANQUE NATIONALE