UQÀM

CHAIRE RAOUL-DANDURAND
EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES
25 ans

Cyberincidents géopolitiques au Canada

ÉTAT DES LIEUX 2022

Proposé par l'Observatoire des conflits multidimensionnels

@Joiseyshowaa/Flickr

Sommaire

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 le public sur la manière dont les mutations sécuritaires contemporaines, notamment l'usage malveillant des technologies de l'information, affectent des États comme le Canada, leurs gouvernements, la société civile, le secteur privé et les citoyennes et citoyens.

Les auteur.e.s de ce rapport

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 diplômé en relations internationales de l'Université de Genève et titulaire d'une maîtrise en études internationales de l'Université de Montréal. 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 politique étrangère.

Danny Gagné est candidat au doctorat en science politique à l'Université du Québec à Montréal 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 ont fait l'objet de nombreuses chroniques des nouvelles conflictualités de la Chaire Raoul-Dandurand portant sur la manipulation de l'information à des fins géopolitiques comme lors des récents troubles au Kazakhstan ou encore dans les relations entre la Russie et les Forces armées canadiennes postées en Europe sous l'égide de l'OTAN.

Gabrielle Gendron est étudiante à la maîtrise en science politique à l'UQAM et chercheure en résidence à l'Observatoire des conflits multidimensionnels. Elle travaille notamment sur le développement de l'économie numérique et des nouvelles technologies chinoises, la cybersécurité dans la région de l'Asie du Sud-Est, les initiatives numériques du projet Belt and Road Initiative (BRI), et l'exportation numérique chinoise dans le monde. Elle contribue régulièrement aux chroniques des nouvelles conflictualités de la Chaire Raoul-Dandurand.

Quelques cyberincidents récents

Février 2020

DÉSINFORMATION SUR L'ORIGINE DU CORONAVIRUS

Des sites de propagande russes et arabophones propagent une fausse rumeur selon laquelle la COVID-19 aurait été créée dans des laboratoires canadiens, avant d'être envoyée en Chine. D'autres versions de la fausse nouvelle affirment que la souche du virus aurait été volée par des espions chinois infiltrés au Canada.

Septembre 2020

CAMPAGNE DE SURVEILLANCE D'ACTIVISTES IRANIENS

Le rapport d'une ONG révèle l'existence d'une vaste campagne de cyberespionnage d'activistes pour la défense des droits humains en Iran. Celle-ci a visé plusieurs centaines d'individus dans une quinzaine de pays, dont le Canada.

Octobre 2020

VAGUE DE CYBERESPIONNAGE « SILENT LIBRARIAN »

Une firme de cybersécurité dévoile que le groupe de pirates informatiques iranien Silent Librarian a mené des tentatives de piratage contre des universités dans huit pays, dont le Canada. L'Université de Toronto, l'Université Western et l'Université McGill figurent parmi les cibles identifiées.

Novembre 2020

CYBERESPIONNAGE DE LA RECHERCHE SUR LA COVID-19

Une nouvelle vague de cyberespionnage pharmaceutique vise sept entreprises travaillant sur un vaccin contre la COVID-19. Ces activités se déploient dans cinq pays, dont le Canada. Microsoft attribue les attaques à des groupes de pirates informatiques étatiques travaillant pour la Russie et la Corée du Nord.

Février 2021

IDENTIFICATION DE TWEETS RUSSES FRAUDULEUX

Twitter désactive un ensemble de 373 comptes frauduleux, suspectés d'être utilisés par des États à des fins de désinformation. L'organisme canadien DisinfoWatch identifie des comptes provenant de Russie ayant publié des messages sur le Canada. Ceux-ci ont traité d'enjeux comme l'Arctique, l'OTAN ainsi que de leaders politiques canadiens, dont Justin Trudeau, Stephen Harper et Chrystia Freeland.

CYBERINCIDENT À LA NSIRA

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (abrégé NSIRA en anglais) annonce avoir été victime d'un cyberincident. Des fichiers protégés, mais non classifiés, ont été volés par un acteur tiers, dont l'identité n'a toutefois pas été révélée.

MARS 2021

CAMPAGNE DE SURVEILLANCE CONTRE DES ACTIVISTES OUÏGHOURS

Facebook révèle l'existence d'une opération de cyberespionnage chinoise ayant visé des journalistes et des activistes militant pour les droits des Ouïghours dans plusieurs pays. Environ vingt des personnes ciblées sont établies au Canada.

Janvier 2022

CYBERINCIDENT À AFFAIRES MONDIALES CANADA

Affaires mondiales Canada est victime d'un cyberincident, dont la nature exacte n'est pas précisée. Certains services en ligne du ministère sont rendus temporairement indisponibles par les mesures de mitigation de l'incident. Sur fond de crise entre la Russie et l'Ukraine, des sources gouvernementales anonymes interrogées dans les médias envisagent que la Russie puisse avoir une responsabilité.

LE CANADA ET LES CYBERINCIDENTS GÉOPOLITIQUES À L'HORIZON 2022

L'actualité de l'année 2021 a montré à quel point les cyberattaques, les campagnes de surveillance électronique ou encore les opérations de désinformation en ligne font partie du quotidien international aujourd'hui. La poursuite de la pandémie de COVID-19, particulièrement, a contribué à sa manière à une multiplication des cyberincidents de tous types, à laquelle le Canada n'a pas échappé. Si l'immense majorité des actions malveillantes menées dans le cyberespace continue de relever essentiellement de cybercriminalité, les cyberincidents à caractère géopolitique, le plus souvent orchestrés par des États, ne diminuent pas. En janvier 2022 encore, on apprenait qu'Affaires mondiales Canada avait fait l'objet d'une cyberintrusion, que différentes sources gouvernementales soupçonnaient de provenir de Russie.

S'inscrivant dans une dynamique globale de « cyberconflictualité » constante entre les États, de tels incidents se révèlent relativement fréquents au Canada : l'analyse réalisée dans le cadre de ce rapport (sans prétendre à l'exhaustivité) a recensé **pas moins de 75 cyberincidents géopolitiques au Canada depuis 2010**. Dans une perspective plus récente, on dénombre 21 cyberincidents à caractère géopolitique ayant touché le Canada sur la période 2020-2021. En quoi précisément ont consisté ces actions malveillantes ? Que sait-on de leur origine ? Quels genres d'entités ont-ils visés ? La présente section répond à ces questions en se concentrant sur la période 2020-2021. Les informations présentées ci-après s'appuient sur les données actualisées du répertoire des cyberincidents canadiens entretenu par la Chaire Raoul-Dandurand en études stratégiques et diplomatiques depuis la création de l'OCM en 2019.

Quels genres de cyberincidents sont les plus fréquents ?

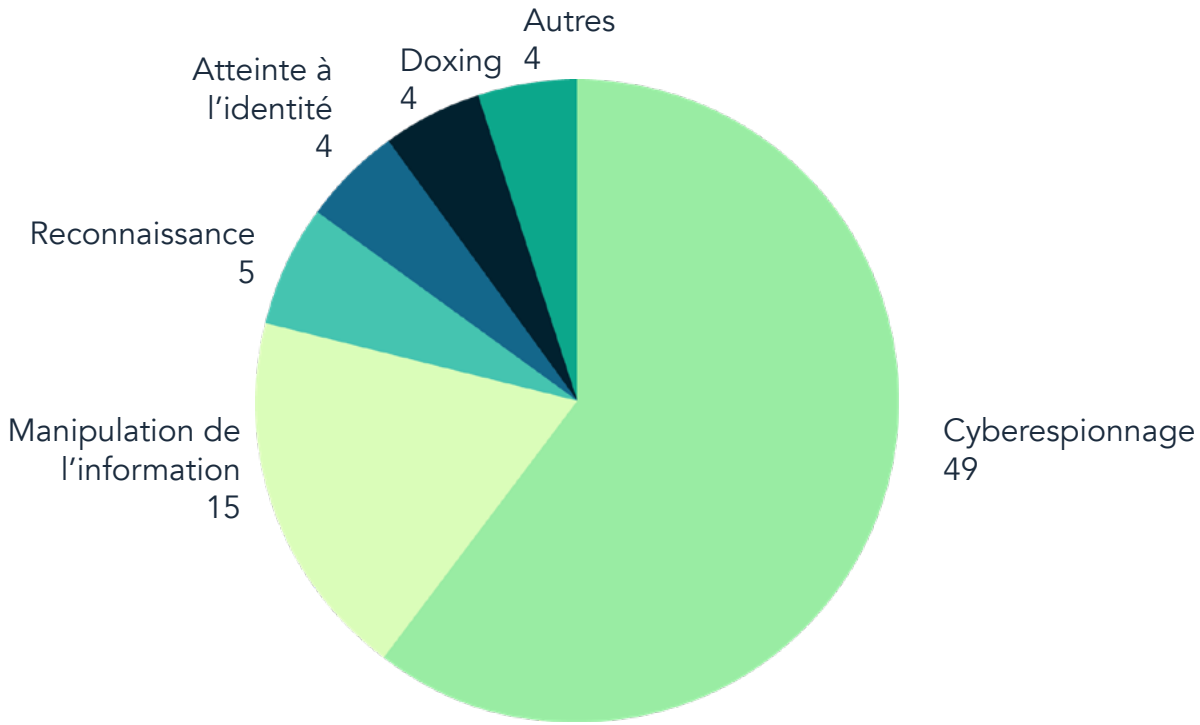
La très grande majorité des cyberincidents à caractère géopolitique touchant le Canada continue de relever du cyberespionnage, soit le fait d'obtenir par des moyens numériques de l'information sans l'accord préalable du détenteur de cette information. Cette catégorie comprend par exemple le vol de secrets d'État, le vol de propriété intellectuelle, ou encore la surveillance clandestine d'individus. **Sur les 75 incidents répertoriés depuis 2010, pas moins de 49 relèvent de cyberespionnage**. Le deuxième type de cyberincident le plus fréquent est la manipulation de

Qu'entend-on par cyberincidents ?

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 disponible 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 recherches, 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 ayant touché une diversité de pays (incluant le Canada). Les incidents recensés remontent jusqu'à 2010.

TYPES DE CYBERINCIDENTS LES PLUS FRÉQUENTS



Source : Répertoire des cyberincidents canadiens (www.dandurand.uqam.ca/cyberincidents)

l'information, à savoir la diffusion intentionnelle, massive et coordonnée de nouvelles fausses ou biaisées dans le cyberespace à des fins politiques hostiles. Notre équipe estime qu'une quinzaine d'incidents notables de ce type se sont produits depuis 2010. Viennent ensuite (par ordre de prévalence) les opérations de reconnaissance, les atteintes à l'identité et les actes de doxing[1].

Cyberespionnage : quelles sont les cibles connues ?

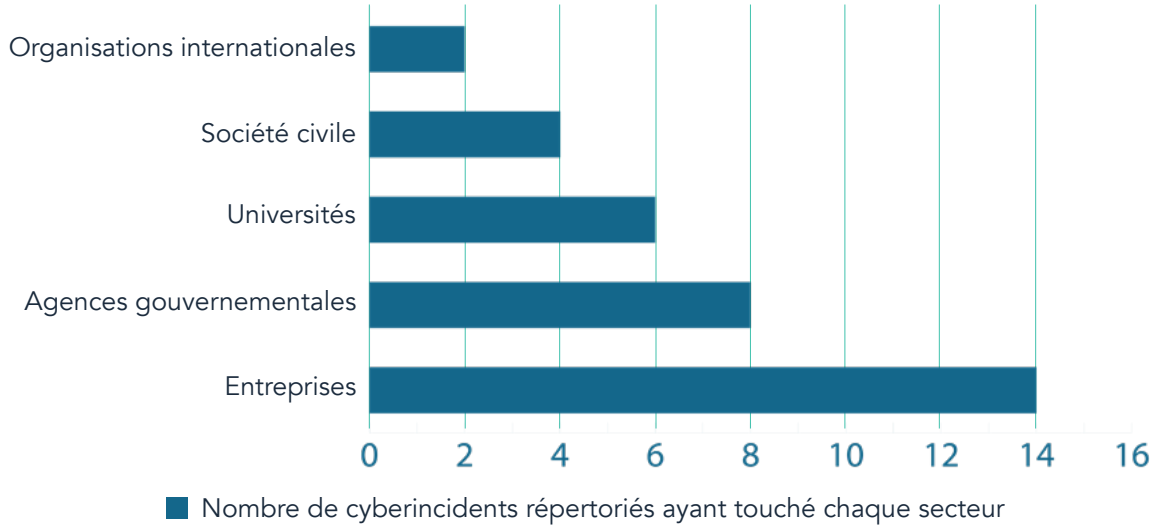
Si l'on ne connaît pas toujours la nature exacte des campagnes de cyberespionnage, il apparaît toutefois qu'environ la moitié des opérations répertoriées relevait au moins en partie d'espionnage économique ou industriel, visant par exemple des entreprises ou des universités. Parmi les secteurs d'activité ou de recherche et développement les plus touchés figurent les technologies de l'information, l'énergie, la finance et l'aérospatiale. Environ un quart des incidents relève d'espionnage interétatique plus traditionnel, visant des agences gouvernementales canadiennes. Dans bien des cas, toutefois, la nature des entités visées demeure inconnue.

À quelle fréquence le Canada est-il objet de cyberincidents ?

Depuis 2017, **on recense en moyenne dix cyberincidents à caractère géopolitique par année au Canada**. L'année 2020 a été marquée

1 Pour les définitions spécifiques de chaque type de cyberincidents, voir la rubrique « Comment ce rapport a-t-il été établi ? » située à la fin du document.

VICTIMES CONNUES DE CYBERESPIONNAGE AU CANADA



Source : Répertoire des cyberincidents canadiens (www.dandurand.uqam.ca/cyberincidents)

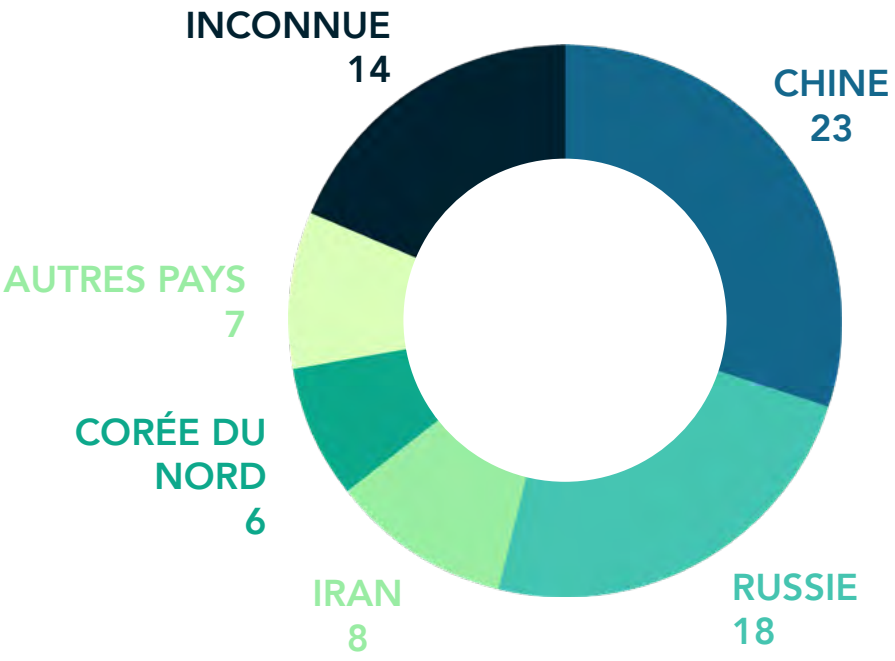
par un pic, avec treize incidents, tandis que 2021 a bénéficié d'une relative accalmie, avec huit incidents. Il importe toutefois de noter que de nombreux cyberincidents ne sont repérés ou publiquement révélés que plusieurs mois après leur occurrence. Il faut donc envisager que d'autres événements viendront prochainement s'ajouter au bilan de 2021.

D'où proviennent la plupart de ces actes ?

Depuis 2010, **quatre pays sont à l'origine de la grande majorité des cyberincidents géopolitiques** recensés dans le cadre de cette analyse : la Chine (23 incidents sur 75), la Russie (18), l'Iran (8) et la Corée du Nord (6). Ces données concernent l'origine géographique des cyberincidents ayant touché le Canada et n'impliquent pas nécessairement une responsabilité des gouvernements des pays mentionnés[2]. Occasionnellement, certains incidents sont par exemple l'œuvre d'acteurs non étatiques qui agissent indépendamment des gouvernements des pays d'où ils opèrent. Par ailleurs, établir l'origine d'un incident exige souvent du temps et des ressources importantes. Dès lors, quatorze des incidents recensés depuis 2010 n'ont pour le moment pas d'origine connue.

2 Pour plus de détails, voir la rubrique « Comment ce rapport a-t-il été établi ? ».

ORIGINE GÉOGRAPHIQUE DES CYBERINCIDENTS (depuis 2010)



Source : Répertoire des cyberincidents canadiens (www.dandurand.uqam.ca/cyberincidents)

Quels groupes de pirates sont particulièrement actifs contre le Canada ?

Bien qu'attribuer la responsabilité d'un cyberincident soit une démarche complexe et souvent de longue haleine, un certain nombre de groupes de pirates informatiques étatiques sont bien connus de la communauté de la cybersécurité. Par exemple, les méthodes d'intrusion déployées par ces groupes sont reconnaissables et permettent de les retracer ainsi que d'associer divers incidents à un même acteur. Ces efforts d'investigation cumulés démontrent qu'une petite poignée de groupes de pirates sont responsables d'un nombre important de cyberincidents ayant touché le Canada dans les dernières années. Il s'agit notamment des groupes Cozy Bear (Russie), Silent Librarian (Iran), APT 10 (Chine) et Lazarus Group (Corée du Nord), qui cumulent à eux seuls onze cyberincidents depuis 2017. Cozy Bear et Lazarus Group ont par exemple pris part aux tentatives d'espionnage de la recherche canadienne sur la COVID-19 au fil de l'année 2020. Les pirates de Silent Librarian ont, quant à eux, mené trois campagnes successives de vol de propriété intellectuelle auprès d'universités, dont plusieurs canadiennes. Le tableau ci-dessous présente les incidents canadiens ayant été formellement attribués à chacun de ces acteurs[3].

3 La classification et la nomenclature entourant les groupes de pirates informatiques sont complexes. D'une part, les grandes firmes de cybersécurité emploient des systèmes d'appellation distincts, qui donnent lieu à une diversité de noms pour un même acteur. D'autre part, les groupes de pirates changent de composition au gré de leurs campagnes. Il est donc difficile de savoir quand et comment établir une filiation ou au contraire une distinction entre des groupes. Le tableau ci-contre présente des acteurs dont la composition semble être restée stable au fil des incidents mentionnés. Il se limite aux appellations les plus fréquemment utilisées.

COZY BEAR	SILENT LIBRARIAN	LAZARUS GROUP	APT 10
• Espionnage de la recherche canadienne sur la COVID-19 (2020) • Incident Solar Winds (2020); une centaine d'entités canadiennes visées • Vague d'hameçonnage contre des entreprises et agences étatiques dans différents pays (2021)	• Campagne d'espionnage contre des universités (2013-2017) • Campagne d'espionnage contre des universités (2019) • Vague d'hameçonnage (2020); au moins trois universités canadiennes visées	• Attaque du rançongiciel WannaCry (2017) • Campagne d'espionnage « Operation GhostSecret » (2018) • Espionnage de la recherche canadienne sur la COVID-19 (2020)	• Piratage de la firme Equifax (2017), données de 19 000 clients canadiens compromises • Campagne d'espionnage Cloud Hopper (2018)

Trois tendances à surveiller

Si la cyberconflictualité n'est pas un phénomène nouveau au Canada, la période 2020-2021 a consacré l'apparition ou l'accentuation de certaines dynamiques notables en matière de cyberincidents. La présente section vise à présenter et à analyser trois tendances qui, sans être nécessairement représentatives de la majorité des cyberincidents au Canada, semblent importantes à surveiller à l'avenir : le cyberespionnage de plus en plus fréquent par des puissances étrangères d'activistes établis au Canada ; l'usage grandissant du cybermercenariat par les États et d'autres acteurs ; l'essor massif des cyberattaques par rançongiciel.

ACTIVISTES & DISSIDENTS

LORSQUE LA SURVEILLANCE S'EXPORTE

Dans les dernières années, le développement de nouvelles capacités cyber par de plus en plus d'États a contribué à transformer drastiquement le paysage mondial du renseignement. Le cyberespace fournit en effet aux États un moyen de recueillir de l'information confidentielle et de mener des cyberattaques sans craindre de répercussions importantes. L'information convoitée par les cyberespions étatiques est vaste, allant des secrets d'État à la propriété intellectuelle, ou aux informations personnelles de décideurs clés, pour ne citer que certains exemples. Cependant, depuis quelques années, une nouvelle tendance vient s'ajouter aux phénomènes déjà bien connus du cyberespionnage stratégique et économique : la surveillance électronique de membres de la société civile, d'activistes pour les droits humains ou d'individus appartenant à des minorités opprimées.

L'information convoitée par les cyberespions étatiques est vaste, allant des secrets d'État à la propriété intellectuelle (...)

Si le développement des nouvelles technologies, des réseaux d'information et du cyberespace offrait la possibilité de démocratiser l'accès à celui-ci, ces mêmes technologies sont désormais utilisées par des gouvernements, le plus souvent autoritaires, contre les opposants politiques, les lanceurs d'alerte et les dissidents. Le cyberespace est devenu un territoire où se prolongent les

luttes de pouvoir sociopolitiques et où les capacités de surveillance des régimes en place ont été décuplées. Porteuses de grandes conséquences, ces attaques ne cessent de se multiplier, traversent les frontières et touchent directement le Canada.

Opprimés en Chine, surveillés à l'étranger : le cas des Ouïghours

L'espionnage d'activistes par les instances étatiques a augmenté massivement au cours de la dernière décennie, tout comme la surveillance ciblée des minorités. Cette expansion s'illustre notamment dans le cas de la surveillance chinoise à l'encontre de la communauté ouïghoure. En Chine même, Pékin a développé depuis quelques années des compétences saisissantes dans le domaine de la surveillance numérique à des fins de contrôle social, notamment grâce aux entreprises technologiques chinoises de pointe. La République populaire démontre également une volonté d'étendre sa machine de surveillance hors de ses frontières : les diasporas ouïghoures à l'étranger font fréquemment l'objet de cyberattaques visant à collecter des renseignements ou à intimider les critiques du parti.

En septembre 2019, la firme d'analyse en cybersécurité Volexity a identifié onze sites Internet dédiés aux enjeux ouïghours et à la région du Turkestan oriental ayant été compromis à des fins de surveillance. Selon Volexity, ces sites, qui représentent une source majeure d'informations sur ces questions, ont été exploités à leur insu depuis 2013 pour espionner et lancer des cyberattaques contre la communauté ouïghoure dans le monde entier. La firme constatait en effet que tous les sites compromis sont bloqués par le « grand pare-feu » de la Chine[1]. Tout indique que ce sont donc spécifiquement les membres de la diaspora qui étaient visés.

En Chine même, Pékin a développé depuis quelques années des compétences saisissantes dans le domaine de la surveillance numérique à des fins de contrôle social

Plus récemment, les entreprises de cybersécurité Check Point et Kaspersky ont repéré une nouvelle campagne chinoise de piratages visant des personnalités importantes de la communauté ouïghoure en Chine et au Pakistan. Les pirates se faisaient passer pour des membres d'organismes des Nations unies ou pour ceux d'une organisation de défense des droits humains nommée Turkic Culture and Heritage Foundation. Sous ces fausses identités, les espions invitaient leurs cibles à télécharger un faux scanner de vulnérabilité[2],

1 Grande muraille virtuelle qui censure, grâce à de nombreux filtres, l'accès à différents sites ou réseaux sociaux. Des systèmes automatisés traquent aussi les mots-clés dans l'optique de censurer la population chinoise, mais aussi d'éviter l'influence externe.

2 Un scanner de vulnérabilité est un programme conçu pour rechercher et détecter des vulnérabilités dans une application, un système d'exploitation ou un réseau.

qui permettait en réalité l'installation d'un logiciel malveillant donnant discrètement accès aux ordinateurs des victimes. La manœuvre permettait par exemple d'exfiltrer des informations sur les appareils infectés, y compris des programmes en cours d'exécution.

Un schéma qui se répète

Ces campagnes sont devenues un outil important dans l'arsenal répressif déployé par Pékin contre cette minorité musulmane, en Chine et dans bien d'autres pays, y compris le Canada. Le cas des Ouïghours n'est cependant pas isolé, et d'autres communautés de la diaspora, elles aussi jugées problématiques par le parti, font l'objet de cyberespionnage et de harcèlement par l'appareil sécuritaire chinois.

Le cas des Ouïghours n'est cependant pas isolé, et d'autres communautés de la diaspora, elles aussi jugées problématiques par le parti, font l'objet de cyberespionnage et de harcèlement par l'appareil sécuritaire chinois.

Au Canada, des individus d'origine tibétaine ou des organisations militant pour la cause du Tibet ont été victimes de telles opérations. Le *Citizen Lab* de l'Université de Toronto a notamment révélé en 2013 une campagne de cyberespionnage du groupe de pirates informatiques chinois APT 1 (unité 61398 de l'Armée populaire de libération) ayant visé des organisations tibétaines canadiennes.

Depuis 2010, les adeptes du Falun Gong[3] vivant au Canada disent également avoir fait l'objet de plusieurs opérations d'intimidation et de salissage orchestrées par Pékin. En 2015, 2018 et 2019 notamment, des courriels insultants et menaçants ont été envoyés à des ministres ou des membres du Parlement canadien. Leurs auteurs se présentaient faussement comme des pratiquants du Falun Gong. Le traçage de plusieurs de ces courriels renvoyait à des adresses IP en Chine, incitant de nombreux observateurs à conclure à une implication de l'État chinois.

D'autres États impliqués

Il apparaît par ailleurs que la Chine n'est pas le seul État à s'adonner au cyberespionnage d'opposants ou activistes pour les droits humains sur le sol canadien. En 2018, le Citizen Lab révélait que le dissident saoudien (établi au Québec) Omar Abdulaziz avait été visé par une opération de surveillance électronique. Son téléphone avait été infecté par le désormais bien connu logiciel espion Pegasus. Créé par la firme israélienne NSO, ce logiciel donne un accès presque illimité[4]

3 Le Falun Gong, ou Falun Dafa, est un mouvement spirituel inspiré de la tradition bouddhiste et interdit en Chine depuis 1999. Ses pratiquants sont persécutés par le Parti communiste, qui considère le mouvement comme une menace à son hégémonie politique.

4 Selon Lookout Threat, Pegasus est l'un des logiciels de surveillance et d'espionnage les plus sophistiqués à ce jour. Il est muni

à l'ensemble des données contenues dans un téléphone et permet une surveillance en temps réel via la caméra et le microphone de l'appareil. L'incident était attribué au groupe KINGDOM, qu'on soupçonne d'être associé aux services de sécurité saoudiens.

En septembre 2020, un rapport de l'ONG Miaan Group révélait l'existence d'une campagne d'espionnage ayant visé plusieurs centaines d'activistes impliqués dans la défense des droits humains en Iran. Mêlant journalistes, activistes, avocats, ou militants étudiants, le plus souvent issus de minorités ethniques ou religieuses iraniennes, les victimes en question étaient établies dans une quinzaine de pays, dont le Canada. Faisant enquête sur cette même opération, la firme de cybersécurité Check Point concluait à une très probable implication de l'État iranien.

De plus en plus fréquents, de tels cyberincidents laissent craindre que le Canada, abritant de nombreuses ONG et membres de groupes de défense des droits humains, ne devienne un terrain d'intrusion privilégié pour les puissances étrangères autoritaires. Ces incidents soulèvent également de graves enjeux pour le respect des droits humains et du droit à la vie privée en sol canadien. Alors que la Chine, particulièrement, témoigne d'un développement numérique fulgurant et tente d'exporter son modèle d'autoritarisme numérique auprès d'autres régimes, cette problématique n'est vraisemblablement appelée qu'à s'accentuer.

d'un mécanisme pour s'installer, se cacher et obtenir l'accès aux sauvegardes de données sur un système. Sa collecte de données est l'une des plus complètes : données de valeur évidente, mots de passe, contacts, entrées de calendrier, données de nombreux réseaux sociaux et bien d'autres.

Un cas canadien : campagne d'hameçonnage contre des activistes ouïghours (2021)

En mars 2021, Facebook annonce avoir pris des mesures contre un groupe de pirates informatiques ayant utilisé sa plateforme pour espionner des activistes ouïghours établis à l'étranger. La compagnie dit avoir identifié un peu moins de 500 cibles, en grande partie originaire de la région chinoise du Xinjiang, mais vivant en Turquie, au Kazakhstan, aux États-Unis, en Syrie, en Australie ou encore au Canada. Environ 20 personnes touchées par cette vaste campagne de surveillance vivraient en sol canadien.

L'opération est attribuée par Facebook au groupe de hackers se faisant appeler Earth Empusa, ou Evil Eye et parfois Poison Carp. Le groupe, basé en Chine, est largement suspecté d'entretenir des liens avec le gouvernement de la République populaire. C'est d'ailleurs aussi à Earth Empusa que les campagnes découvertes par Volexity en 2019, et Checkpoint & Kapersky en 2021, ont été attribuées.

Selon Facebook, les pirates ont usé de plusieurs tactiques pour mener à bien leur campagne de cyberespionnage. Ils ont notamment créé des comptes Facebook frauduleux destinés à inspirer la confiance de la communauté ouïghoure, en se faisant passer pour des journalistes, ou pour des membres des communautés étudiante, de défense des droits humains ou de la communauté ouïghoure elle-même. Les pirates ont également mis en ligne des pages Internet imitant des sites de nouvelles populaires ouïghours et turcs, ainsi que des boutiques et des applications qui contenaient un logiciel espion connu sous le nom d'Insomnia.

Cette récente campagne de cyberespionnage apparaît comme une extension de la machine de surveillance chinoise qui sévit au Xinjiang, et qui fait écho aux directives de sécurité nationale et aux efforts de « contre-terrorisme » promulgués par le gouvernement chinois. En effet, la campagne « Strike Hard Campaign against Violent Terrorism », qui est dirigée contre la communauté musulmane chinoise, a engendré une forte hausse du développement de logiciels malveillants utilisés par la suite dans le cadre des diverses campagnes d'espionnages citées précédemment.

Alors que le Canada héberge une communauté ouïghoure d'environ 2000 personnes, de nombreux membres de cette minorité ont rapporté avoir subi de fréquents actes de harcèlement ou d'intimidation en sol canadien, dont des appels téléphoniques assortis de menace de mort ou de viol. Certains ont également témoigné que les autorités locales dans le Xinjiang s'en prenaient à leurs proches restés au pays, afin de les dissuader de poursuivre leurs revendications.

HACKERS À GAGE

LE CANADA DANS L'ŒIL DES CYBER-MERCENAIRES

Le Canada était déjà la cible d'actions malveillantes de la part de cybercriminels ou de pirates informatiques étatiques. Or, il est désormais confronté à un nouveau type d'acteur : des groupes privés pratiquant le piratage informatique sur demande, pour le compte du plus offrant. Prenant souvent la forme d'entreprises de sécurité privée, ou parfois d'organisations clandestines, ces cybermercenaires rassemblent un savoir-faire de pointe qu'ils monnaient plus ou moins ouvertement à une variété d'acteurs. Parmi ceux-ci figurent des sociétés peu scrupuleuses en quête de secrets commerciaux, ou des gouvernements cherchant à doper leur appareil sécuritaire.

Phénomène encore embryonnaire il y a quelques années, le cybermercenariat constitue maintenant un marché transnational bien organisé, dont l'offre de services rivalise avec celle de certaines agences de sécurité étatiques. Ces dernières s'avèrent d'ailleurs un bassin de recrutement important pour cette industrie. En 2019, une enquête de Reuters révélait l'existence d'une firme baptisée Dark-Matter, employant d'anciens membres de la NSA et marchandant ses capacités de cyber-espionnage au gouvernement des Émirats arabes unis. Plus récemment, la société Global Risk Advisors, comptant dans ses rangs des personnes précédemment employées par la CIA, était accusée d'avoir mené une vaste campagne de piratages informatiques pour le compte du gouvernement qatari.

Le cybermercenariat constitue maintenant un marché transnational bien organisé, dont l'offre de services rivalise avec celle de certaines agences de sécurité étatiques.

Entre prolifération et déni plausible

La palette des prestations offertes par cette industrie s'échelonne sur plusieurs niveaux, et ne cesse de s'élargir : formation de services de sécurité étrangers, assistance à l'élaboration de techniques d'intrusion, et dans bien des cas, exécution directe de cyberopérations hautement sophistiquées (le plus souvent d'espionnage électronique). Les

modes d'organisation des acteurs du cybermercenariat varient. Certains, travaillant dans une clandestinité relative, s'appuient sur les réseaux cybercriminels pour vendre des services ponctuels. D'autres, professionnalisés et parfois formellement constitués en entreprise, agissent sur une base quasi contractuelle.

Cette dynamique de sous-traitance, qui s'ajoute à la commercialisation de logiciels espions par des firmes privées (telle la société israélienne NSO), soulève de nombreuses questions relatives à la prolifération des capacités cybernétiques offensives. Elle vient également brouiller les cartes d'une cyberconflictualité internationale déjà souvent difficile à déchiffrer : agissant comme des intermédiaires pour les puissances qui les emploient, les groupes de cybermercenaires offrent aux États un potentiel de déni plausible et compliquent donc le fameux problème de l'attribution des cyberattaques à leurs auteurs.

Causes peu louables

Ce n'est toutefois pas là le seul objet de controverse entourant le cybermercenariat : un nombre croissant d'observateurs reproche à certains cybermercenaires d'employer leur savoir-faire contre les intérêts de leur État d'origine. Des ex-membres de la NSA recrutés par DarkMatter furent par exemple mandatés de viser des citoyennes et citoyens américains, certains allant jusqu'à intercepter des courriels échangés entre la Première dame

de l'époque, Michelle Obama, et un membre de la famille royale qatarie. D'autres voix reprochent parallèlement aux pirates américains de Global Risk Advisors d'avoir aidé le Qatar à espionner de hauts dirigeants de la FIFA, l'aidant ainsi à remporter l'organisation de la Coupe du monde de football 2022, pour laquelle les États-Unis concourraient eux aussi.

> (...) agissant comme des intermédiaires pour les puissances qui les emploient, les groupes de cybermercenaires offrent aux États un potentiel de déni plausible

Plus globalement, les fréquentes révélations entourant l'industrie du cybermercenariat démontrent aussi que celle-ci est dans bien des cas mise au service de causes peu louables, souvent au bénéfice de régimes autoritaires : traque d'opposants politiques, espionnage d'ONG et de journalistes, vol d'informations personnelles à des fins de chantage, entre autres. Si la communauté des « hackers à gage » prétend être simplement pourvoyeuse de cybersécurité pour ses clients, force est de constater qu'en l'absence de régulations dignes de ce nom, elle constitue une sérieuse source d'insécurité pour de nombreux individus à travers le monde.

Premiers signes au Canada

Le phénomène du cybermercenariat commence maintenant à toucher le Canada. En juin 2020, la firme Norton LifeLock et le Citizen Lab de l'Université de Toronto révélaient une vaste campagne malveillante menée par une firme indienne de piratage sur demande, ayant entre autres visé des entités canadiennes (voir plus bas). Plus récemment, en novembre 2021, la firme de cybersécurité Trend Micro publiait un rapport détaillé sur un groupe de cybermercenaires russophones baptisé Void Balaur (ou Rockethack). Ce dernier aurait, depuis 2015, mené de vastes campagnes de piratage dans 30 pays, dont le Canada.

> Les prestations fournies par ces « hackers à gage » auraient donc inclus autant la surveillance d'opposants politiques que le cyberespionnage économique.

Bien que le nombre et la nature des cibles canadiennes de Void Balaur n'aient pas été précisés, Trend Micro indiquait que le groupe s'était, globalement, adonné au cyberespionnage et au vol de données d'une grande variété de cibles : activistes pour les droits humains, journalistes, membres de partis politiques ou diplomates, mais aussi cadres d'entreprises de plusieurs secteurs. Les prestations fournies par ces « hackers à gage » auraient donc inclus autant la surveillance d'opposants politiques que le cyberespionnage économique. L'identité des commanditaires de Void Balaur demeure néanmoins inconnue, de même que le pays depuis lequel opère le groupe.

Cible avérée, sanctuaire potentiel

Les effets du cybermercenariat se font sentir jusque sur les plateformes de médias sociaux : fin 2021, Meta annonçait avoir identifié et désactivé 1500 comptes Facebook frauduleux, employés par diverses firmes de piratage pour piéger leurs cibles. Ces profils factices cherchaient à se faire passer pour des personnes dignes de confiance, pour prendre contact avec les personnes visées et les inviter à cliquer sur des liens infectés, dans le but d'espionner leur ordinateur ou leur téléphone cellulaire. Alors que Meta disait avoir recensé près de 50 000 victimes dans plus de 100 pays, il est plus que probable que des individus résidant au Canada figuraient parmi celles-ci.

Si le Canada figure donc déjà parmi les pays touchés par les groupes de cybermercenaires, il pourrait aussi devenir un territoire depuis lequel opèrent de telles entités. En mars 2017 déjà, sur requête de la justice américaine, un citoyen canadien était arrêté pour avoir monnayé ses compétences en piratage au renseignement russe, dans le cadre d'une colossale brèche informatique ayant frappé Yahoo. Le pirate en question n'entretenait pas de liens particuliers avec Moscou, mais avait simplement été mandaté par des agents russes via une plateforme cybercriminelle sur laquelle il promouvait ses services. Le Canada, riche en main-d'œuvre du secteur des technologies de l'information et abritant de nombreuses firmes du domaine de la cybersécurité, présente donc lui aussi le potentiel de voir émerger une industrie du piratage sur demande, avec toutes les dérives potentielles qu'un tel phénomène impliquerait.

Un cas canadien : la campagne de piratage de « Mercenary.Amanda » (2020)

En juin 2020, la firme de cybersécurité américaine NortonLifeLock et le Citizen Lab de l'Université de Toronto publient simultanément deux rapports, fruits de plusieurs mois d'investigation. Les documents en question jettent la lumière sur une longue campagne de piratages informatiques, menée entre 2017 et 2020 par un groupe de « hackers à gage » basé en Inde. Cette entité, baptisée « Mercenary.Amanda » par NortonLifeLock (et « Dark Basin » par le Citizen Lab), aurait pris pour cible au moins 220 organisations et plus de 1800 adresses courriel dans une quinzaine de pays, dont le Canada. Une enquête de Reuters, publiée au même moment, avance quant à elle que le groupe aurait piraté plus de 10 000 comptes de messagerie depuis 2013.

Les enquêtes conjointes révèlent que ces pirates, mêlant espionnages politique, industriel et financier, s'en sont pris à une large palette d'acteurs : figures politiques, journalistes, groupes environnementalistes, juges, hauts fonctionnaires, fonds d'investissement, bureaux d'avocats, ou firmes de consultation politique, entre autres. Le Citizen Lab détaille notamment d'importantes activités menées contre une dizaine d'organisations écologistes américaines impliquées dans la campagne #ExxonKnew, comme Greenpeace ou Public Citizen.

L'équipe de l'Université de Toronto indique également avoir identifié, avec « un haut degré de confiance », l'entité se cachant derrière cette campagne de piratage : BellTroX InfoTech Services, une société basée à New Delhi, menant des piratages sur demande et active depuis 2013. Fait intéressant : BellTroX figurera en 2021 parmi les entreprises accusées par Meta d'avoir utilisé Facebook pour tenter de piéger ses victimes grâce à des clics sur des liens infectés.

Si les détails sur les entités canadiennes visées par Mercenary.Amanda sont maigres, le rapport de NortonLifeLock livre toutefois quelques chiffres : 4 % des entités ciblées seraient basées au Canada, ce qui en fait le cinquième pays le plus touché par la campagne. Plus de la moitié des victimes sont toutefois situées aux États-Unis. Sans distinguer par pays, le document révèle que les secteurs d'activité les plus visés sont respectivement la finance (32 % des cibles), les bureaux d'avocats (14 %), les organismes à but non lucratif (9 %), les consultants (8 %), le secteur manufacturier (6 %) et les médias (4 %).

Les commanditaires de la campagne opérée par BellTroX demeurent eux aussi pour l'heure inconnus. Reuters, citant d'anciens employés de la compagnie, suggère toutefois que celle-ci est généralement sollicitée par des figures politiques ou des entreprises pour espionner des opposants et des concurrents. Un autre ex-salarié, cité par le média indien *The Economic Times*, avance que BellTroX compterait au moins quatre ou cinq clients réguliers à l'étranger. Impliquant donc une firme privée, implantée dans un pays étranger, elle-même probablement employée par des acteurs basés dans d'autres pays encore, le cas de Mercenary.Amanda démontre tout le caractère protéiforme de l'enjeu du cybermercenariat.

RANÇONGICIELS

CROISSANCE EXPONENTIELLE, IMPACTS STRATÉGIQUES POTENTIELS

Les attaques par rançongiciels peuvent (...) engendrer des pertes financières importantes ou perturber les chaines d'approvisionnement d'un pays.

Si à première vue le caractère géopolitique des attaques par rançongiciel (ou « ransomware ») ne saute pas aux yeux, leur multiplication et l'amplification de leurs impacts, particulièrement au fil de l'année 2021, appellent à questionner cette perspective. Relevant dans la grande majorité des cas de cybercriminalité, les attaques par rançongiciels peuvent néanmoins engendrer des pertes financières importantes ou perturber les chaines d'approvisionnement d'un pays. Par ailleurs, ces attaques sont souvent menées par des groupes de pirates se jouant des frontières et opérant depuis des pays où ils ne sont pas repérés ou menacés par les autorités. Elles soulèvent donc également des enjeux diplomatiques pour les États qui en font les frais.

Comme l'indique son nom, l'attaque par rançongiciel est une tentative d'extorsion basée sur le déni et le vol de données. Des groupes criminalisés qui sillonnent Internet vont, par exemple, s'attaquer aux systèmes informatiques de grandes entreprises ou de services publics pour tenter d'accéder à leurs données et les rendre inaccessibles en les cryptant. Les pirates marchandent ensuite le décryptage et la restitution des informations en échange d'une rançon (souvent proportionnelle aux moyens financiers de l'entité visée).

Prises individuellement, les attaques par rançongiciel sont plus souvent une nuisance qu'un danger existentiel. Leur nombre a néanmoins explosé dans les dernières années et plus encore dans les derniers mois. En effet, une enquête de la firme britannique CybSafe révèle une augmentation de plus de 900 % des attaques par rançongiciel si on compare les six premiers mois de 2021 à la même période en 2020. Pour les entités ciblées, la facture est aussi de plus en plus salée. Le montant moyen des rançons exigées est passé de 5000 dollars américains en 2018, à pas moins de 200 000 dollars en 2020. Le département américain du Trésor estimait l'année dernière que les

attaques par rançongiciels avaient, durant la première moitié de 2021, permis d'extorquer au moins 590 millions de dollars (en crypto-monnaies) à diverses cibles.

> (...) une enquête de la firme britannique CybSafe révèle une augmentation de plus de 900 % des attaques par rançongiciel si on compare les six premiers mois de 2021 à la même période en 2020.

Risques d'impacts systémiques : le cas du Colonial Pipeline

Parmi les incidents récents aux retombées les plus spectaculaires, on retrouve bien sûr le cas du Colonial Pipeline. Rappelons les faits : le 7 mai 2021, l'employé d'un terminal de contrôle de cet oléoduc de la côte est américaine reçoit sur son poste de travail une demande de rançon en cryptomonnaie estimée à 5 millions de dollars américains. Inquiète d'une potentielle infiltration des serveurs de la compagnie par des pirates informatiques, l'entreprise décide d'éteindre tout son système informatique. L'oléoduc, par lequel transitent plus de 2.5 millions de barils de pétrole par jour, est alors inopérant.

Les systèmes vont rester verrouillés jusqu'au 12 mai, déclenchant ultimement une pénurie d'essence dans les stations-service d'une partie de la côte est des États-Unis, non pas parce que l'approvisionnement est coupé,

mais parce que la nouvelle du piratage a causé la panique chez les consommateurs, qui, inquiets, se sont rués vers les pompes pour faire des réserves. Résultat : jusqu'à 43% des stations-service en Géorgie et en Caroline du Sud et jusqu'à 65% en Caroline du Nord sont à sec. L'attaque, attribuée au groupe cybercriminel Darkside, a mené à une hausse des prix du carburant de 8% à l'échelle des États-Unis.

Évidemment, de telles attaques peuvent aussi avoir des ramifications à l'international. Si l'on prend l'exemple canadien, bien que le prix à la pompe n'ait que légèrement augmenté dans l'est du pays, l'incident a fait craindre un ralentissement de l'approvisionnement. Au niveau international, ce type d'attaque peut aussi faire des vagues sur les marchés financiers, puisqu'elles poussent les investisseurs à la méfiance. Fait particulièrement inquiétant : la brèche exploitée par Darkside est attribuable à un seul mot de passe compromis.

Au niveau international, ce type d'attaque peut aussi faire des vagues sur les marchés financiers

Quand des vies sont en jeu

D'autres attaques par rançongiciel sont d'autant plus inquiétantes qu'elles mettent des vies humaines en danger. Les 13 et 14 mai 2021, deux incidents de ce type ont visé le département de la Santé irlandais. En quelques heures, les systèmes informatiques du Health Service Executive (HSE), responsables de la gestion en ligne de plusieurs hôpitaux et cliniques externes du pays, ont été attaqués. Une rançon de 20 millions de dollars fut demandée pour restituer l'accès aux serveurs.

Dans un domaine d'opération aussi sensible, l'incident met des vies en danger.

Les conséquences de l'attaque se sont révélées majeures. De nombreux rendez-vous ont dû être annulés (jusqu'à 80% dans certaines régions), les employés du HSE ont été privés de l'usage de leurs courriels et ont dû s'en remettre à l'utilisation du papier uniquement. Plus de 500 patients ont par ailleurs vu leurs dossiers médicaux compromis par les pirates. Dans un domaine d'opération aussi sensible, l'incident met des vies en danger. Or, celui-ci serait dû au simple fait qu'un employé a ouvert un lien infecté depuis son poste de travail. L'attaque est attribuée au groupe criminel Wizard Spider, qui opérerait à partir de la Russie.

La géopolitique du rançongiciel

Ce dernier point a son importance. En effet, on observe que l'écrasante majorité des groupes de hackers utilisant ces techniques sont basés en Russie, et qu'une plus petite fraction provient de pays d'Europe de l'Est, ou encore de Corée du Nord, d'Iran ou de Chine. Autant d'États dans lesquels ces pirates ne semblent pas véritablement menacés par les autorités. Impotence du système judiciaire ou politique

assumée de la part de ces gouvernements ? La réponse demeure incertaine. Force est toutefois de constater qu'en Russie, en Iran ou en Corée du Nord, l'usage d'Internet est soumis à un contrôle relativement rigide, ce qui suggère que les groupes de hackers sont connus des autorités, mais tolérés tant qu'ils ne causent pas de tort à l'État hôte.

Impotence du système judiciaire ou politique assumée de la part de ces gouvernements ? La réponse demeure incertaine.

Un accord tacite ou explicite bien compris par les pirates : des spécialistes en cybersécurité ont par exemple découvert que le groupe cybercriminel REvil, basé en Russie, programme ses maliciels pour qu'ils ne s'attaquent pas à des ordinateurs dont le langage paramétré est le russe, l'ukrainien, le biélorusse, et plusieurs autres langues parlées dans les pays de l'ex-URSS. Il apparaît par ailleurs que ces groupes cybercriminels représentent un bassin de recrutement potentiel pour les services de renseignement de l'État hôte, et offrent occasionnellement de mettre leurs capacités cybernétiques au service de celui-ci, en effectuant par exemple des opérations d'espionnage en marge de leur cyberbanditisme. Il existe donc de subtiles, mais multiples imbrications entre géopolitique et cybercriminalité.

Des pistes de solution

Une chose est certaine : le Canada n'a pas fini d'entendre parler de rançongiciels. Selon un récent rapport du Centre de la sécurité des télécommunications (CST), il y aurait eu 235 cas répertoriés d'attaques par rançongiciel contre des entités canadiennes dans la dernière année (le total est toutefois vraisemblablement beaucoup plus élevé). Sans dévoiler toutes les cibles et l'étendue des dégâts, les experts du CST affirment cependant que des infrastructures critiques ont été touchées, notamment dans le domaine hospitalier, manufacturier et énergétique.

Les autorités déploient ainsi des efforts croissants pour tenter de répondre au problème. Sur le plan de la sensibilisation d'abord, le Centre canadien pour la cybersécurité a publié fin 2021 un « playbook », guide pratique visant à expliquer la cybercriminalité au public et à aider les entreprises de tout acabit à s'ajuster face à la menace croissante. Parallèlement, alors que la *Loi sur la sécurité de l'information* a été modifiée en 2019 pour donner plus de mordant à la politique de défense cybernétique, le Canada commence aussi à montrer les dents aux auteurs de rançongiciels : en décembre 2021, le CST a annoncé avoir mené, pour la première fois, des cyberattaques contre des groupes cybercriminels étrangers.

Un cas canadien : le piratage du Collège militaire royal de Kingston (2020)

Le Canada n'est pas épargné par les attaques par rançongiciel. En juillet 2020, le Collège militaire royal de Kingston a par exemple été victime d'un tel incident, qui a paralysé une partie des activités de l'établissement. Parmi les systèmes affectés figurait le réseau administratif qui gère les boîtes courriel, les communications entre étudiants et l'intranet réservé aux employés. Les plateformes en question furent temporairement mises hors service pour éviter des dégâts plus importants. Les systèmes informatiques du Collège n'étaient d'ailleurs pas encore tous opérationnels à la rentrée scolaire, fin août.

Le ministère de la Défense nationale (dont relève le Collège militaire) indiqua d'abord que l'incident était le fruit d'une « campagne massive d'hameçonnage[1] », et n'avait pas compromis d'informations classifiées, ajoutant que les données les plus susceptibles d'avoir été à risque étaient des travaux de recherche menés au sein de l'institution. Un mois après l'attaque, toutefois, on découvrit que des documents financiers et des données personnelles avaient aussi été compromis et publiés sur le Dark Web, notamment des relevés de notes ou encore des rapports de progression d'élèves-officiers, contenant noms et adresses.

L'obtention de ce type de renseignements permet généralement aux auteurs d'attaques par rançongiciel de personnaliser la demande de rançon en faisant, par exemple, mention de personnel employé à des postes précis. Cette tactique confère plus de crédibilité à la demande, accentue les craintes des utilisateurs, et maximise donc les chances que l'argent soit versé. Des observateurs extérieurs firent toutefois remarquer que, vu l'entité ciblée, de telles informations présentaient une sensibilité particulière : un État adverse pourrait par exemple mettre ces données à profit pour évaluer quels individus seraient à l'avenir appelés à gravir la hiérarchie de l'appareil de défense canadien, et cumuler de l'information personnelle sur ceux-ci.

Dans le cas du Collège militaire de Kingston, plus de peur que de mal a priori. L'attaque, que certains observateurs attribuent au groupe cybercriminel DoppelPaymer, semble à première vue ne pas avoir été commanditée par un État adverse. Certaines informations dérobées ont toutefois été mises en ligne sur le Dark Web. Il est donc difficile d'estimer qui peut y avoir eu accès et à quelles fins elles peuvent être utilisées à l'avenir. Le cas du Collège militaire royal de Kingston illustre toute l'ambiguïté des attaques par rançongiciel : si elles sont surtout et avant tout motivées par l'appât du gain, elles soulèvent également de multiples enjeux d'ordre géopolitique.

1 L'hameçonnage (ou « phishing » en anglais) est une méthode d'intrusion informatique consistant à envoyer, par exemple, des courriels frauduleux contenant des liens URL piégés qui, une fois ouverts, permettent aux hackers d'accéder à un appareil ou d'y installer un logiciel espion.

CONCLUSION
Ukraine, la grande inconnue

Le présent rapport a cherché à faire l'état des lieux des cyberincidents à caractère géopolitique touchant le Canada, ainsi qu'à présenter certaines tendances à surveiller à l'avenir autour de cet enjeu. À cet égard, le conflit qui a récemment débuté en Ukraine est porteur de bouleversements importants et pourrait bien ne pas rester sans conséquences pour le Canada sur le plan cyber. Alors que le gouvernement canadien s'est joint à différents efforts diplomatiques, économiques et militaires multinationaux ayant pour but de soutenir l'Ukraine et de sanctionner la Russie, le cyberespace représente un domaine de choix dans lequel l'État russe ou d'autres acteurs pourraient vouloir répondre à ces mesures.

Début mars 2022, une cyberattaque au rançongiciel contre l'aluminerie Alouette de Sept-Îles, revendiquée par le groupe cybercriminel russe Conti, a laissé craindre une première tentative de représailles aux sanctions canadiennes. Bien que Conti figure parmi les groupes de pirates ayant signifié leur volonté de soutenir l'État russe dans le cadre du conflit, il apparaît toutefois que la brèche informatique en question précédait l'invasion de l'Ukraine de plusieurs jours : cette tentative de cyberextorsion ne cachait donc pas de motivations idéologiques. Les mois à venir pourraient toutefois être le théâtre de cyberincidents au statut plus ambigu sur le plan géopolitique, voire carrément de cyberattaques revendiquant ouvertement un caractère punitif.

Bien que le Canada ne fasse pas pour l'instant figure de cible prioritaire, les scénarios potentiels sont nombreux. À minima, on peut envisager que Moscou encourage les réseaux cybercriminels russes à redoubler leurs cyberattaques – par rançongiciel notamment – contre des entités canadiennes, particulièrement celles ayant pris des mesures spécifiques à l'encontre de la Russie (des boycotts par exemple). Bien que les pays membres de l'OTAN s'efforcent actuellement de prévenir les risques d'escalade ou d'élargissement du conflit, on peut aussi concevoir que la Russie tente éventuellement de s'en prendre aux infrastructures critiques de membres de l'Alliance atlantique. À cet égard, les infrastructures électriques canadiennes, fortement intégrées au réseau américain, font donc figure de cible potentielle. En outre, alors que les États-Unis ont annoncé l'abolition de toutes leurs importations d'hydrocarbures provenant de Russie, on peut imaginer aussi que Moscou tente de nuire aux producteurs susceptibles de combler ce vide. Les pétrolières canadiennes, qui se proposent par exemple d'augmenter leurs livraisons à destination des États-Unis, pourraient faire également l'objet de cyberattaques.

Certes, la guerre en Ukraine n'a jusqu'ici pas vraiment été le théâtre de cyberattaques de grande ampleur. Pour autant, le caractère furtif et clandestin des moyens cyber demeure un atout important dans les antagonismes plus indirects qui entourent le conflit, et auxquels le Canada est, à bien des égards, partie prenante. Non négligeable, ce potentiel de perturbations s'ajoute donc aux tendances à surveiller dans un avenir proche.

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, soit 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 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 (autrement dit, 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).

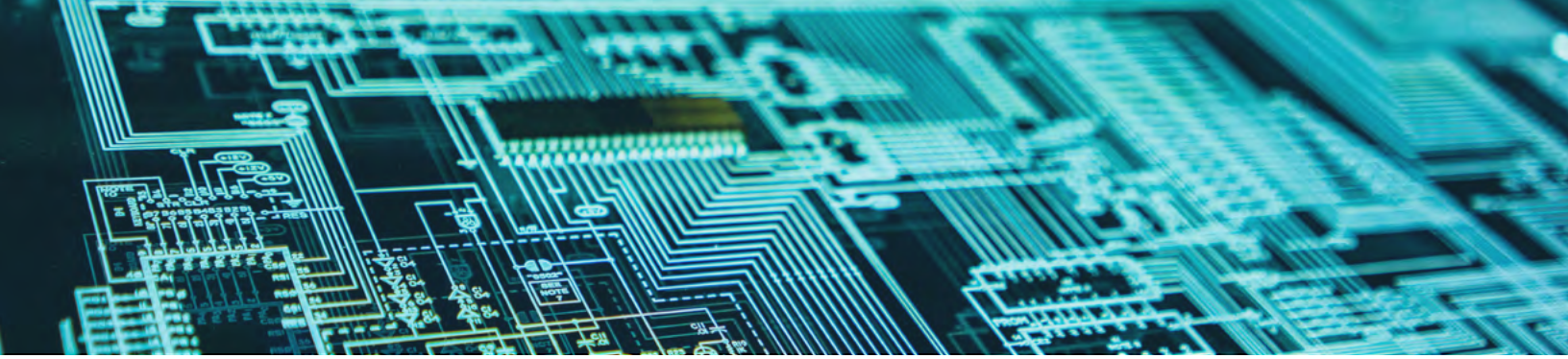
ATTEINTE À L'IDENTITÉ : Fait d'usurper, prendre le contrôle, ou modifier l'apparence de manière non autorisée d'un site web (*defacement*), d'un compte ou d'une page à des fins politiques hostiles.

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 ORIGINES DES INCIDENTS

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 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 les 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