UQÀM

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

CYBERINCIDENTS GÉOPOLITIQUES AU CANADA

État des lieux 2024

Proposé par l'Observatoire des conflits multidimensionnels

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 chercheur-e-s étudiant les transformations de la conflictualité internationale. Les cyberattaques, les manipulations de l'information, la géoéconomie, et les ingérences politiques ou électorales figurent parmi les principaux 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 cyber-conflictualité, 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, la cyberdéfense et les opérations d'influence. Il est l'auteur de plusieurs publications académiques en français et en anglais portant sur la politique internationale 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. Alexis Rapin est également membre du comité éditorial du Rubicon, une plateforme francophone d'analyse des questions internationales.

Danny Gagné est candidat au doctorat en science politique à l'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 et coordonnatrice à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand. Étudiante à la maîtrise en science politique à l'UQAM, détentrice d'un baccalauréat en médias numériques (UQAM) et d'un certificat en design de jeux vidéo (UQAT), elle écrit régulièrement sur la technologie dans les médias en tant que journaliste indépendante. Elle est collaboratrice techno à l'émission *Moteur de recherche* (ICI Première) et membre du collectif de protection de la vie privée le Lab 2038.

QUELQUES INCIDENTS MARQUANTS

2023

février

ATTAQUE PAR RANÇONGICIEL CONTRE BLACK & MCDONALD

La multinationale canadienne d'ingénierie Black & McDonald est visée par une attaque par rançongiciel. Black & McDonald maintient plusieurs contrats avec le ministère de la Défense nationale dans le secteur de la gestion d'installations militaires et des services de soutien logistique. Alors que des données stratégiquement sensibles pourraient avoir été compromises par la cyberattaque, le ministère de la Défense indique que ses systèmes n'ont pas été affectés.

mai

RÉVÉLATIONS DE CAMPAGNES D'INFLUENCE CHINOISES CONTRE TROIS POLITICIEN-NE-S

Plusieurs médias révèlent que trois élu-e-s canadiens ont été la cible de campagnes d'influence chinoises, comprenant des opérations informationnelles en ligne. L'ex-député conservateur Kenny Chiu, la parlementaire du NPD Jenny Kwan ainsi que l'ex-chef du Parti conservateur Erin O'Toole auraient entre autres été visés par des efforts de manipulation de l'information sur le média social WeChat. Ces opérations auraient visé à interférer dans les élections fédérales de 2019 et 2021.

août

CAMPAGNE D'INFLUENCE CHINOISE « SPAMOUFLAGE » CONTRE LA CLASSE POLITIQUE CANADIENNE

Plusieurs dizaines de politicien-ne-s canadiens sont la cible d'une campagne d'influence orchestrée par l'État chinois sur les plateformes Facebook et X. L'opération repose notamment sur l'utilisation de vidéos hypertruquées (*deepfakes*) qui semblent présenter un blogueur sino-canadien critique de Pékin et dans lesquelles celui-ci calomnie les élu-e-s visés. Par la suite, un réseau de faux comptes de médias sociaux automatisés (*bots*) était utilisé pour amplifier la visibilité des vidéos truquées.

novembre

COMPROMISSION DE CYBERLINK PAR LA CORÉE DU NORD

Microsoft révèle une cyberattaque nord-coréenne ayant visé certains utilisateurs de CyberLink, un logiciel d'édition photo et vidéo. Les pirates auraient piégé l'outil d'installation de CyberLink, leur permettant ainsi d'accéder frauduleusement aux données des machines ayant installé le logiciel compromis et de les exfiltrer. Plus d'une centaine d'organisations auraient été visées, notamment au Japon, à Taïwan, au Canada et aux États-Unis.

avril

RÉVÉLATIONS D'INTRUSIONS RUSSES DANS DES SYSTÈMES DE GAZODUC

Une fuite d'information survenue aux États-Unis suggère que des pirates pro-russes se seraient introduits dans les infrastructures informatiques d'un opérateur de gazoduc canadien. Collaborant avec les services de renseignement russes, les pirates auraient affirmé avoir compromis les systèmes de commande du gazoduc, dans l'intention de pouvoir causer un accident industriel. Les revendications des pirates sont toutefois mises en doute par de nombreux observateurs du secteur.

juillet

OPÉRATION D'APT 29 CONTRE DES AMBASSADES

Une campagne de cyberespionnage est attribuée au groupe de pirates APT 29, affilié au Service de renseignement extérieur de Russie. Une opération en particulier a cherché à hameçonner des diplomates basés à Kyiv, en Ukraine, par l'entremise d'une annonce de vente de voiture frauduleuse. Visant l'installation d'un logiciel malveillant, cette opération aurait ciblé le personnel diplomatique de 22 pays, dont le Canada.

septembre

ATTAQUE PAR DÉNI DE SERVICE CONTRE L'AGENCE DES SERVICES FRONTALIERS

Une vingtaine de sites gouvernementaux canadiens sont visés par des attaques par déni de service, initiées par le groupe de hacktivistes pro-russes NoName057 (16). L'opération touche notamment l'Agence des services frontaliers et provoque une panne informatique dans plusieurs aéroports canadiens. Les bornes d'enregistrement électronique des services d'immigration sont rendues temporairement indisponibles, ralentissant le traitement des arrivées. Les pirates disent vouloir s'opposer à l'aide militaire canadienne à l'Ukraine.

décembre

FAUX REPORTAGE VIDÉO DIFFUSÉ PAR L'IRAN

Une opération d'influence iranienne prend pour cible des services de diffusion télévisuelle en ligne (*streaming television services*), qui sont piratés pour diffuser une vidéo critiquant l'intervention militaire israélienne à Gaza. Se présentant frauduleusement comme un reportage télévisé, la séquence a en fait été créée par un outil d'intelligence artificielle (IA) générative. L'opération aurait touché des audiences aux Émirats arabes unis, au Royaume-Uni et au Canada.

Le Canada et les cyberincidents géopolitiques à l'horizon 2024

Dans un monde où les tensions géopolitiques apparaissent en nette recrudescence, le Canada peut sembler relativement épargné par les évènements ayant agité la scène internationale au fil de 2023. Pour autant, qu'il s'agisse de la poursuite du conflit en Ukraine ou de l'intervention militaire israélienne à Gaza, le cyberespace se révèle désormais un canal par lequel la conflictualité globale ressurgit de plus en plus sur le quotidien des Canadiennes et Canadiens. Entre vols de données, attaques par déni de service ou opérations d'influence, plusieurs cyberincidents récents montrent que la distance et les océans ne constituent plus tout à fait les remparts géopolitiques que le Canada a longtemps tenus pour acquis.

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 ci-dessous). La présente analyse se concentre sur les cyberincidents présentant un caractère géopolitique ou stratégique, le plus souvent orchestrés par des États-nations.

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, d'incidents ayant touché une diversité de pays (incluant le Canada). Les incidents recensés par notre équipe remontent jusqu'à 2010.

À ce titre, l'analyse réalisée dans le cadre de ce rapport (sans prétendre à l'exhaustivité) a recensé **pas moins de 16 cyberincidents à caractère géopolitique en 2023** au Canada, soit le plus haut total annuel parmi l'ensemble de nos données. Or, celles-ci ne proviennent que de sources ouvertes et ne reflètent donc probablement qu'une fraction seulement des activités numériques malveillantes ayant cours au pays. Au total, le répertoire des cyberincidents canadiens de la Chaire Raoul-Dandurand, dont les données du présent rapport sont issues, dénombre aujourd'hui **114 cyberincidents géopolitiques ayant touché le Canada depuis 2010**. Que sait-on de ces incidents, de leur nature, de leurs cibles ou encore de leur origine ? La présente section entend proposer un aperçu global des données recueillies par notre équipe.

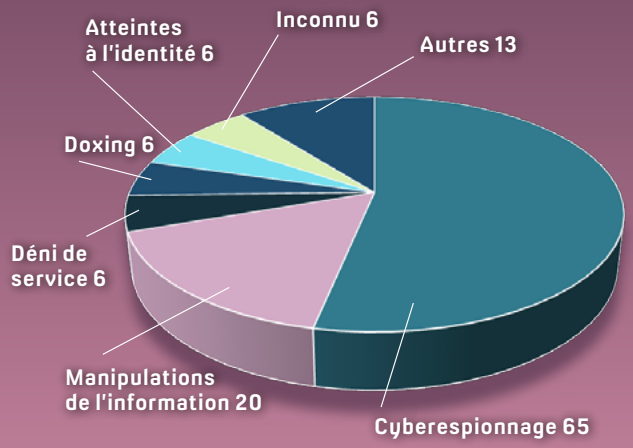
Quels types de cyberincidents sont les plus fréquents ?

La très grande majorité des cyberincidents à caractère géopolitique touchant le Canada continue de relever de cyberespionnage, tels le vol de propriété intellectuelle et de secrets d'État, ou encore la surveillance clandestine d'individus. Sur les 114 incidents répertoriés depuis 2010, pas moins de 65 relèvent de cyberespionnage (soit 57%). Les actes de manipulation de l'information (soit la diffusion intentionnelle, massive et coordonnée de nouvelles fausses ou biaisées à des fins

politiques) représentent le deuxième type de cyberincidents les plus fréquents, au nombre de 20 depuis 2010 (soit 17,5%). Sans surprise, ces deux catégories sont aussi les plus prévalentes pour l'année 2023.

Fait intéressant, la répartition des types d'incidents observée en 2023 consacre néanmoins une recrudescence notable des attaques par déni de service (DDoS). Ce type d'action malveillante, très prisé dans les années 2000, puis tombé en désuétude dans les années 2010, connaît un regain important à travers le monde du fait de la mobilisation de groupes d'hacktivistes s'étant constitués en réaction aux conflits en Ukraine ou à Gaza (voir section 1). Au Canada, **quatre cyberincidents géopolitiques de ce type ont été observés en 2023, alors qu'on en recensait seulement deux sur toute la période 2010-2022.** Cette évolution ne doit pas faire oublier que tous les cyberincidents ne se valent pas : les attaques par déni de service se font plus fréquentes, mais s'avèrent relativement inoffensives, là où d'autres types d'incidents restent rares, mais présentent des implications plus sérieuses (voir section 3).

Types de cyberincidents les plus fréquents (depuis 2010)



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

Quelles sont les cibles connues ?

Il n'est pas toujours aisé, sur la base de sources ouvertes, d'établir l'identité ou la nature des entités visées par des cyberincidents. La vaste campagne de cyberespionnage chinoise ayant exploité le logiciel Barracuda, révélée à l'été 2023, en fournit un bon exemple : le Canada semble avoir constitué la deuxième cible la plus importante de cette opération (derrière les États-Unis), sans que soit divulgué le nombre précis ou la nature des entités canadiennes touchées. Pour autant, d'autres cyberincidents survenus en 2023 donnent une idée plus précise de leurs impacts et des victimes.

C'est notamment le cas des vagues d'attaques par déni de service, dont les responsables cherchent souvent à faire sensation et publicisent eux-mêmes la liste des cibles. À ce chapitre, on peut observer que **les sites web de près d'une vingtaine d'organisations gouvernementales fédérales ou provinciales ont été visés par ce genre d'attaque en 2023**, dont certains à plusieurs reprises (à l'instar du Sénat ou du Cabinet du premier ministre). Plusieurs grandes entreprises canadiennes ont également été ciblées, comme Hydro-Québec, le Canadien Pacifique, la Banque TD ou encore Husky Energy. Notons cependant que l'impact des attaques sur l'accès aux sites web visés a grandement varié d'une cible à l'autre et a généralement été insignifiant.

Deux autres incidents plus sérieux ont quant à eux ciblé des firmes contractantes du secteur de la défense, Black & McDonald et Brookfield Global Relocation Services, vraisemblablement via des rançongiciels. Ces attaques, a priori de nature criminelle, ont été incluses dans cette analyse du fait de la potentielle sensibilité stratégique des données compromises — les deux firmes ayant notamment des contrats avec la Défense canadienne (voir page 21). À l'été 2023, une opération de cyberespionnage attribuée à des pirates du renseignement russe a pour sa part visé du personnel diplomatique

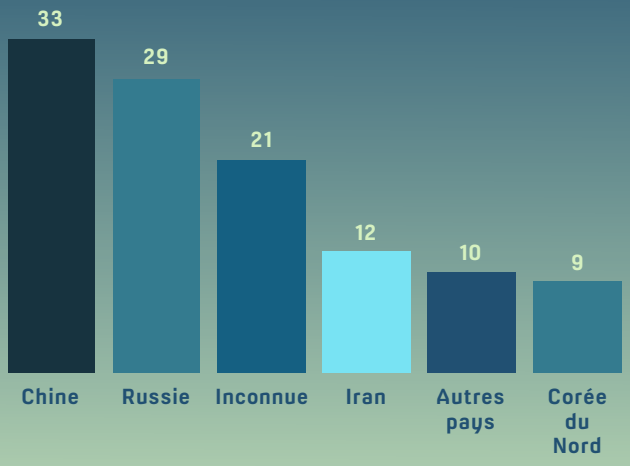
canadien stationné en Ukraine (en plus de celui d'une vingtaine d'autres pays).

D'où proviennent la plupart de ces attaques ?

Quatre pays sont à l'origine de la grande majorité des cyberincidents géopolitiques canadiens recensés dans le cadre de cette analyse : la Chine (33 incidents sur 114), la Russie (29), l'Iran (12) et la Corée du Nord (9). Ces données concernent l'origine *géographique* des cyberincidents ayant touché le Canada ; elles n'impliquent pas nécessairement une responsabilité avérée des gouvernements des pays mentionnés (pour plus de détails, voir la rubrique méthodologique). Par ailleurs, en raison de l'absence de données probantes publiées en la matière, il apparaît que 21 des incidents recensés depuis 2010 n'ont pour le moment pas d'origine connue.

Les incidents répertoriés durant l'année 2023 reflètent assez fidèlement cette répartition globale, avec 6 incidents provenant de Russie, 4 de Chine et 3 incidents provenant respectivement d'Iran, de Corée du Nord et d'Inde. Il importe de souligner que depuis 2022 l'essor de groupes hacktivistes et cybercriminels basés en Russie vient conférer un poids grandissant à ce pays dans les données. Le caractère particulièrement visible de ce genre d'acteurs pourrait induire un biais de représentativité vis-à-vis d'autres États étudiés ici.

Origine géographique des cyberincidents (depuis 2010)



Source : Répertoire des cyberincidents canadiens

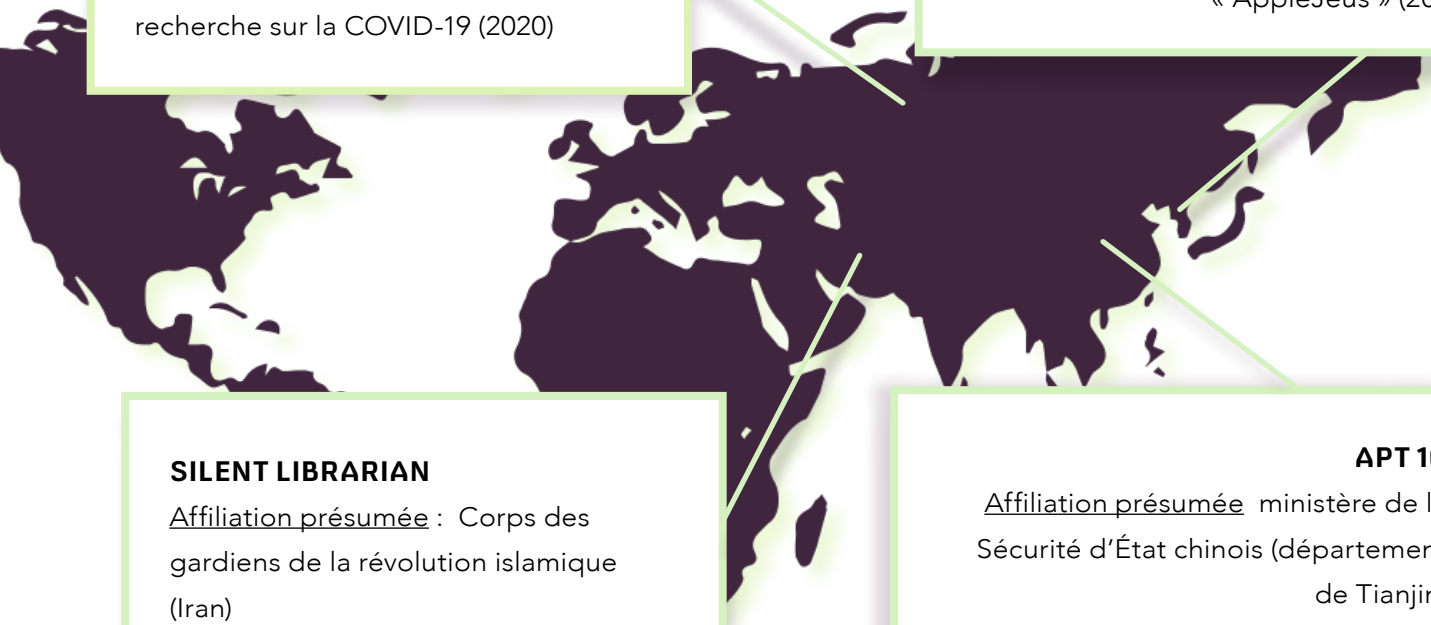
Quels groupes de pirates ont visé le Canada en 2023 ?

Plusieurs cyberincidents ayant touché le Canada en 2023 ont été attribués à des groupes de pirates informatiques déjà bien connus de la communauté de cybersécurité. C'est par exemple le cas du groupe APT 29 (ou Cozy Bear), rattaché au service de renseignement extérieur de la Fédération de Russie, qui serait responsable du piratage ayant visé l'ambassade canadienne en Ukraine à l'été 2023. Cette attribution paraît cohérente, APT 29 s'étant illustré depuis 2022 par d'importants efforts de cyberespionnage contre les diplomaties occidentales. Un autre incident ayant touché le Canada en 2023, la compromission du logiciel CyberLink, est quant à lui attribué au Lazarus Group, un acteur affilié à la Corée du Nord et actif depuis 2009 au moins. Au cours des dernières années, Lazarus s'est notamment fait connaître pour ses opérations de vol de cryptomonnaies, dont l'une a d'ailleurs touché le Canada en février 2021. On peut d'ailleurs noter qu'APT 29 et Lazarus Group figuraient déjà parmi les groupes de pirates ayant visé le plus fréquemment le Canada depuis 2010 (voir plus bas).

Un autre acteur, nouveau venu, a beaucoup fait parler de lui au Canada en 2023 : NoName057(16). Ce groupe hacktiviste pro-russe s'est constitué dans la foulée de l'invasion de l'Ukraine de 2022 et est désormais l'un des principaux responsables d'attaques par déni de service visant les pays alliés de Kyiv. C'est à NoName057 (16) que l'on doit deux des quatre incidents de ce genre ayant touché le Canada l'année dernière. Comme la plupart des collectifs hacktivistes, NoName057 (16) présente un faible degré de sophistication, mais impressionne par son assiduité en maintenant depuis plus d'un an un rythme d'attaques soutenu (parfois jusqu'à 15 par jour). Bien que l'indépendance de certains « hackers patriotiques » russophones soit parfois remise en question, aucun indice ne suggère jusqu'ici un lien entre NoName057 (16) et l'appareil gouvernemental russe.

Quelques groupes de pirates étatiques très actifs contre le Canada

Certains groupes de pirates informatiques étatiques sont bien connus de la communauté de la cybersécurité. Sur la base des efforts d'attribution déployés par les firmes du secteur ou par les pouvoirs publics, on peut observer que quelques groupes de pirates affiliés à des États ont été particulièrement actifs au Canada (ou à l'encontre d'acteurs canadiens) dans les dernières années.



APT 29 (COZY BEAR)

Affiliation présumée : Service des renseignements extérieurs de la Fédération de Russie (SVR)
Actif depuis : 2008 au moins
Opérations récentes au Canada : campagnes contre des ambassades (2023), compromission de Solar Winds (2020), cyberespionnage de la recherche sur la COVID-19 (2020)

LAZARUS GROUP

Affiliation présumée : Bureau général de reconnaissance (Armée populaire de Corée)
Actif depuis : 2009 au moins
Opérations récentes au Canada : compromission de CyberLink (2023), espionnage d'entreprises énergétiques (2022), vol de cryptomonnaies « AppleJeus » (2021)

SILENT LIBRARIAN

Affiliation présumée : Corps des gardiens de la révolution islamique (Iran)
Actif depuis : 2013 au moins
Opérations récentes au Canada : trois campagnes d'espionnage contre des universités (2020, 2019, 2018)

APT 10

Affiliation présumée ministère de la Sécurité d'État chinois (département de Tianjin)
Actif depuis : 2006 au moins
Opérations récentes au Canada : opération Cloud Hopper (2018), brèche d'Equifax (2017)

Groupes hacktivistes et attaques par déni de service distribué : de l'inoffensif au nuisible ?

2023 représente une année record en termes d'attaques par déni de service distribué perpétrées par des groupes hacktivistes contre le Canada. Quatre grands épisodes de ce genre ont en effet ciblé les secteurs privé et public du pays l'année dernière [1] [2] [3] [4], touchant au total une cinquantaine d'entités canadiennes. Déployées par des acteurs politiquement motivés, ces attaques ont fait œuvre de représailles contre des décisions ou des annonces du gouvernement fédéral, le plus souvent avec des ramifications internationales. L'augmentation de l'activité de ces groupes, directement liée aux tensions géopolitiques et conflits actuels, a d'ailleurs été observée à l'échelle globale par plusieurs firmes de cybersécurité [1] [2].

Contrairement au cyberespionnage ou aux attaques destructrices perpétrées par des groupes plus sophistiqués, les attaques de type déni de service distribué (DDoS) commises par les groupes hacktivistes n'ont généralement pas d'impact important. Dans la grande majorité des cas, les sites web visés, dont les serveurs sont inondés d'un torrent de requêtes artificielles, sont ralentis ou rendus indisponibles pendant quelques heures, voire quelques minutes seulement. Toutefois, la sophistication grandissante des groupes hacktivistes et l'intensification des dommages causés par leurs attaques ont de quoi inquiéter.

L'HACKTIVISME PRO-RUSSE EN HAUSSE

L'invasion russe de l'Ukraine en février 2022 a entraîné une recrudescence des activités malveillantes de la part de groupes de pirates pro-russes ciblant l'Ukraine et les pays de l'OTAN. Parmi les groupes hacktivistes pro-russes les plus actifs en 2023 figure NoName057 (16), qui a mené deux grandes campagnes d'attaques par déni de service contre le Canada en 2023 en s'attaquant à des sites web d'organisations publiques et privées, comme le site web du premier ministre Justin Trudeau et celui d'Hydro-Québec. Sur le service de messagerie chiffrée Telegram, le groupe a indiqué agir en représailles au soutien militaire et politique du gouvernement canadien envers l'Ukraine. Sa première vague d'attaques visant le Canada au printemps 2023 faisait d'ailleurs suite à la visite du premier ministre ukrainien en sol canadien et à l'annonce d'une nouvelle livraison d'armement à l'Ukraine par Ottawa.

Dans la première moitié de l'année 2023, NoName057 (16) aurait ainsi mené plus d'un millier d'attaques par déni de service distribué contre diverses entités basées en grande majorité en Europe et en Amérique du Nord. La plupart des cyberattaques du groupe auraient été perpétrées à l'aide de son outil DDosia, qui encourage la participation

de « bénévoles » en échange d'une rémunération versée en cryptomonnaies pouvant atteindre jusqu'à 1200 dollars américains en cas d'attaque réussie. Cette incitation pécuniaire permet non seulement au groupe d'augmenter sa force de frappe, son taux de réussite et sa popularité, mais elle brouille également les frontières entre les motivations politiques et celles financières des internautes menant de telles attaques.

La sollicitation de masse des internautes montre la facilité avec laquelle sont perpétrées les attaques par déni de service distribué, qui nécessitent peu de compétences techniques de la part de leurs auteur-e-s. La popularité du canal Telegram associé au projet DDosia, qui comptait en janvier 2023 plus d'un millier d'abonné-e-s, témoigne d'une organisation encore plus efficace dans le déploiement de ces attaques généralement bénignes. L'automatisation grandissante de ce type d'attaques, ainsi que le spectre de l'usage de l'intelligence artificielle pour les rendre encore plus performantes, tend à indiquer que les attaques DDoS en tant qu'outil de revendication politique ont encore de beaux jours devant elles.

> « La sollicitation de masse des internautes montre la facilité avec laquelle sont perpétrées les attaques par déni de service distribué, qui nécessitent peu de compétences techniques de la part de leurs auteur-e-s. »

DES ATTAQUES PLUS DESTRUCTRICES À L'AVENIR ?

La dernière vague de cyberattaques par déni de service distribué de NoName057 (16) visant le Canada à l'automne dernier a surpris par l'intensité de ses perturbations, plus importantes qu'escomptées. En effet, le groupe hacktiviste a ciblé l'Agence des services frontaliers, provoquant des pannes informatiques dans plusieurs aéroports du pays. Le flot de requêtes induit par l'attaque a généré des problèmes de connectivité intermittents avec les bornes d'enregistrement numériques et les portiques électroniques déployés par les services frontaliers dans les terminaux aériens. Bien qu'aucune information sensible n'ait été exfiltrée ou compromise lors de cette attaque — le but général des attaques par DDoS étant de causer des perturbations et non pas de voler des informations personnelles ou sensibles —, celle-ci est néanmoins venue ralentir pendant plus d'une heure le traitement des arrivées dans les postes de contrôle frontalier de plusieurs aéroports canadiens. Il s'agit de conséquences très rares pour une attaque de ce type, estiment différents spécialistes, qui s'inquiètent du fait qu'un procédé généralement bénin ait en l'occurrence pu causer des dommages aussi importants.

Ailleurs dans le monde, la force de frappe des attaques de groupes hacktivistes s'est vue multipliée via des attaques plus sophistiquées. À titre d'exemple, le groupe pro-russe From Russia with Love a déployé le rançongiciel Somnia contre plusieurs organisations ukrainiennes. Dans le camp opposé, le groupe pro-Ukraine Team OneFist a revendiqué une attaque destructrice sur le système de télégestion à grande échelle (SCADA) d'un

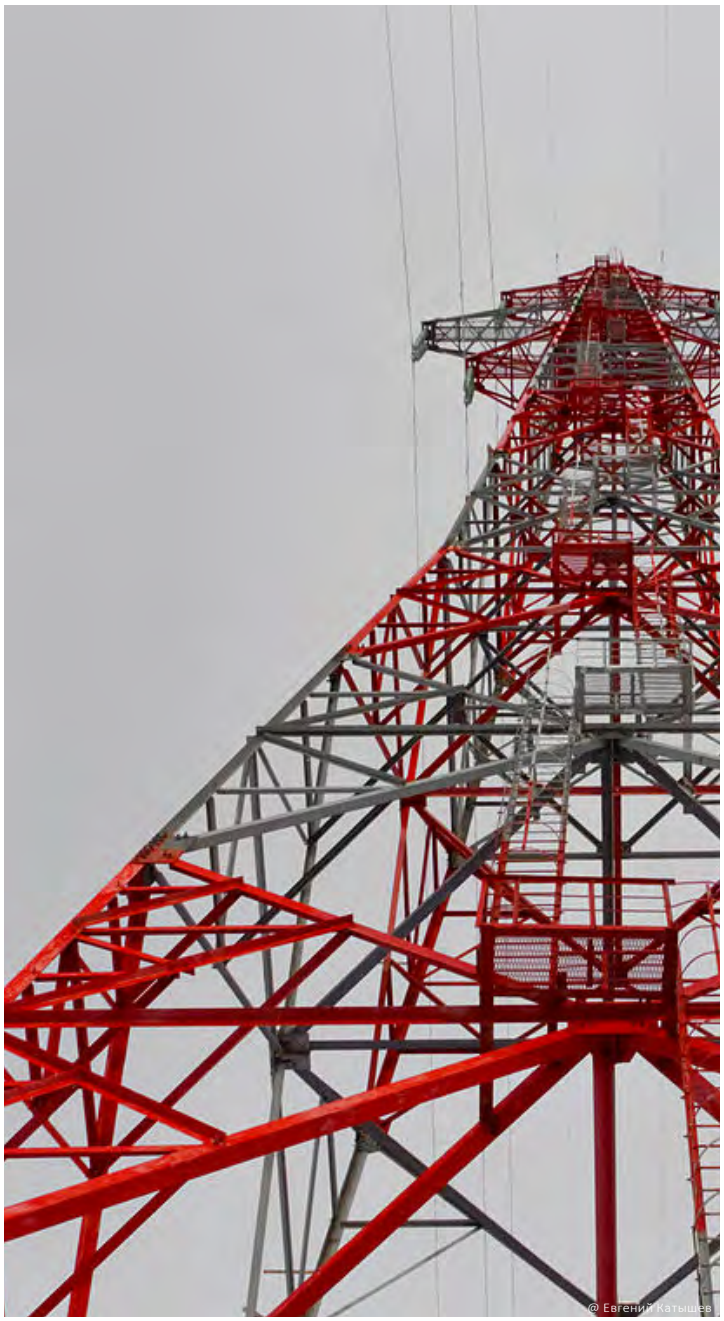
réseau électrique russe. Cette affirmation doit toutefois être prise avec un grain de sel : effectivement endommagé, le système SCADA aurait plutôt été mis hors service par un incendie ayant touché une centrale électrique connexe, et non pas par une cyberattaque.

Cet évènement rappelle que l'usage de revendications opportunistes demeure une stratégie importante pour les hacktivistes en quête de visibilité et de notoriété. Alors que la communication des groupes hacktivistes tend souvent à exagérer l'ampleur réelle de leurs offensives, elle contribue à attirer l'attention sur des cyberattaques qui seraient autrement peut-être passées inaperçues. En instillant ainsi un sentiment de peur et d'incertitude parmi la population des pays ciblés, les groupes hacktivistes produisent en définitive des effets bien plus psychologiques que technologiques.

EN PHASE DE MATURATION

Le pouvoir de nuisance grandissant des groupes hacktivistes depuis le début de l'invasion russe en Ukraine permet aussi de faire la lumière sur le potentiel de filiation entre des États et des groupes de hackers de prime abord indépendants. En effet, des groupes menant des activités perturbatrices contre des pays alliés à l'Ukraine, tels que Xaknet ou CyberBerkut, sont soupçonnés depuis des années de servir de façade au service de renseignement militaire russe (GRU). Pour certains hauts responsables de l'appareil de cybersécurité ukrainien, la grande majorité des groupes hacktivistes pro-russes agirait en vérité sous les ordres de Moscou. Bien qu'il soit souvent impossible de prouver hors de tout doute le degré de proximité entre le gouvernement russe et les groupes hacktivistes indépendants, des chercheur-e-s-occidentaux soulignent que l'établissement de relations avec ceux-ci présenterait plusieurs bénéfices pour le régime russe.

Si des groupes comme NoName057 (16) semblent toujours agir de manière indépendante, ils apparaissent de plus en plus organisés et sophistiqués, s'inspirant des campagnes menées par les groupes de pirates informatiques commandités par les États. Bien que le Canada demeure somme toute rarement ciblé par des groupes pro-russes comparativement à plusieurs pays d'Europe (notamment orientale), et malgré les revendications parfois exagérées des groupes hacktivistes, on observe que ceux-ci sont en phase de maturation. Cette dernière, qui se traduit par l'amélioration des structures, des capacités et des outils des groupes hacktivistes, fait craindre une intensification de leurs activités malveillantes à l'avenir.



L'attaque par déni de service distribué du groupe Indian Cyber Force

(septembre 2023)

Le 18 septembre 2023, le premier ministre Justin Trudeau annonce que les services de renseignement canadiens se penchent sur des « accusations crédibles » selon lesquelles le gouvernement indien aurait été directement impliqué dans l'assassinat d'un citoyen canadien, le militant sikh Hardeep Singh Nijjar, tué en juin 2023 à Vancouver. Dans la foulée des accusations, un diplomate indien est également expulsé du pays.

Moins d'une semaine plus tard, le 22 septembre, une vague d'attaques par déni de service distribué cible plusieurs sites web canadiens, dont ceux de la Chambre des communes et des Forces armées canadiennes, rendus indisponibles pendant une à deux heures. Ces attaques, ainsi qu'une poignée d'autres n'ayant pu être confirmées, sont revendiquées par un groupe hacktiviste se faisant appeler Indian Cyber Force.

Sur Telegram et sur X (anciennement Twitter), le nébuleux collectif indique agir en représailles contre « les allégations et les politiques anti-indiennes » du gouvernement Trudeau, des actions qui auraient « dépassé les limites », aux yeux des pirates. Le groupe aurait proféré des menaces sur X contre le gouvernement canadien la semaine précédant les cyberattaques, lui demandant de se préparer à subir l'ire des attaquants à cause du « désordre » que le Canada aurait causé.

Si plusieurs attaques par déni de service de la part de groupes pro-russes ont été observées dans les mois précédents, l'incident consacre le premier cas publiquement documenté d'attaque par déni de service distribué de la part d'un groupe pro-Inde contre le Canada. Cependant, l'Indian Cyber Force avait fait les manchettes quelques mois plus tôt en perpétrant des attaques similaires contre un site web du gouvernement du Qatar en réponse à la condamnation à mort de huit anciens officiers militaires indiens dans une affaire d'espionnage. Le groupe a aussi revendiqué de multiples cyberattaques contre des sites web affiliés au Hamas ou des sites gouvernementaux chinois et bangladais au courant de l'année, bien que ces actions n'aient pas été confirmées.

Cet épisode montre que le Canada n'est pas à l'abri des cyberattaques à motivation politique menées par des acteurs émergents. Loin de passer inaperçues, les déclarations des autorités canadiennes peuvent être contestées et sanctionnées en quelques heures par de nébuleux acteurs en ligne situés aux quatre coins du globe. Bien que peu destructrice au Canada, la multiplication des offensives hacktivistes — et l'arrivée de nouveaux joueurs dans ce domaine — met en évidence le potentiel de nuisance que ces acteurs font peser sur le cyberespace canadien.

Influence numérique : la Chine fait sentir sa présence

Comme bon nombre de pays, le Canada est loin d'être épargné par les campagnes de désinformation et d'influence. Dans les dernières années, Ottawa a dû composer avec son lot d'opérations du genre, notamment en lien avec la guerre en Ukraine, l'exploitation de terres rares, ou encore l'origine de la COVID-19. Or, l'année 2023 a exposé le Canada à un type d'actions malveillantes auquel il était jusqu'ici moins habitué : l'ingérence électorale. Au gré de fuites dans les médias et de communiqués officiels, divers éléments suggèrent désormais que le processus démocratique canadien est, depuis 2019 au moins, lui aussi une cible de tentatives d'influence extérieure, en l'occurrence de la Chine.

Qu'il s'agisse de dissémination d'informations erronées ou de financements politiques douteux, les périodes électorales représentent évidemment des moments opportuns pour des acteurs cherchant à orienter le débat public ou le processus politique d'un autre pays. S'il n'est pas véritablement nouveau, le phénomène de l'ingérence électorale évolue néanmoins dans ses formes et ses méthodes. À ce titre, les révélations ayant secoué le Canada en 2023 ont permis d'observer un usage d'outils numériques toujours plus pointus en la matière, qui livre probablement un avant-goût de l'avenir des opérations d'influence.

LE NUMÉRIQUE MOBILISÉ

C'est en novembre 2022 que débute la controverse entourant l'ingérence chinoise dans les élections canadiennes. Une série de révélations médiatiques expose un réseau de donations entretenant des liens avec le Parti communiste chinois, qui aurait appuyé financièrement des candidatures du Parti libéral dans les élections de 2019 et 2021, vraisemblablement dans le but de nuire à des figures conservatrices critiques de Pékin. Parmi les personnes au cœur de la polémique figure le député ontarien Han Dong, qui aurait reçu l'aide du consulat chinois de Toronto lors de sa campagne de 2019.

La dimension numérique entre véritablement dans l'équation en mai 2023, lorsqu'il est révélé que l'ex-député conservateur Kenny Chiu, la députée néodémocrate Jenny Kwan et l'ex-chef du Parti conservateur Erin O'Toole ont fait l'objet de campagnes d'influence en ligne chinoises. Selon le Service canadien du renseignement de sécurité (SCRS), ils auraient entre autres été ciblés par des contenus fallacieux, disséminés de manière coordonnée sur le média social WeChat, très prisé par la diaspora chinoise au Canada. Des soupçons similaires avaient déjà été exprimés par des chercheur-e-s fin 2021 sans toutefois qu'un lien formel avec l'État chinois ne puisse être démontré.

Deux mois plus tard, on découvre que ce genre d'activités numériques malveillantes se poursuit : le Mécanisme de réponse rapide (MMR) d'Affaires mondiales Canada révèle une campagne d'influence chinoise ayant visé le député conservateur Michael Chong en mai 2023, à nouveau sur WeChat. Jamais deux sans trois, une autre opération d'influence chinoise en ligne est révélée en août, touchant cette fois plusieurs dizaines d'élu-e-s canadiens, dont le premier ministre, Justin Trudeau, et le chef du Parti conservateur, Pierre Poilièvre. Celle-ci met à contribution un outil jusqu'alors jamais observé de la sorte au Canada : un hypertrucage, vidéo frauduleuse générée par l'IA, déployée entre autres pour calomnier les politicien-ne-s en question (voir encadré).

DISSÉMINATION INAUTHENTIQUE ET COORDONNÉE

Ces opérations de nature numérique viennent donc s'ajouter aux manœuvres plus « traditionnelles » révélées en premier lieu à la fin 2022. Celles-ci incluent en partie des techniques de manipulation de l'information bien connues, basées sur la dissémination inauthentique et coordonnée de contenus. Par inauthentique, on entend l'utilisation de pages, de profils ou de personnalités numériques masquant ou déguisant l'identité véritable de l'émetteur d'un message. Dans le cas des campagnes contre Kenny Chiu, Jenny Kwan, Erin O'Toole et Michael Chong, on parle notamment de la création de faux profils utilisés pour diffuser et repartager massivement les publications en question. L'aspect coordonné renvoie quant à lui à un fort degré de synchronisation et d'automatisation dans la fabrication de contenus fallacieux, impliquant vraisemblablement l'utilisation d'automates (ou *bots*). En effet, on observe souvent une publication massive de messages similaires à un intervalle fréquent et précis, par exemple, à la première minute de chaque heure.

> **\\ Les périodes électorales représentent évidemment des moments opportuns pour des acteurs cherchant à orienter le débat public ou le processus politique d'un autre pays. **

Utilisées depuis plusieurs années maintenant, ces méthodes sont graduellement devenues plus faciles à repérer, comme en attestent les révélations publiques effectuées par les autorités canadiennes au fil de 2023. Néanmoins, entre désormais en jeu l'intelligence artificielle, qui permet de brouiller les pistes plus facilement. En effet, l'IA permet par exemple de créer de faux profils faisant appel à des « robots conversationnels » qui sont capables de converser avec un groupe d'utilisateurs ciblés. Ces nouveaux outils rendent la détection d'activités frauduleuses plus complexe et les campagnes d'influence plus insidieuses, car ils permettent entre autres d'entretenir des conversations exhaustives avec l'auditoire visé. L'usage, en août 2023, de l'hypertrucage visant à dénigrer de nombreux politicien-ne-s canadiens livre un autre exemple des périls informationnels que laissent entrevoir les progrès de l'IA.

ALIGNEMENT D'INTÉRÊTS

Que nous révèlent ces opérations quant aux objectifs poursuivis par la Chine? Il importe de souligner que dans certains des cas discutés, les autorités canadiennes n'ont pas formellement mis en cause l'État chinois. Reste qu'on observe un alignement d'intérêts manifeste entre les cibles de ces opérations d'influence et les priorités géopolitiques de Pékin. Dans le cas de Michael Chong, celui-ci avait parrainé avec succès, en 2021, une motion parlementaire désignant le traitement des Ouïghours par la Chine comme un génocide. De son côté, Kenny Chiu s'était montré très critique de Pékin au sujet de la répression des manifestations hongkongaises de 2019. La néo-démocrate Jenny Kwan, quant à elle, était à l'origine d'une pétition visant à créer un registre des acteurs suspectés d'ingérence au Canada. Erin O'Toole s'est par le passé distingué par ses positions très dures à l'encontre de la Chine, aussi bien dans le dossier Huawei que durant la pandémie de COVID-19.

En vue de faire la lumière sur ces campagnes d'influence, Ottawa a finalement mis sur pied en septembre 2023 une commission d'enquête publique sur la question, présidée par la juge Marie-Josée Hogue. Bien que celle-ci se penche également sur les soupçons d'ingérence impliquant d'autres États, la Chine se sait particulièrement visée et a déjà prévenu que le Canada devrait « en subir les conséquences ». Pour l'heure, un premier rapport intérimaire doit être rendu public par la commission le 3 mai 2024 : c'est alors que l'on saura si le Canada passe des soupçons aux accusations.

La campagne d'influence de « Spamouflage »

(octobre 2023)

En octobre 2023, le MRR d'Affaires mondiales Canada annonce que le premier ministre Justin Trudeau, le chef de l'opposition Pierre Poilièvre, des ministres fédéraux ainsi que plusieurs dizaines de membres de la classe politique canadienne ont été la cible d'une campagne d'influence orchestrée par l'État chinois sur les plateformes Facebook et X. Dans son annonce, le MRR associe cette opération à un acteur informationnel baptisé « Spamouflage », dont les firmes Graphika et Meta ont déjà observé les agissements auparavant, l'estimant affilié à Pékin.

Cette campagne a reposé sur la diffusion massive d'hypertrucages (*deepfakes*), des vidéos frauduleuses fabriquées en utilisant l'intelligence artificielle. Celles-ci paraissent mettre en scène Liu Xin, un blogueur d'origine chinoise établi à Burnaby en Colombie-Britannique et très critique du Parti communiste chinois. Dans les vidéos, l'avatar de Liu Xin déverse toutes sortes d'accusations à l'encontre des élu-e-s en question, qui se seraient soi-disant rendus coupables de corruption, de manquements à l'éthique, voire d'actes criminels. Les vidéos étaient ensuite diffusées par un vaste réseau de faux profils de médias sociaux, laissant dans la foulée des milliers de commentaires calomnieux sur les comptes Facebook et X des personnalités politiques visées.

Cet incident se démarque par une impressionnante capacité d'intégration de différents outils numériques. D'une part, celui-ci représente le premier cas documenté au Canada d'utilisation d'un hypertrucage à des fins de désinformation géopolitique. D'autre part, un vaste réseau de faux comptes de médias sociaux automatisés a été mobilisé pour organiser la diffusion massive des vidéos truquées, et ce, de manière synchronisée pour conférer une visibilité maximale à ces contenus.

D'autre part, la campagne se distingue aussi par la variété des cibles touchées, en jouant simultanément sur deux niveaux. Il s'agissait évidemment de diffuser, auprès de l'opinion publique, diverses rumeurs dommageables à l'encontre de plusieurs élu-e-s canadiens de toutes allégeances politiques. Parallèlement, l'opération permettait aussi de discréditer Liu Xin, un détracteur du régime chinois comptant des centaines de milliers de personnes abonnées sur les réseaux sociaux. Notons qu'une campagne similaire avait été observée en 2017 à l'encontre des membres canadiens du mouvement spirituel Falun Gong. De faux courriels insultants ou menaçants, prétendument signés par des membres de cette communauté, avaient alors été envoyés à de nombreux membres de la classe politique canadienne dans le but de décrédibiliser le Falun Gong auprès d'elle.

Les opérations d'influence chinoises repérées jusqu'alors au Canada semblaient de prime abord épargner le Parti libéral et plutôt se concentrer sur son rival conservateur. L'étendue tout comme la teneur de la campagne de « Spamouflage » suggèrent que, prenant acte de l'évolution du débat politique canadien, la Chine se montre désormais plus agressive dans le choix de ses cibles.

Infrastructures critiques : des voyants rouges s'allument

Dans les débats et réflexions entourant les cybermenaces, les risques pesant sur les infrastructures critiques sont probablement l'enjeu faisant couler le plus d'encre, au Canada et ailleurs. Probablement à raison : la perspective que des cyberattaques puissent un jour endommager les réseaux électriques, les systèmes de traitement des eaux ou encore des installations industrielles vitales a de quoi inquiéter. Pour autant, certains spécialistes en cybersécurité ont dans les dernières années appelé à ne pas exagérer l'importance de ces menaces : celles-ci représentent en effet un scénario « à fort impact et de faible probabilité », là où de nombreuses cyberattaques moins spectaculaires se produisent au quotidien et nécessiteraient une plus grande attention des décisionnaires. À l'horizon 2024, toutefois, la faible probabilité attribuée jusqu'ici aux menaces visant les infrastructures critiques est de plus en plus sujette à questionnement.

INFILTRER ET PRÉPOSITIONNER

De fait, au Canada et ailleurs dans le monde, l'année 2023 a été marquée par plusieurs incidents démontrant que les infrastructures critiques sont des cibles toujours moins « hors limite » pour les pirates informatiques. En mai 2023 et février 2024, les autorités américaines ont par exemple révélé différentes activités attribuées aux groupes de pirates étatiques chinois Volt Typhoon, qui seraient parvenus à prépositionner des logiciels malveillants aussi bien dans des infrastructures énergétiques que dans des systèmes de transport ou de traitement des eaux américains. En novembre 2023, on apprenait que le groupe de pirates Sandworm (lié au renseignement militaire russe) était parvenu à pirater l'alimentation électrique d'une ville ukrainienne — répétant pour une troisième fois un tour de force déjà réalisé en 2015 puis en 2016. Entre-temps, en avril 2023, la fuite d'information dite des *Discord Leaks* révélait qu'un autre groupe de pirates russes aurait quant à lui tenté de s'introduire dans les systèmes de commande d'un gazoduc canadien (voir encadré).


@Cody Hiscox

Très préoccupants, ces incidents nous rappellent un fait encore souvent mal compris par le grand public : autrefois contrôlées manuellement par le biais de manettes, de leviers ou d'interrupteurs, les infrastructures critiques sont aujourd'hui hautement informatisées, voire automatisées. Les systèmes SCADA, notamment, sont devenus la cheville ouvrière de nombreuses infrastructures vitales, en numérisant les mesures et les contrôles auparavant effectués par des opérateurs humains. Sans surprise, ces technologies deviennent également une cible privilégiée des pirates informatiques, particulièrement ceux affiliés à des États, dans la perspective de prendre le contrôle de systèmes industriels à distance et, potentiellement, les perturber ou les saboter. Qu'il s'agisse de la Chine, des États-Unis ou de la Russie, plusieurs grandes puissances semblent chercher depuis plusieurs années déjà à infiltrer discrètement les infrastructures critiques de puissances adverses en vue de pouvoir pirater celles-ci le jour où un conflit majeur viendrait à éclater.

> \\ **À l'horizon 2024, la faible probabilité attribuée jusqu'ici aux menaces visant les infrastructures critiques est de plus en plus sujette à questionnement.** \\

INSTALLATIONS VITALES, INFORMATIONS CRITIQUES

Pour l'heure, de telles opérations restent extrêmement complexes et difficiles à entreprendre, du fait qu'elles nécessitent un savoir-faire de pointe et un effort de renseignement considérable en vue de bien cartographier l'architecture numérique des systèmes en question. Pour autant, différents incidents témoignent de l'appétit grandissant des pirates informatiques pour des informations sensibles pouvant par la suite faciliter le ciblage d'infrastructures critiques. En août 2023 par exemple, la Commission des services électriques de Montréal a été victime d'une attaque par rançongiciel conduite par le groupe cybercriminel russe LockBit. Sans viser directement l'infrastructure électrique, celle-ci a néanmoins permis aux pirates de mettre la main sur de nombreux documents techniques confidentiels, dont le contenu pourrait a priori aider un acteur malveillant à concevoir une opération contre des systèmes de contrôle. Il est concevable qu'un groupe comme LockBit puisse chercher à transmettre ce genre d'information à d'autres acteurs, notamment étatiques, par appât du gain ou pour s'acheter une immunité.

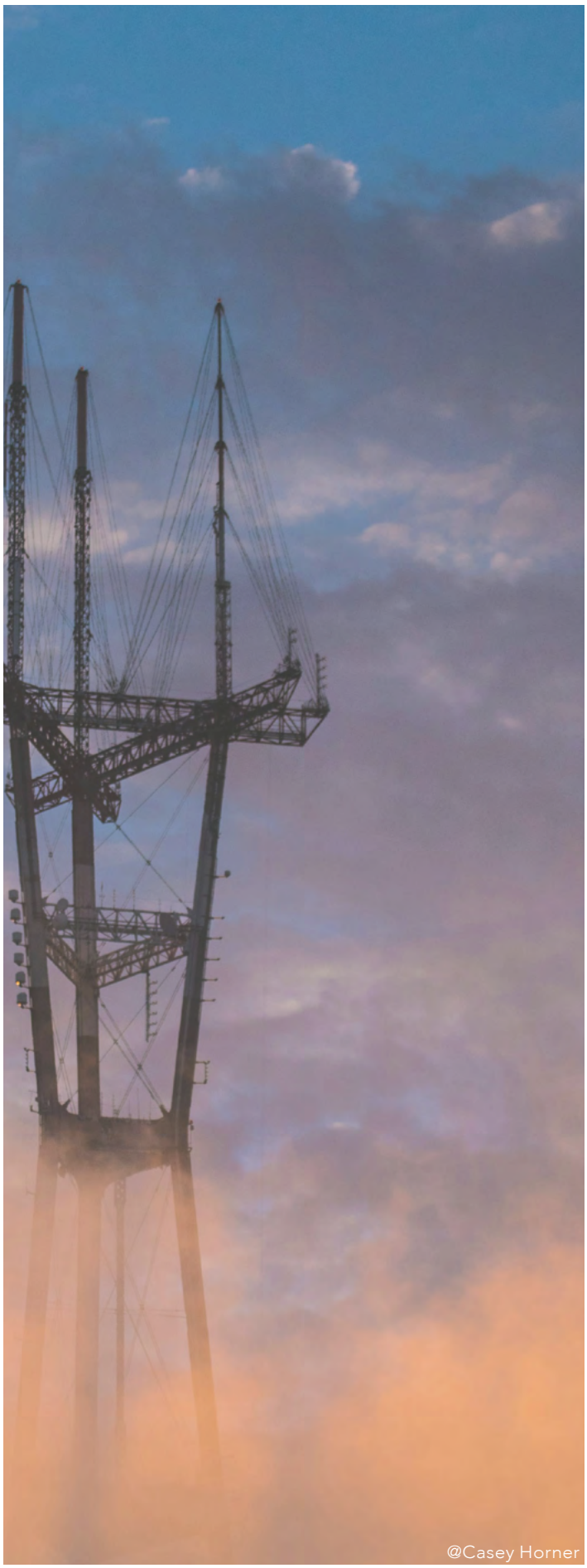
Un autre précédent canadien illustre encore mieux ce phénomène : en 2012, la société albertaine Telvent, concepteur de logiciels de gestion d'infrastructures pétrolières, a été la cible d'une opération de cyberespionnage attribuée à des hackers étatiques chinois. On soupçonne aujourd'hui que le piratage aurait servi à collecter des données techniques sur les produits de Telvent, qui équipent différentes infrastructures énergétiques américaines. Ainsi, sous des apparences anodines, l'opération contre Telvent en 2012 pourrait bien avoir servi à préparer des activités plus agressives, comme celles du groupe chinois Volt Typhoon observées récemment aux États-Unis. Ceci démontre, d'une part, que la sécurité des infrastructures critiques ne se limite pas aux installations vitales, mais s'étend dans une certaine mesure à toute la chaîne d'approvisionnement qui en assure la conception et l'entretien. D'autre part, cela met en évidence que le Canada, siège de nombreux concepteurs de systèmes industriels, peut aussi représenter une cible « intermédiaire » pour des pirates informatiques cherchant à compromettre les infrastructures d'autre pays.

TABOU À GÉOMÉTRIE VARIABLE

Il importe de souligner que les piratages touchant aux infrastructures critiques représentent pour l'heure une infime minorité des activités malveillantes globalement

observées dans le cyberespace. Il semble d'ailleurs persister une part de tabou ou de retenue sur cette question parmi les puissances cyber, pour qui de telles cyberattaques doivent manifestement être réservées aux situations de conflit ouvert. Cette règle non écrite varie cependant dans sa vigueur, dépendamment du contexte géopolitique considéré : pas directement en guerre, mais ennemis jurés néanmoins, l'Iran et Israël échangent de plus en plus fréquemment des cyberattaques visant des infrastructures importantes, voire critiques. Depuis 2020, tous deux ont tour à tour visé des systèmes de traitement des eaux, des terminaux portuaires, des aciéries ou des stations essence de l'adversaire. L'autolimitation des États sur la question des infrastructures critiques ne peut donc être entièrement tenue pour acquise.

Face à cette menace, certains pays s'emploient déjà à renforcer activement leurs défenses. En 2018, les États-Unis ont par exemple créé une agence dédiée, la Cybersecurity and Infrastructure Security Agency (CISA), dont c'est la mission principale. La même année, la Defense Advanced Research Projects Agency (DARPA) a conduit un premier exercice grandeur nature de cyberattaque contre un réseau électrique sur une infrastructure de test spécialement créée pour l'occasion et située sur une petite île de l'État de New York. Durant plusieurs jours, une équipe d'ingénieur-e-s s'est vu confier la mission de protéger l'alimentation électrique de l'île face à une équipe de pirates mandatée par le département de la Défense. Rappelant à bien des égards les exercices de protection civile fréquemment tenus pendant la guerre froide en cas d'attaque nucléaire, de telles simulations peuvent contribuer à accroître la résilience des États en cas de piratages d'infrastructures critiques de grande ampleur. C'est là le genre de pratiques novatrices dont le Canada, s'il ne le fait pas déjà, pourrait s'inspirer à l'avenir pour mieux gérer les menaces aux infrastructures vitales.



@Casey Horner

Révélations d'intrusions russes dans des systèmes de gazoduc

(printemps 2023)

Au printemps 2023, une fuite d'information majeure vient bouleverser le cycle de nouvelles. Des centaines de documents provenant de la communauté du renseignement américaine ont fait leur apparition sur Discord, une plateforme de discussion pour adeptes de jeux vidéo. On y découvre une masse d'informations classifiées sur divers enjeux géopolitiques sensibles, du conflit russo-ukrainien aux capacités militaires taïwanaises. On apprendra plus tard que la fuite est l'œuvre d'un jeune Américain engagé dans une unité de renseignement militaire de la garde nationale. Dans le torrent de révélations qui s'échelonnent sur tout le mois d'avril, une nouvelle vient créer la stupeur au Canada : un groupe de pirates informatiques russes aurait tenté de s'introduire dans les systèmes de gestion d'un gazoduc canadien.

En effet, selon des documents contenus dans les fuites, le renseignement américain aurait intercepté des échanges entre le FSB, un des services du renseignement russe, et un groupe de pirates se faisant appeler Zarya. À la mi-février 2023, les pirates auraient notamment transmis au FSB des captures d'écran censées prouver qu'ils étaient parvenus à compromettre les systèmes d'un gazoduc de l'Ouest canadien. Dans les échanges, les hackers affirmaient être en mesure de contrôler à distance la pression des valves du gazoduc ou d'en désactiver les systèmes d'urgence en vue de pouvoir causer une explosion. Convaincus des allégations de Zarya, les officier-ère-s du FSB impliqués disaient alors surveiller l'actualité canadienne, à l'affût de nouvelles annonçant un accident industriel de grande ampleur.

Les manœuvres de Zarya se voulaient évidemment des représailles à l'aide militaire fournie à l'Ukraine par le Canada. Quelques semaines avant l'échange entre les pirates et le FSB, Ottawa avait notamment annoncé la livraison de chars Leopard 2 aux forces ukrainiennes. Les révélations issues des *Discord leaks* suscitent toutefois le scepticisme. Alors que l'origine des fuites n'a pas encore été établie, plusieurs doutent de l'authenticité des documents. D'autres soulignent que les agent-e-s du renseignement russe sont historiquement connus pour leurs exagérations, suggérant ainsi que Zarya pourrait bien avoir inventé ses exploits de toutes pièces.

Néanmoins, quelques jours plus tard, le premier ministre Justin Trudeau est interrogé sur l'incident lors d'une conférence de presse. Celui-ci déclare alors qu'« il n'y a eu aucun dommage physique à une infrastructure énergétique » à la suite de la cyberattaque. Rassurante compte tenu des affirmations de Zarya, la déclaration semble toutefois confirmer qu'une tentative de cyberintrusion a bien eu lieu. L'emplacement de l'installation concernée de même que l'identité de son opérateur demeurent cependant un mystère.

Si des pirates russes ont donc vraisemblablement cherché à compromettre une infrastructure énergétique canadienne, il est très peu probable qu'ils aient été en mesure de causer un accident industriel. Une telle entreprise (tentée en 2018 par des pirates du FSB contre une raffinerie saoudienne) requerrait en effet un degré d'expertise, de ressources et de préparation colossal, qui n'est à la portée que d'un petit nombre d'acteurs cyber. Or, Zarya est bien loin de pouvoir prétendre à ce statut : groupe de « hackers patriotiques », il ne s'est fait connaître que par des piratages de faible sophistication, tels des attaques par déni de service ou des défacements de sites web.

Pour l'heure, faute de plus amples détails publicisés par les autorités canadiennes, il reste difficile de déterminer précisément quels aspects de l'incident doivent être considérés comme avérés ou non. Une chose est néanmoins certaine : il faut présumer que d'autres acteurs pourront à l'avenir tenter de répéter l'expérience, et tous pourraient ne pas être aussi inoffensifs que Zarya.

Arsenalisation des rançongiciels : la vulnérabilité des chaînes d'approvisionnement et des entités contractantes

L'année 2023 a démontré une fois de plus que les attaques par rançongiciels figurent parmi les principales menaces cyber au Canada. Désormais bien connus du grand public, ces logiciels malveillants servent à crypter les données stockées sur un ordinateur, les rendant ainsi inaccessibles à son utilisateur-trice, et permettent aux pirates informatiques de demander une rançon en échange d'une clé de décryptage. À l'échelle internationale, l'une des attaques les plus médiatisées à ce titre s'est produite en 2021, lorsque l'opérateur d'oléoducs américain Colonial Pipeline a dû suspendre ses activités et payer une rançon de 4,4 millions de dollars à des membres d'organisations cybercriminelles, vraisemblablement du groupe russe DarkSide selon les autorités fédérales américaines. A priori motivées par l'appât du gain, les attaques par rançongiciel peuvent néanmoins revêtir une dimension géopolitique.

D'une part, celles-ci peuvent compromettre des données sensibles d'organisations œuvrant dans des domaines stratégiques, ouvrant la possibilité que les cybercriminel-le-s ne cherchent à transmettre ces informations à des acteurs étatiques. Au cours des dernières années, notre répertoire des cyberincidents canadiens a recensé plusieurs cas présentant ce potentiel. En mai 2022, par exemple, l'entreprise aéronautique CMC Électronique, basée à Montréal et active dans le secteur de l'aérospatiale de défense, était — selon les hypothèses les plus plausibles — ciblée par le groupe cybercriminel ALPHV (ou BlackCat), basé en Russie. Le même mois, LockBit, un autre groupe malveillant basé en Russie, était soupçonné d'avoir attaqué Top Aces, une entreprise canadienne œuvrant à l'entraînement des pilotes de chasse. D'autre part, comme le démontre l'épisode Colonial Pipeline, les attaques par rançongiciels peuvent aussi ébranler des secteurs clés de l'économie canadienne ou nord-américaine et ainsi déstabiliser le quotidien de la société canadienne dans son ensemble. Le Centre canadien pour la cybersécurité estime d'ailleurs que les rançongiciels « sont en hausse » et figurent désormais parmi « les cybermenaces les plus courantes qui guettent les Canadiennes et les Canadiens ».

@Top Aces Alpha Jet

DERRIÈRE LE MASQUE DES GANGS NUMÉRIQUES

Le ciblage par rançongiciel d'entités stratégiquement sensibles a continué d'être observé au Canada en 2023, consacrant une emphase notable sur des entités contractantes de la défense canadienne. En octobre dernier, le ministère de la Défense nationale a par exemple révélé qu'un cyberincident avait touché l'entreprise Brookfield Global Relocation Services (BGRS), qui fournit des services de déménagement à un grand nombre de personnes employées par le gouvernement fédéral. Apparemment dû à un rançongiciel, l'incident aurait mené à la compromission des données personnelles de membres des Forces armées canadiennes, du corps diplomatique, ou encore de la GRC. Bien que des soupçons planent à l'encontre du groupe criminel russe LockBit, l'identité des responsables de l'attaque de BGRS n'a pour l'heure pas été officiellement établie.

Il faut néanmoins envisager aussi que l'information obtenue par les cybercriminel-le-s puisse revêtir un grand intérêt pour des services de renseignement étranger. Alors que nombre de gangs auteurs de rançongiciels sont basés en Russie, diverses études suggèrent l'existence de liens significatifs entre la sphère cybercriminelle et les autorités russes. Les criminel-le-s collaboreraient notamment avec le Kremlin pour s'acheter une impunité et représenteraient par ailleurs un bassin de recrutement pour le renseignement russe. Toute information compromise à valeur géopolitique ou stratégique peut ainsi représenter une monnaie d'échange pour les groupes cybercriminels. Un autre cyberincident canadien soumis à cette problématique a été observé en 2023 : le piratage du contractant de la défense canadienne Black & McDonald (voir plus bas).

LE CANADA AU CŒUR D'UNE RÉGION ATTRAYANTE POUR LES CYBERCRIMINEL-LE-S

Il s'avère par ailleurs que les attaques par rançongiciel peuvent aussi occasionner des perturbations majeures de l'activité économique, représentant ainsi un potentiel enjeu de sécurité nationale. Un rapport sur les rançongiciels et les campagnes d'extorsion publié en 2023 par l'entreprise de cybersécurité Palo Alto Networks souligne l'ampleur des risques auxquels le Canada est confronté en la matière. Non seulement figure-t-il parmi les cinq pays les plus fréquemment touchés par des rançongiciels, avec les États-Unis, la Grande-Bretagne, l'Allemagne et la France, mais il fait également partie de la région la plus ciblée par les cybercriminel-le-s, soit l'Amérique du Nord. Le Canada, les États-Unis et le Mexique ont effectivement été victimes de près de 50% des attaques par rançongiciels recensées par l'entreprise. Puisque plusieurs incidents du genre ne sont jamais divulgués, ces données ne sont qu'une indication partielle du paysage des offensives par rançongiciels dans le monde. Elles portent toutefois à croire que le Canada doit continuer à prendre ce risque au sérieux pour au moins deux raisons.

> \\ A priori motivées par l'appât du gain, les attaques par rançongiciel peuvent néanmoins revêtir une dimension géopolitique. \\

D'une part, les États-Unis sont à la fois le pays le plus touché par les attaques par rançongiciels et le premier partenaire économique du Canada. Les cybercriminel-le-s qui les visent ciblent souvent des entreprises œuvrant dans des secteurs névralgiques pour la sécurité économique et où les chaînes d'approvisionnement canado-américaines sont fortement intégrées, dont les secteurs manufacturier, financier, du transport et de la construction. En plus des opérations pouvant viser directement le Canada dans ces secteurs, des attaques contre des entreprises américaines dont dépendent

fortement les Canadiennes et les Canadiens peuvent donc avoir des contrecoups immédiats au pays.

Un récent rapport de la Banque du Canada souligne notamment que les effets d'une cyberattaque contre une banque américaine (ou canadienne) vont généralement bien au-delà de l'entreprise ciblée, ébranlant le système financier dans son ensemble et nuisant aux investisseurs des deux pays. En août 2003, une panne d'électricité monstre plongeant 50 millions de personnes dans le noir pendant plusieurs jours, en Ontario, au Québec et dans plusieurs États américains (comme l'Ohio, New York et le Michigan), avait été causée par un « ensemble d'erreurs d'origine électrique, informatique et humaine ». Or, cet épisode rappelle le type de paralysie qui pourrait découler d'une attaque par rançongiciel contre l'une ou l'autre des mailles d'un système énergétique canado-américain fortement intégré. Dans l'édition 2023 de notre rapport sur les cyberincidents géopolitiques au Canada, nous mettions également en évidence le risque que des acteurs étatiques chinois ciblent des entreprises canadiennes opérant dans des secteurs cruciaux pour la compétition géoéconomique entre Washington/Ottawa et Pékin (minéraux critiques, semi-conducteurs, etc.).

D'autre part, les récentes réponses du Canada aux grands évènements mondiaux de l'heure permettent de croire qu'il s'expose plus qu'avant au risque que des rivaux géopolitiques n'utilisent les rançongiciels en représailles à certaines prises de position internationales. Après le déclenchement de l'invasion tous azimuts de l'Ukraine en février 2022, de nombreux observateurs-trices ont par exemple craint que les groupes cybercriminels russes ne soient mobilisés pour nuire aux pays soutenant Kyiv. Le rançongiciel déployé en mars 2022 par des pirates russes contre l'aluminerie Alouette à Sept-Îles, notamment, a suscité de telles inquiétudes au Canada. Bien que les groupes cybercriminels russes n'aient jusqu'ici pas véritablement réorganisé leurs activités à des fins de coercition géopolitiques, ce risque n'a pas complètement disparu pour autant. À cet égard, on peut noter que la firme montréalaise Top Aces, déjà visée par un rançongiciel en 2022, a récemment annoncé sa participation à l'entraînement de pilotes ukrainiens sur les avions de chasse F-16. De telles activités pourraient susciter l'attention des gangs de cyberextorsion basés en Russie ; qu'ils veuillent dénicher des données sensibles ou qu'ils désirent punir les organisations concernées.


@Renan Kamikoga

L'attaque par rançongiciel contre Black & McDonald

(mars 2023)

Le 8 mars 2023, le ministère de la Défense du Canada annonçait que l'entreprise Black & McDonald avait été la cible d'une attaque par rançongiciel quelques semaines auparavant. Née à Toronto au début des années 1920, Black & McDonald compte aujourd'hui des bureaux aux quatre coins du Canada ainsi que des filiales dans plusieurs États américains comme New York, le Kentucky, l'Arkansas, l'Utah et l'Oregon. L'entreprise se spécialise dans de nombreux secteurs : infrastructures de recharge pour véhicules électriques, construction d'infrastructures de services publics, ingénierie et conception de systèmes électriques, entretien de centrales nucléaires, etc.

Black & McDonald peut également représenter une valeur stratégique pour de potentiels rivaux géopolitiques du Canada, car elle est la société mère de Canadian Base Operators, qui « maintient plusieurs contrats avec le ministère de la Défense nationale pour de la gestion d'installations militaires et des services de soutien logistique ». Comme l'indique son site Internet, Canadian Base Operators remplit notamment de nombreuses fonctions de soutien spécialisé auprès des militaires canadiens en matière de transport, d'approvisionnement, de gestion des munitions, de logistique, et de maintenance des armes et des équipements de communication.

Par crainte du potentiel d'infection, le ministère de la Défense du Canada a pendant plusieurs jours bloqué ses échanges de courriels avec Black & McDonald, en attendant que les efforts de remédiation soient achevés. Bien que le ministère ait par la suite indiqué que ses propres systèmes n'avaient pas été affectés par la cyberattaque, la nature des données compromises dans les systèmes du contractant n'a cependant pas été précisée. Près d'un an après la cyberopération contre Black & McDonald, l'identité des responsables de même que leurs motifs demeurent inconnus, notamment parce que les entreprises canadiennes ne sont pas tenues de divulguer ce type d'information au public. D'ailleurs, l'entreprise n'a à ce jour pas même confirmé si l'incident avait eu lieu.

Des expert-e-s en cybersécurité n'ont toutefois pas manqué de rappeler, comme le fait le présent rapport, que de telles attaques sont régulièrement commises par des groupes basés dans des pays rivaux du Canada et des États-Unis, comme l'Iran, la Corée du Nord ou encore la Russie. Si des groupes russes ou d'autres pays rivaux du Canada sont effectivement derrière l'attaque au rançongiciel contre Black & McDonald, ce cyberincident rappellerait une fois de plus les vulnérabilités du Canada dans des secteurs hautement stratégiques. Plus globalement, l'épisode souligne aussi le fait que l'infrastructure globale de défense du Canada intègre désormais un nombre important d'acteurs du secteur privé, qui peuvent représenter des cibles de choix pour les pirates.

CONCLUSION : UN CYBERESPACE ENTRE ACTIONS ET RÉACTIONS

Depuis les années 1980, le Canada cherche à s'affirmer comme un défenseur des droits humains et des valeurs démocratiques sur la scène internationale, notamment par son implication dans plusieurs opérations de paix autour du globe. Avantagé par sa proximité avec le géant américain et protégé par deux océans, le Canada a longtemps joui d'une situation dans laquelle ses critiques à l'encontre de pays ou d'acteurs étrangers — souvent jugés en rupture avec les idées libérales — portaient peu à conséquence. Or, force est de constater que l'essor de la cyberconflictualité et la dilution des déterminants géographiques dans le cyberespace viennent progressivement changer cet état de fait. À cela s'ajoute une instabilité croissante du système international, qui voit se multiplier les fractures et les crises sur lesquelles le Canada est amené à prendre position.

À cet égard, 2023 a montré qu'une multiplicité de groupes et d'individus sont à l'affût des décisions politiques canadiennes et ont désormais l'opportunité de « punir » le Canada pour celles-ci, au moyen de technologies de plus en plus accessibles. Qu'il s'agisse de critiques à l'encontre du traitement des Ouïghours par la Chine, de soupçons d'assassinat de militant-e-s sikhs par le gouvernement indien, ou de l'aide militaire canadienne octroyée à l'Ukraine, les choix politiques du Canada deviennent de plus en plus rapidement synonymes de représailles numériques. Sans être directement visé, le Canada peut aussi constituer un champ de bataille dans le contexte d'affrontements idéologiques. Fin 2023, des internautes provenant du Canada ont par exemple été exposés à une opération d'influence orchestrée par l'Iran, dans laquelle des services de diffusion télévisuelle en ligne (*streaming television services*) ont été piratés pour diffuser un hypertrucage dénonçant l'intervention militaire israélienne à Gaza.

La prolifération d'acteurs non étatiques, comme les groupes hacktivistes, complique de surcroît la gestion de ces enjeux : armés de leurs claviers, de simples citoyennes et citoyens peuvent désormais pratiquer une forme de politique étrangère parallèle, par l'entremise de cyberattaques à caractère idéologique. Ces actions, sans forcément occasionner de dégâts notables, ont néanmoins des retombées psychologiques en perturbant le quotidien de Canadiennes et Canadiens et en suscitant potentiellement un sentiment d'insécurité. C'est d'ailleurs souvent là leur logique : en troublant la population, les acteurs malveillants cherchent vraisemblablement à induire une pression sur les décideur-euse-s politiques, dans l'idée de les faire revoir certaines de leurs positions à caractère géopolitique.

Il est donc impératif de bien appréhender la facilité croissante avec laquelle des acteurs politiquement motivés peuvent désormais mener des actions numériques potentiellement perturbatrices. Cela ne veut évidemment pas dire que le Canada doive se montrer plus discret ou circonspect en matière de politique étrangère, y compris dans la défense des valeurs libérales. Néanmoins, cette nouvelle réalité implique que l'opinion publique canadienne pourrait à l'avenir se montrer plus sensible ou fébrile à l'encontre des décisions à portée internationale adoptées à Ottawa. Des plus en plus fréquents, les cyberincidents touchant le Canada ne doivent donc pas être abordés comme des défis de nature uniquement technologique, mais aussi comme des actes ayant une portée éminemment politique.

Rubrique méthodologique

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, qu'il s'agisse de sa population, de ses pouvoirs publics, de ses entreprises, de sa société civile, de ses infrastructures ou des entités y étant basées. Le répertoire se veut une source de référence, régulièrement mise à jour, mais ne prétend pas à l'exhaustivité. Ses données remontent pour l'heure jusqu'à 2010. 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 politiques, militaires, 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.

UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

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-trice 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 offensives 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 (défacement), 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-trice 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 manipulation de l'information 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 plus fréquemment publicisée que la responsabilité d'un cyberincident. 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 gouvernementales, etc. Nous invitons les lectrices et lecteurs à parcourir le répertoire en ligne pour plus de détails sur l'origine attribuée 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 :
Daphné St-Louis Ventura
Louis Collerette

Graphisme :
Françoise Conea

Avec l'appui de :

BANQUE NATIONALE

Photo de couverture : easy-peasy.ai