UQÀM

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

Cyberincidents géopolitiques au Canada

Un état des lieux proposé par l'Observatoire des conflits multidimensionnels

Introduction

Lors des élections présidentielles américaines de 2016, des pirates informatiques russes ébranlent l'une des plus grandes démocraties du monde. Ils favorisent l'élection de Donald Trump, candidat préféré de Moscou, en diffusant de fausses informations à caractère politique sur les médias sociaux et en dévoilant des courriels du comité national du Parti démocrate par le biais de *Wikileaks*. L'ingérence russe paralyse souvent la vie politique américaine par la suite, conduisant les démocrates à remettre en question la légitimité de la présidence Trump dès le départ, incitant le Congrès des États-Unis à mener de nombreuses enquêtes sur la présumée collaboration entre Moscou et les proches de Trump, et amenant le département de la Justice à lancer l'enquête Mueller, qui divise Washington et la population américaine pendant près de deux ans.

Ce cyberincident ne touche pas directement le Canada, mais revêt néanmoins une importance indéniable pour les Canadiennes et Canadiens. D'une part, il prouve qu'il est désormais possible de déstabiliser n'importe quel pays en quelques clics de souris, même la superpuissance américaine. D'autre part, l'ingérence russe rappelle que les actions malveillantes dans l'espace cyber sont désormais au cœur des nouvelles conflictualités internationales et que le Canada doit également y réfléchir, lui qui a fait l'objet de nombreux cyberincidents ces dernières années.

C'est dans cet esprit que l'Observatoire des conflits multidimensionnels (OCM) de la Chaire Raoul-Dandurand publie le présent rapport sur les « cyberincidents géopolitiques au Canada ». Ce rapport s'appuie sur des données colligées dans le tout nouveau ***répertoire des cyberincidents canadiens*** de l'OCM, qui recense pour l'heure une cinquantaine de cyberincidents géopolitiques et stratégiques ayant directement touché le Canada depuis une dizaine d'années. Ce répertoire — disponible en libre accès — ainsi que le présent rapport visent trois objectifs :

1. ***Mieux définir le phénomène des cyberincidents géopolitiques et stratégiques et leurs conséquences pour le Canada.*** Comme l'indique le présent rapport, ces cyberincidents sont plus fréquents qu'on pourrait le croire et prennent la forme d'actions malveillantes de la part d'acteurs internationaux, souvent étatiques, qui recourent, dans leur quête de puissance, aux cyberattaques, aux manipulations de l'information, au cyberespionnage ou encore au vol de données pour des motifs politiques, militaires ou économiques ;

2. ***Aider les instances gouvernementales, médias, grand public ainsi que les gens d'affaires canadiens à mieux distinguer les types de cyberincidents touchant le Canada, et favoriser le débat sur les stratégies et politiques nécessaires pour prévenir ceux-ci et protéger les intérêts du Canada dans l'espace cyber.*** Ce rapport se concentre notamment sur trois réalités qui font du Canada un pays vulnérable aux cyberincidents géopolitiques et stratégiques : a) le cyberespionnage des entreprises canadiennes ; b) les campagnes de désinformation visant les gouvernements ou intérêts du Canada à l'étranger ; et c) les cyberattaques contre des organisations internationales dont le Canada est membre ou le pays hôte ;

3. ***Répertorier les principaux cas de cyberincidents géopolitiques et stratégiques ayant touché le Canada au cours des dernières années, et offrir à la population canadienne une base de données utile pour prévoir le type d'incidents qui pourrait survenir à l'avenir.*** Présentant trois des 51 cyberincidents répertoriés par l'équipe de l'OCM (les activités de cyberespionnage de 2014 contre le Conseil national de recherches du Canada, les manipulations de l'information visant les soldats canadiens en Lettonie, et la cyberattaque contre le siège social de l'Organisation de l'aviation civile internationale à Montréal en 2016), ce rapport donne un avant-goût des informations disponibles dans le ***répertoire des cyberincidents canadiens***.

Le répertoire permet notamment de connaître les années et les cibles des cyberincidents ayant touché le Canada (secteur public, secteur privé, etc.), leur type (cyberespionnage, manipulations de l'information, etc.) ainsi que leur origine (Chine, Russie, Corée du Nord, etc.). La liste des cas recensés n'est pas exhaustive, mais sera régulièrement mise à jour grâce au travail de veille des chercheures et chercheurs de l'OCM. Nous invitons d'ailleurs les Canadiens et Canadiennes à communiquer avec nous s'ils ont connaissance de tout cyberincident géopolitique et stratégique pouvant être ajouté au répertoire. Nous présentons les critères de définition des cyberincidents inclus dans le répertoire plus loin dans ce rapport.

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 du 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, et les effets de la compétition géoéconomique sino-américaine sur les relations entre le Canada et les États-Unis.

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 l'essor des stratégies de désinformation et la cyberdéfense, ainsi que sur la politique américaine. Il a contribué à plusieurs ouvrages collectifs en français et en anglais portant sur les conflits armés et la politique étrangère.

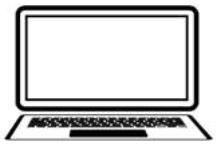
Danny Gagné est étudiant au doctorat en science politique à l'UQAM, chercheur en résidence et boursier-stagiaire des Commissionnaires du Québec à l'Observatoire des conflits multidimensionnels. Ses recherches portent sur les stratégies de guerre par procuration américaines et l'ingérence des puissances étrangères dans les guerres civiles dans le monde. Ses récents travaux à l'OCM ont fait l'objet de nombreuses « chroniques des nouvelles conflictualités » de la Chaire Raoul-Dandurand, portant sur les manipulations de l'information lors des élections canadiennes ou encore le bras de fer entre Washington et Huawei sur la 5G.

Gabrielle Gendron est étudiante à la maîtrise en science politique à l'UQAM, chercheure en résidence et boursière-stagiaire des Commissionnaires du Québec 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, et contribue régulièrement aux « chroniques des nouvelles conflictualités » de la Chaire Raoul-Dandurand.

Simon Piché-Jacques est candidat à la maîtrise en science politique à l'UQAM et chercheur en résidence à l'Observatoire des conflits multidimensionnels. Ses recherches portent sur l'implication des services de renseignement dans les nouvelles conflictualités et l'espionnage économique chinois à l'égard du Canada. Ses récents travaux à l'OCM ont fait l'objet de nombreuses « chroniques des nouvelles conflictualités » de la Chaire Raoul-Dandurand, sur les stratégies de subversion russe ou encore l'espionnage des secteurs stratégiques du Canada.

Sommaire

DIX INCIDENTS MARQUANTS



2011

CYBERINTRUSION AU CONSEIL DU TRÉSOR

Une cyberattaque vise à dérober des accès au Conseil du trésor, au ministère des Finances et à Recherche et développement pour la défense Canada. Les pirates informatiques ont tenté de prendre le contrôle des ordinateurs des cadres supérieurs du gouvernement canadien, afin de voler les mots de passe clés qui déverrouillent des systèmes de données gouvernementaux. Un virus aurait également été inséré dans les réseaux informatiques pour chercher des documents précis.

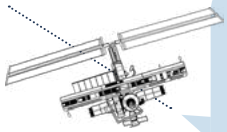
2012

RÉVÉLATIONS DE L'AFFAIRE NORTEL

Des opérations d'espionnage économique chinoises échelonnées sur plusieurs années ont visé le géant canadien des télécommunications Nortel, contribuant à sa faillite en 2009. Les pirates informatiques chinois ont volé des mots de passe de hauts dirigeants pour pouvoir s'introduire dans les ordinateurs de la compagnie. Ils ont ensuite récupéré des données sensibles de l'entreprise au moyen d'une « porte dérobée » (*backdoor*). L'incident a été révélé en février 2012.

2014

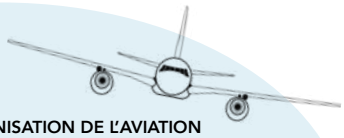
PIRATAGE DU CONSEIL NATIONAL DE RECHERCHES DU CANADA



Le Conseil national de recherches du Canada (CNRC) est visé par une importante opération de cyberespionnage provenant de Chine. Une importante quantité d'informations sensibles pourrait avoir été dérobée, alors que le CNRC travaillait notamment sur le développement de la communication quantique et les technologies satellites.

page 16

2016



PIRATAGE DE L'ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Le système informatique de l'Organisation de l'aviation civile internationale (OACI) est victime d'une cyberattaque de grande ampleur. Des logiciels malveillants devaient servir à piéger des États membres et des compagnies aériennes. Les cyberespions ont eu accès aux mots de passe et courriels de plus de 2000 utilisateurs des systèmes de l'OACI et pourraient avoir accédé aux données de citoyennes et citoyens canadiens.

page 24

2016

CYBERATTAQUE CONTRE L'AGENCE MONDIALE ANTIDOPAGE

L'Agence mondiale antidopage affirme qu'un groupe de pirates informatiques russes a accédé à ses données en s'introduisant dans son système d'administration et de gestion. Le groupe a ensuite divulgué des informations médicales confidentielles d'athlètes sur le web, dont celles de sept athlètes canadiens. Les systèmes du Centre canadien pour l'éthique dans le sport ont également été compromis. Ces actions font suite aux révélations, en mai 2016, d'une vaste campagne de dopage d'athlètes russes dans le cadre des Jeux olympiques de Sotchi de 2014. En 2018, le gouvernement du Canada attribue l'intrusion au service du renseignement militaire russe.

2017

CAMPAGNE DE DÉSINFORMATION CONTRE LES FORCES CANADIENNES EN LETTONIE

En marge du déploiement (sous l'égide de l'OTAN) de 450 soldats canadiens en Lettonie, une vague de fausses nouvelles sont publiées en russe sur le web pour dénigrer la présence du contingent. En avril 2018, le premier ministre Justin Trudeau accuse officiellement le gouvernement russe d'être derrière ces fausses rumeurs.

page 20

CAMPAGNE DE TROLLING SAOUDIENNE

En marge d'une crise diplomatique entre le Canada et l'Arabie saoudite, des « trolls » saoudiens initient une campagne coordonnée sur Twitter visant à ternir l'image du gouvernement canadien. Les contenus en question exploitent notamment les enjeux du traitement des communautés autochtones au Canada et de l'indépendance du Québec.

2018

OPÉRATION CLOUD HOPPER

Le Canada et plusieurs pays alliés attribuent à la Chine une vaste campagne de cyberespionnage économique. Des entreprises canadiennes ont été, depuis 2016 au moins, parmi les cibles de pirates informatiques cherchant à voler des titres de propriété intellectuelle ainsi que des secrets d'entreprises. Les renseignements dérobés concernent notamment les télécommunications, les biotechnologies, l'automobile et l'industrie minière.

2019

CAMPAGNE DE TROLLING SUR LES PIPELINES ET L'IMMIGRATION

Une analyse révèle que 9,6 millions de tweets ont été publiés entre 2013 et 2019 dans le but d'orienter les narratifs entourant des enjeux politiques canadiens. Parmi les sujets exploités figurent notamment le développement des pipelines au Canada et les politiques d'immigration. Selon Twitter, les faux comptes derrière ces tweets seraient liés à la Russie, au Venezuela et à l'Iran.

2020

CYBERESPIONNAGE RUSSE EN LIEN AVEC LA COVID-19

Le Canada, le Royaume-Uni et les États-Unis accusent officiellement la Russie des cyberintrusions contre leurs organismes de recherche travaillant sur la COVID-19. Le nom des organismes touchés demeure inconnu, les autorités ne précisent pas si cette attribution inclut la cyberattaque contre une entreprise pharmaceutique canadienne annoncée en avril 2020.

Les cyberincidents à caractère géopolitique : où en est le Canada ?

Depuis plusieurs années maintenant, les enjeux de cybersécurité font régulièrement les manchettes à travers le Canada. Si la majorité des incidents dans ce domaine relève de cybercriminalité, les actes malveillants à caractère géopolitique et provenant de puissances adverses se multiplient eux aussi : cyberespionnage du Centre national de recherches du Canada par la Chine en 2014, piratage du Centre canadien pour l'éthique dans le sport par la Russie en 2016, ou encore cyberattaques contre des organismes de recherche travaillant sur la COVID-19 en 2020. Certes, le Canada n'a pas encore été victime de cyberincidents aussi spectaculaires que certains autres pays. L'Ukraine, par exemple, était en 2015 victime d'une cyberattaque privant d'électricité 225 000 de ses citoyennes et citoyens pendant plusieurs heures. Néanmoins, on observe que la menace cybernétique a discrètement, mais fermement fait son entrée dans le quotidien des Canadiennes et des Canadiens.

Souvent abordés comme des faits isolés, parfois réduits à leur dimension technique, vite oubliés dans le cycle de nouvelles, ces événements s'inscrivent néanmoins dans une dynamique diffuse, mais désormais omniprésente, de cyberconflictualité internationale. Qu'il s'agisse d'espionnage industriel, de campagnes de désinformation, d'ingérences électorales ou encore de cybersabotage, de plus en plus d'États recourent au cyberespace pour faire agressivement valoir leurs intérêts.

> Le gouvernement fédéral à lui seul subissait chaque année près de 2 500 tentatives d'intrusions informatiques de la part d'acteurs étatiques étrangers.

Or, qu'il soit ou non partie prenante de cette escalade, le Canada en fait manifestement les frais : en 2017, le Centre de la sécurité des télécommunications révélait par exemple que le gouvernement fédéral à lui seul subissait chaque année près de 2 500 tentatives d'intrusions informatiques de la part d'acteurs étatiques étrangers. Si l'immense majorité de ces activités demeurent sans conséquence, une petite fraction donne occasionnellement lieu à des brèches importantes.

En s'appuyant sur des sources ouvertes

et sans prétendre à l'exhaustivité, l'analyse réalisée dans le cadre de ce rapport a recensé 51 cyberincidents à caractère géopolitique ayant directement touché le Canada dans les dix dernières années. En quoi consistent ces cyberincidents ? Comment évolue leur fréquence ? Que sait-on de leur origine ? La présente section entend proposer un rapide survol ainsi qu'un état des lieux de ces questions. Les informations présentées ici se basent sur les données du répertoire des cyberincidents canadiens récemment lancé par l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand. Elles s'appuient sur une méthodologie et une classification spécifiques établies par les auteurs et auteure de ce rapport ; nous encourageons les lectrices et lecteurs à en prendre connaissance dans la section « Comment ce rapport a-t-il été établi ? ».

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 section « Typologie »). La présente analyse se concentre sur les cyberincidents présentant un caractère géopolitique ou stratégique. En d'autres termes, les incidents traités ici ne relèvent pas de criminalité, mais plutôt 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, ou autres.

Les incidents discutés ici ont touché le Canada, qu'il s'agisse de ses pouvoirs publics, sa population, ses entreprises ou institutions de recherche, ou encore d'individus ou organisations internationales 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 ici remontent jusqu'à 2011.

Quel genre de cyberincidents sont les plus fréquents ?

Deux catégories de cyberincidents dominent largement le résultat du recensement effectué. Premièrement, il apparaît que la majorité des cyberincidents recensés au Canada (26 sur 51) relève de cyberespionnage. Cette catégorie recouvre plusieurs cas de figure différents. Il s'agit dans la plupart des cas de vol – ou de tentative de vol – de propriété intellectuelle visant des institutions de recherche ou des fleurons industriels canadiens. La campagne de cyberespionnage économique Cloud Hopper, attribuée à la Chine en 2018, en est un bon exemple (voir la section « cyberespionnage »). Il s'agit aussi souvent d'espionnage interétatique plus traditionnel, visant à collecter des informations gouvernementales confidentielles, à l'instar de la cyberintrusion de 2011 contre le Conseil du trésor du Canada.

Il apparaît que la majorité des cyberincidents recensés au Canada (26 sur 51) relève de cyberespionnage. Cette catégorie recouvre plusieurs cas de figure différents.

La seconde catégorie d'incidents les plus fréquemment observés relève de manipulations de l'information, soit « 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). On recense au moins 17 événements de ce type impliquant directement le Canada depuis 2017. Parmi eux figure par exemple la vague de *trolling* provenant d'Arabie saoudite survenue en août 2018 en marge d'une crise diplomatique entre Ottawa et Riyad. Dans plusieurs cas, ce type d'incidents relève d'efforts de longue haleine, échelonnés dans le temps. C'est par exemple le cas d'une campagne de désinformation sur Twitter décelée en 2018 et attribuée à la Russie, instrumentalisant une diversité de sujets, notamment la fusillade de la mosquée de Québec ou l'attaque à la voiture bélier d'Edmonton.

Comment leur fréquence évolue-t-elle ?

Les données établies dans le cadre de cette analyse (qui remontent jusqu'à 2011) esquissent une tendance à la hausse de la fréquence des cyberincidents. On peut essentiellement distinguer deux périodes. L'intervalle 2011-2015, d'une part, se caractérise par une moyenne de 2 cyberincidents par année. La période 2017-2020 voit ensuite s'instaurer une moyenne de 9 incidents par an. Il importe de souligner que cette augmentation est en bonne part générée par les actes de manipulation de l'information, dont on observe une hausse globale à travers le monde depuis 2016 (voir Bradshaw et al., 2021). Notons que dans le cas de campagnes d'espionnage ou de manipulation de l'information, les incidents s'étalent parfois sur plusieurs années, c'est alors l'année de commencement ou de publicisation qui est prise comme référence (voir la section « Comment ce rapport a-t-il été établi ? »).

D'où proviennent le plus souvent ces incidents ?

Il est relativement rare que la responsabilité d'un cyberincident à caractère géopolitique soit rigoureusement et publiquement attribuée à un acteur spécifique ou à un gouvernement étranger. Le présent rapport s'attache donc plutôt à l'origine géographique, par pays, des cyberincidents ayant touché le Canada. À ce chapitre, il apparaît que seuls quatre pays sont à l'origine de la grande majorité des cyberincidents recensés dans le cadre de cette analyse : la Russie (19 incidents), la Chine (12), l'Iran (7) et la Corée du Nord (5).

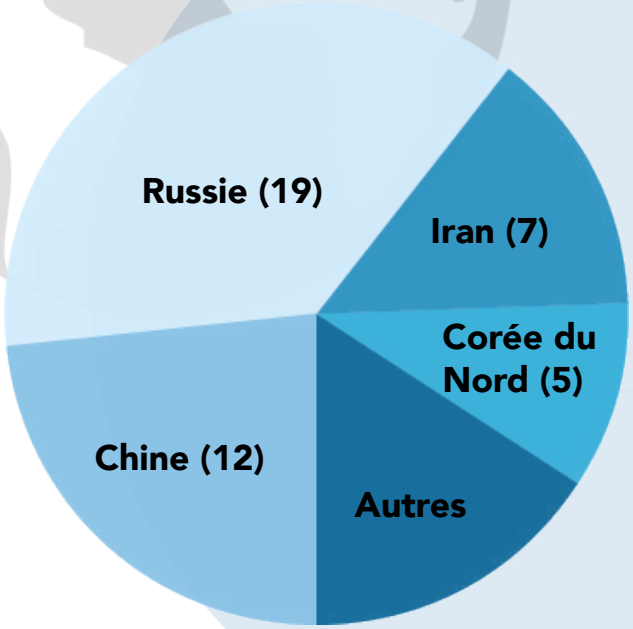
Il importe toutefois de noter les importantes disparités quant aux types d'incidents provenant de chaque pays. L'essentiel des incidents provenant de Russie relève d'actes de manipulation de l'information, tels que la diffusion sur le web de fausses nouvelles touchant le Canada par des médias basés en Russie. À l'inverse, la quasi-totalité des incidents provenant de Chine se rattache à des opérations de cyberespionnage, le plus souvent du vol de propriété intellectuelle. Il faut par ailleurs noter que six cas demeurent ambigus : il est difficile d'en établir l'origine géographique, et ils pourraient dans certains cas provenir du Canada.

La partie émergée de l'iceberg

Il est important de souligner que les données récoltées dans le cadre de la présente analyse ne prétendent pas à l'exhaustivité et ne représentent certainement pas l'ensemble des cyberincidents à caractère géopolitique ayant touché le Canada. Nombre d'incidents ne sont en effet jamais ou que très tardivement publicisés, pour diverses raisons. Les pouvoirs publics (au Canada et ailleurs) d'une part, préfèrent souvent garder confidentiels les incidents jugés sensibles, relevant par exemple du domaine de la défense, etc. D'autre part, le secteur privé, au-delà de certaines obligations légales, possède aussi de fortes incitations à ne pas publiciser l'existence de brèches informatiques, afin de préserver l'image et la crédibilité des entreprises touchées.

Il faut donc envisager que de nombreux incidents demeurent pour l'heure inconnus du grand public canadien et n'ont en conséquence pas été recensés dans le cadre de ce rapport, qui s'appuie sur des sources ouvertes. L'Observatoire des conflits multidimensionnels invite d'ailleurs les lectrices et lecteurs à porter à son attention tout cyberincident qui mériterait d'être ajouté au répertoire des cyberincidents canadiens, pour le rendre aussi exhaustif que possible.

Répartition des cyberincidents par pays



Trois tendances majeures

Au-delà des données brutes, quelles observations générales peut-on tirer des dix dernières années de cyberincidents ? La présente section vise à mettre en évidence trois tendances majeures se dégageant des incidents recensés ici : la prévalence importante du vol de propriété intellectuelle ; la nature encore très indirecte des actes de manipulation de l'information ; et l'incidence du statut de « pays hôte » du Canada.

CYBER ESPIONNAGE

LE SAVOIR-FAIRE CANADIEN AU CENTRE DES CONVOITISES

Alors que la majorité des cyberincidents à caractère géopolitique recensés relève de cyberespionnage, un premier constat important se dégage. Cet espionnage comprend évidemment la quête clandestine de secrets d'État, mais aussi et surtout le vol de propriété intellectuelle. Les pirates informatiques étrangers témoignent en effet d'une forte convoitise pour le savoir canadien, qu'il s'agisse de recherches et découvertes scientifiques, de secrets industriels ou économiques. Ainsi, en marge des organes gouvernementaux, ce sont les universités, les centres de recherche, les entreprises et autres organismes de recherche et développement qui figurent parmi les principales cibles des actes de cyberespionnage au Canada (comme dans bien d'autres pays). Certains domaines spécifiques semblent avoir été particulièrement ciblés dans les dernières années.

On remarque en premier lieu un fort intérêt pour les technologies à usage stratégique et militaire. En atteste notamment le piratage, en 2011, de l'Agence de recherche et déve-

loppement du ministère de la Défense nationale du Canada. Le phénomène semble être d'autant plus prononcé dans les domaines où le Canada détient un savoir-faire de pointe, comme l'aérospatiale, qui fait partie des secteurs concernés par le piratage du Centre national de recherches du Canada en 2014 (pour lire l'étude de cas, voir page 16). Une campagne plus récente, attribuée à la Chine en mars 2019, ayant touché plusieurs pays en plus du Canada, visait quant à elle à mettre la main sur des technologie militaires maritimes.

En second lieu, il apparaît que le cyberespionnage visant le savoir-faire canadien s'étend aussi largement à des secteurs technologiques non militaires, mais présentant néanmoins une valeur stratégique : l'énergie, l'industrie minière, l'informatique quantique ou encore les technologies de l'information.

Les pirates informatiques étrangers témoignent en effet d'une forte convoitise pour le savoir canadien, qu'il s'agisse de recherches et découvertes scientifiques, de secrets industriels ou économiques.

On peut citer à cet égard le cas du cyberespionnage de l'entreprise de télécommunications Nortel, publicisé en 2012 ou la campagne de cyberespionnage Cloud Hopper, publicisée en 2018, qui aurait touché plusieurs entreprises canadiennes.

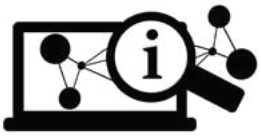
Plus récemment, du fait de la pandémie de COVID-19, c'est le secteur pharmaceutique et les institutions travaillant sur un vaccin contre le coronavirus qui ont fait figure de cible prioritaire. Au moins une entreprise pharmaceutique canadienne (dont le nom n'a pas été révélé) aurait été visée par une tentative de cyberespionnage, en avril 2020.

La crise du coronavirus démontre par ailleurs que des secteurs économiques en apparence secondaires, telle la recherche pharmaceutique, peuvent soudainement revêtir une valeur stratégique, et ainsi devenir la cible de puissances étrangères.

Le caractère géopolitique du vol de propriété intellectuelle à usage civil peut de prime abord ne pas paraître évident. Toutefois ce cyberespionnage est le plus souvent attribué à des pirates informatiques liés de près ou de loin à des gouvernements étrangers. Plusieurs États, dont notamment la Chine, abordent leur compétitivité économique et technologique comme un enjeu de sécurité nationale, que l'appareil d'État se doit de soutenir activement. La crise du coronavirus démontre par ailleurs que des secteurs économiques en apparence secondaires, telle la recherche pharmaceutique, peuvent soudainement revêtir une valeur stratégique, et ainsi devenir la cible de puissances étrangères.

DÉSINFORMATION

LE CANADA COMME CIBLE PLUTÔT QUE PUBLIC CIBLE



Si le second type de cyberincidents le plus fréquemment recensés dans le cadre de ce rapport sont les manipulations de l'information, il importe de souligner que ces dernières touchent le plus souvent le Canada de manière indirecte : nombre de campagnes de désinformation *parlent* du Canada, mais n'ont pas pour objectif premier d'influencer l'opinion publique canadienne. Il est donc utile de distinguer les différentes manipulations de l'information touchant le Canada selon leur sujet (de qui parle-t-on ?), leur public cible (qui veut-on désinformer ?) et leur objectif (à qui l'information doit-elle nuire ?).

On observe en premier lieu un ensemble, pour l'heure assez restreint, de manipulations de l'information parlant du Canada, visant une audience canadienne, le plus souvent dans le but de nuire à l'État canadien (par exemple en dénigrant certaines politiques publiques controversées). C'est notamment le cas d'une campagne de désinformation russe sur Twitter, publicisée en 2018, dans laquelle un certain nombre de tweets frauduleux critiquait les politiques migratoires du gouvernement Trudeau. On pourrait y ajouter la campagne de *trolling* orchestrée par l'Arabie saoudite à l'été 2018 en marge d'une crise diplomatique, dans laquelle certains tweets dénigraient le bilan du Canada en matière de droits des personnes autochtones. De telles opérations ont pour objectif global de porter atteinte à la légitimité des pouvoirs publics et de miner la cohésion sociale du Canada, mais demeurent jusqu'ici minoritaires parmi les cas recensés.

On distingue ensuite un second ensemble de manipulations de l'information, plus fréquentes, portant sur le Canada et visant à nuire à l'État canadien, mais n'étant pas spécifiquement destiné à une audience canadienne. C'est par exemple le cas de campagnes de désinformation russes menées en 2017 et 2018, qui relayaient de fausses nouvelles sur les troupes canadiennes basées en Lettonie et en Ukraine. Publiées en langue locale, celles-ci visaient à ternir l'image des Forces canadiennes auprès des populations lettones et ukrainiennes, afin de remettre en question le bien-fondé de leur présence (pour lire l'étude de cas, voir p. 20). De telles

manipulations de l'information apparaissent passablement courantes, même si elles ne visent pas à influencer l'opinion publique au Canada et retiennent donc moins l'attention. Néanmoins, elles portent atteinte à l'image du Canada à l'étranger et cherchent à infléchir certaines actions extérieures du Canada.

Enfin, un troisième ensemble de manipulations de l'information regroupe des actions plus ambiguës, évoquant le Canada, mais n'étant pas destiné à une audience canadienne, et ne cherchant (a priori) pas spécifiquement à nuire aux intérêts du Canada. C'est par exemple le cas de fausses rumeurs provenant de Russie au sujet d'actes de protestation au sein de la Ligue canadienne de football (CFL), disséminées en 2017 en marge de controverses raciales aux États-Unis. Figure également dans cet ensemble une campagne sur Facebook, attribuée à l'Iran en 2018, dont plusieurs contenus évoquaient le Canada, mais dont le propos visait les États-Unis et l'Arabie saoudite. De telles campagnes cherchent à attiser des controverses dans d'autres pays ou à l'encontre d'autres gouvernements, et ne semblent donc parler du Canada que de manière « accidentelle ».

UN PAYS HÔTE

LE CANADA ENTRE LE MARTEAU ET L'ENCLUME DES CYBER-OPÉRATIONS

Une troisième tendance importante tient au statut de « pays hôte » du Canada : plusieurs cyberincidents majeurs recensés dans le cadre de cette analyse ne visaient ni des acteurs proprement canadiens, ni à nuire spécifiquement aux intérêts du Canada, mais ont touché le Canada parce que celui-ci hébergeait des entités, des individus ou des infrastructures présentant une importance géopolitique ou stratégique. Ces incidents démontrent ainsi que les rivalités entre d'autres États, ou les tensions internes d'autres pays peuvent occasionnellement déborder de leur cadre et induire des effets collatéraux pour le Canada. On observe différents cas de figure en la matière.

En premier lieu, on peut penser aux cyberattaques orchestrées par des États contre des entités internationales, dont le siège se trouve être au Canada. C'est par exemple

le cas de l'Agence mondiale antidopage, basée à Montréal, frappée en 2016 par une cyberopération attribuée à la Russie, en représailles au scandale du dopage d'athlètes russes. La même année, l'Organisation de l'aviation civile internationale (OACI), elle aussi basée à Montréal, a été victime d'une importante cyberattaque provenant de Chine. L'opération semblait avoir pour objectifs d'obtenir des informations confidentielles détenues par l'organisation et de piéger les États membres utilisant les systèmes de l'OACI. Toutefois, elle aurait apparemment pu compromettre aussi des informations personnelles de citoyennes et citoyens canadiens traitant avec l'OACI (pour lire l'étude de cas, voir p. 24).

Les rivalités entre d'autres États, ou les tensions internes d'autres pays peuvent occasionnellement déborder de leur cadre et induire des effets collatéraux pour le Canada.

En second lieu, certains cyberincidents peuvent impliquer des résidentes ou résidents canadiens, ou des individus établis au Canada, dont les activités personnelles (notamment politiques) suscitent l'attention d'États étrangers. C'est par exemple le cas du dissident saoudien vivant au Québec Omar Abdulaziz, visé en 2017 par une opération de surveillance électronique clandestine du gouvernement saoudien. Une importante campagne de cyberespionnage baptisée Dark Caracal, révélée en 2018 et attribuée à l'État libanais, a entre autres touché le Canada et pourrait également avoir eu pour cible des activistes y résidant. De tels incidents mettent évidemment en jeu les droits des personnes concernées, et soulèvent plus largement des questions quant au respect de la souveraineté du Canada.

Enfin, on distingue un troisième cas de figure, jusqu'ici très rare : des incidents dont la cible finale est un pays tiers, mais qui touchent par voie de conséquence des infrastructures ou systèmes canadiens. En 2019, des infrastructures électriques canadiennes auraient par exemple fait l'objet de cyberintrusions provenant de Russie, dont le but premier était a priori d'évaluer les vulnérabilités du réseau électrique américain. Alors que les États-Unis et la Russie entretiennent une relation très conflictuelle dans le cyberespace, et que le Canada fournit une quantité importante d'électricité aux États-Unis, les infrastructures canadiennes font donc figure de cibles potentielles pour la Russie. S'il s'agit pour l'heure du seul incident de ce genre recensé dans le cadre de cette analyse, il illustre toutefois les risques pesant sur les infrastructures critiques informatisées reliant le Canada aux États-Unis, tels les réseaux électriques ou les lignes d'oléoducs.
À ce titre, la section suivante présente des études de cas illustrant la manière dont les cyberincidents peuvent affecter le Canada. Ils sont issus des nombreux cas recensés dans notre répertoire des cyberincidents canadiens, et fournissent des exemples concrets et détaillés des trois tendances majeures présentées ci-dessus.

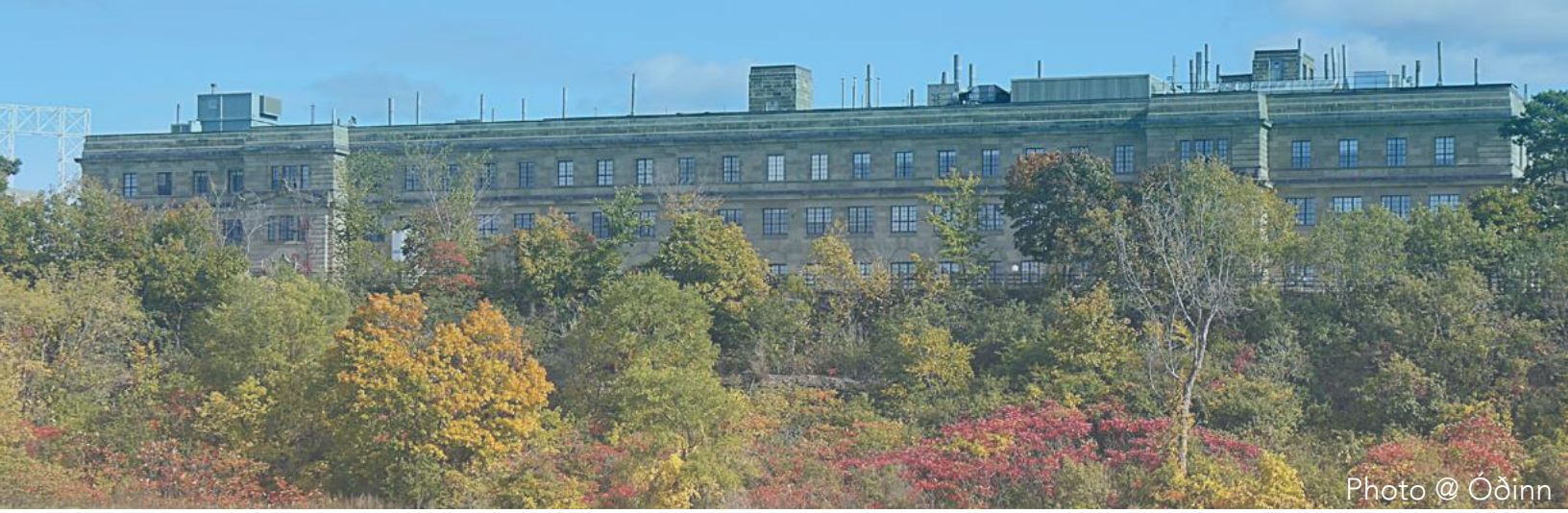


Photo @ Óðinn

Les technologies de pointe dans le collimateur chinois : le piratage du CNRC en 2014

Le 23 juillet 2014, le gouvernement Harper affirmait, par voie de communiqué, que le Conseil national de recherches du Canada (CNRC) avait été victime d'une opération de cyberespionnage d'envergure commanditée par l'État chinois. Ironie du sort ? Cette cyberopération survenait au moment où le CNRC travaillait à l'élaboration d'un système de communication « inviolable », capable justement de prévenir de telles activités clandestines.

Juillet 2014. Les relations entre Ottawa et Pékin sont pour le moins tendues. Le gouvernement canadien tarde à signer un important traité bilatéral en matière d'investissements étrangers avec la Chine (APIE), et vient d'imposer de nouvelles sanctions économiques contre des sociétés d'État chinoises. Dans le but d'apaiser les tensions et de préparer le terrain à une éventuelle visite du premier ministre Stephen Harper à Pékin, John Baird, alors ministre des Affaires étrangères du Canada, se rend en Chine pour y rencontrer son homologue. Or, l'effort diplomatique s'avère rapidement vain, car le Secrétariat du Conseil du trésor sonne l'alerte : l'État chinois vient d'orchestrer une opération de cyberespionnage « hautement sophistiquée » visant le Conseil national de recherches du Canada, l'épine dorsale canadienne en matière d'innovation et de recherche et développement (R&D).

La vulnérabilité des systèmes informatiques canadiens

D'après le bilan officiel de l'événement, le gouvernement canadien attribue la faute à un acteur hostile parrainé par l'État chinois,

lequel a ouvert une brèche dans les réseaux du CNRC par l'entremise d'un logiciel malveillant contenu dans un courriel. Les pirates auraient vraisemblablement pu se procurer non seulement des renseignements sensibles sur des projets et programmes de recherche en cours, mais aussi des données personnelles d'employées et d'employés du CNRC. L'intrusion, une fois détectée, a aussitôt conduit à la fermeture du système informatique du Conseil. Le prix à payer ? Une faramineuse facture de 32,5 millions de dollars, acquittée par le gouvernement fédéral afin de rétablir les réseaux de l'institution. La Chine, de son côté, a nié les allégations à son égard, affirmant que le Canada l'accusait sans la moindre preuve.

Le prix à payer ? Une faramineuse facture de 32,5 millions de dollars, acquittée par le gouvernement fédéral afin de rétablir les réseaux de l'institution.

L'événement soulève plusieurs interrogations quant à l'efficacité de la protection des systèmes vitaux canadiens, alors que des cyberattaques survenues en 2011 (elles aussi attribuées à la Chine) contre le Conseil du trésor et le ministère des Finances sont toujours fraiches dans les mémoires. En 2012, le vérificateur général, Michael Ferguson, soulignait déjà dans un rapport le retard du Canada en matière de sécurité des réseaux informatiques essentiels et appelait à la création d'un réseau interministériel visant le partage de renseignements nécessaires en la matière.

Cyberdéfense : de la cryptographie standard à la cryptographie quantique

La véritable raison de l'intrusion des pirates chinois dans les réseaux du CNRC reste nébuleuse. Des hypothèses se dégagent toutefois : au moment de la cyberattaque, les chercheures et chercheurs du Conseil national travaillaient sur différentes technologies à valeur stratégique, notamment dans le domaine des satellites et des OGM, mais également de l'informatique quantique. Ce secteur, au cœur des convoitises, s'attache au développement de calculateurs hypersophistiqués, capables de réaliser une série de calculs totalement hors de portée des ordinateurs standards, même les plus puissants.

Or, selon toute vraisemblance, la cyberattaque contre le CNRC ciblait ce secteur crucial. En effet, selon le Rapport sur le symposium et l'atelier de Quantique Canada, une étude de 2017 menée par la firme de consultation américaine McKinsey & Company soutenait que le Canada occupait le cinquième rang mondial en termes d'investissement dans la science quantique, se classait premier en matière d'informatique quantique et arrivait premier parmi les pays membres du G7 par rapport aux dépenses par habitant destinées à la recherche. Figurant ainsi parmi les chefs de file dans le domaine, le Canada éveille naturellement la curiosité de ses concurrents.

Pourquoi les systèmes quantiques suscitent-ils tant d'intérêt ? Car cette technologie photonique semble destinée à bouleverser dans un avenir proche de nombreux domaines scientifiques, allant du médical à l'aérospatiale en passant par les télécommunications, poussant nombre de spécialistes à annoncer l'avènement prochain d'une « révolution quantique »[1].

Une étude de 2017 soutenait que le Canada occupait le cinquième rang mondial en termes d'investissement dans la science quantique, se classait premier en matière d'informatique quantique et arrivait premier parmi les pays membres du G7 par rapport aux dépenses par habitant destinées à la recherche.

Ce bouleversement fait cependant planer son lot de menaces. En effet, la puissance de déchiffrage promise par les calculateurs quantiques rendra selon toute vraisemblance la plupart des mécanismes de cryptographie actuels désuets. Il deviendra donc très difficile de garantir l'intégrité de plusieurs infrastructures critiques et la confidentialité de nombreuses communications. Il faudra toutefois attendre 2030 pour que ces supercalculateurs atteignent une puissance susceptible de poser une menace immédiate.

D'un autre côté, l'année 2030 n'est pas une échéance lointaine. Sachant que les processus de R&D s'échelonnent normalement sur une longue période, certains États ont déjà redoublé d'efforts pour bénéficier de la technologie avant les autres. À cet effet, la Chine a déjà lancé en orbite son premier satellite quantique (2016), afin de mettre sur pied le premier réseau de communication quantique intégré au monde[2]. L'agence canadienne Recherche et développement pour la défense, pour sa part, vient d'élaborer une stratégie en matière de science et technologie pour conserver son statut de leader dans le domaine quantique, et permettre au ministère de la Défense ainsi qu'aux Forces armées canadiennes de préserver un certain avantage stratégique.

Technologies de pointe : une urgence pour Pékin

Bien qu'emblématique, l'incident du CNRC est un cas parmi d'autres d'incidents similaires survenus ces vingt dernières années au Canada. La Chine, particulièrement, a été

1 À la différence d'un ordinateur classique, un calculateur quantique ne fonctionne pas en fonction de bits (suite binaire de 0 ou 1), mais de qubits (suite infinie de combinaisons superposables de 0 et 1, y compris les décimales). Un système qui « réfléchit » de la sorte permet de résoudre simultanément plusieurs équations, calculs et opérations très rapidement, depuis une masse d'informations bien plus considérable qu'à l'ordinaire. En matière de cybersécurité, un système de communication quantique laisse ainsi entrevoir un procédé de cryptographie sans faille assurant le transfert sécurisé des flux d'informations. En effet, les systèmes de communication quantique s'appuient sur les propriétés physiques des photons plutôt que sur le code informatique. Par conséquent, le photon utilisé pour communiquer ne peut être intercepté ni décodé aisément entre un émetteur et un récepteur sans les clés de cryptage.

2 Le système intégré se compose de plus de 2000 km de fibre optique dorsale (au sol) et deux liaisons sol-satellite, permettant de couvrir une vaste part du territoire chinois.

pointée du doigt à de nombreuses reprises pour avoir espionné des secteurs considérés comme stratégiques : l'affaire Nortel, révélée en 2012, portait sur des matériaux et logiciels pour les réseaux de télécommunication ; le scandale impliquant le professeur de l'Université McGill Ishiang Shih, en 2018, concernait les circuits intégrés monolithiques hyperfréquence ; la même année, l'affaire entourant l'entreprise LinkOcean portait quant à elle sur des technologies de reconnaissance navale (hydrophones).

La Chine déploie fréquemment son arsenal dédié à l'espionnage dans le but de réduire son retard technologique, d'accélérer sa stratégie de découplage commercial, de nourrir son complexe militaro-industriel ou de court-circuiter sa dépendance à l'égard de l'Occident en matière technologique (par exemple vis-à-vis des semi-conducteurs). Dépendance qu'elle assume d'ailleurs toujours difficilement — mais ouvertement — comme en témoignait une déclaration de Xi Jinping en 2016 : « Notre dépendance aux technologies de base est notre problème caché le plus grave. »

« La géopolitique s'intéresse à vous »

Dans cette impitoyable course aux nouvelles technologies, principalement menée par la Chine mais aussi par d'autres États, le Canada n'est pas épargné et est victime de nombreux croche-pieds clandestins. En 2013 déjà, le Advanced Threat Report publié par l'entreprise de sécurité informatique américaine FireEye indiquait que le Canada était le troisième pays le plus ciblé par les attaques informatiques de type *advanced persistent threat* (APT) suivant, dans l'ordre, les États-Unis et la Corée du Sud[3]. Qui plus est, selon le Centre de la sécurité des télécommunications, entre 2013 et 2015, 2 500 cyberactivités commanditées par des États ont été détectées par le gouvernement canadien, soit plus de 50 par semaine.

Plus récemment, en février 2021, le directeur du Service canadien du renseignement de sécurité, David Vigneault, sommait les chefs d'entreprise et les universitaires canadiens de redoubler de vigilance vis-à-vis de l'espionnage, les prévenant que s'ils ne s'intéressent peut-être pas à la géopolitique, « la géopolitique s'intéresse à [eux] ».

> Entre 2013 et 2015, 2500 cyberactivités commanditées par des États ont été détectées par le gouvernement canadien

L'espionnage n'est certes pas nouveau, mais il représente aujourd'hui une menace omniprésente dans tout environnement stratégique où réside la notion de concurrence. Bien consciente de cela, la Chine exploite largement cette nouvelle réalité, et rien ne semble pouvoir, pour le moment, freiner ses ambitions.

3 Le terme *advanced persistent threat* désigne globalement des cyberattaques sophistiquées et furtives (« avancées »), durant lesquelles les auteurs établissent une présence de longue durée (« persistante ») dans un système informatique visé. L'abréviation fait également souvent référence à des groupes de pirates informatiques financés par un État, poursuivant des objectifs économiques et/ou géopolitiques.

Photo @ U.S. Army Europe

Tir groupé de fausses nouvelles contre les Forces canadiennes en Lettonie

Depuis 2017, les troupes canadiennes déployées en Lettonie sous l'égide de l'OTAN sont l'objet de campagnes de désinformation récurrentes et soutenues. Orchestrées par la Russie, celles-ci visent essentiellement à ternir l'image du contingent auprès de la population locale. De telles opérations peuvent contribuer à compliquer la collaboration, voire attiser les tensions, entre le Canada et des pays alliés.

De par son potentiel militaire relativement modeste, sa présence limitée à l'étranger et sa politique internationale axée sur le multilatéralisme, le Canada ne devrait a priori pas être le premier pays visé par les campagnes de désinformation de puissances étrangères. Pourtant, vu notamment son appartenance à l'OTAN et sa participation aux activités de l'organisation, le Canada fait fréquemment l'objet de tels actes, qui visent généralement à ternir son image internationale. Depuis 2017, les troupes canadiennes stationnées en Lettonie sous l'égide de l'Alliance atlantique sont ainsi la cible de campagnes de désinformation récurrentes et soutenues.

Déployé dans le cadre de l'opération Reassurance, le contingent canadien (l'un des plus importants détachés à l'étranger) compte 450 soldats, une frégate et six avions de chasse CF-18. Face aux quelque 50 000 soldats russes stationnés de l'autre côté de la frontière lettonne, ils ne représentent qu'une modeste contribution et sont là en bonne partie à des fins de dissuasion,

d'exercices, d'instruction et de modernisation des installations locales. Ceci étant, depuis leur déploiement en juin 2017, les militaires canadiens sont visés par des campagnes de manipulation de l'information de la part de la Russie, qui cherche à les discréditer et faire désavouer leur présence.

Un feu roulant bien orchestré

En juin 2017, quatre jours avant le débarquement des troupes canadiennes en Lettonie, une fausse nouvelle concernant les soldats canadiens en poste en Ukraine est publiée en ligne dans trois médias russes. Selon celle-ci, 12 membres des forces spéciales canadiennes viennent d'être abattus dans la région du Donbass, où se déroule une guerre civile entre forces ukrainiennes et séparatistes prorusses ; pourtant, les troupes canadiennes en Ukraine n'effectuent que des missions de formation et sont stationnées loin du Donbass. Les publications frauduleuses étayent leurs propos avec des photos de soldats canadiens portant un cercueil, des clichés datant de plusieurs années, et pris en Irak. Disséminés sur le web russophone, ces contenus sèment le doute sur le bien-fondé de la présence militaire canadienne à l'étranger : est-elle réellement pacifique et bien intentionnée ? Est-elle souhaitable en Lettonie ?

Alors que le contingent canadien s'apprête à poser le pied dans ce pays balte, une autre fausse nouvelle fait son apparition sur un site d'information letton en langue russe. On y affirme que Russel Williams, ancien colonel de l'Aviation royale canadienne condamné à vie pour une série de meurtres, commande les troupes désormais stationnées à la base d'Adazi. Des photos le montrant en sous-vêtements féminins, qui ont fait surface lors de son procès, servent à dénoncer une prétendue déviance sexuelle au sein de l'Armée canadienne. Une autre fausse nouvelle affirme peu après que des soldats de l'OTAN circulent avec des armes chargées à travers Riga, la capitale lettonne, mettant en péril la population locale.

Depuis leur déploiement en juin 2017, les militaires canadiens sont visés par des campagnes de manipulation de l'information de la part de la Russie, qui cherche à les discréditer et faire désavouer leur présence.

Les spécialistes lettons de la propagande russe y voient la preuve que le Canada subit désormais le même traitement que celui réservé par Moscou aux autres pays membres de l'OTAN déployés dans les anciennes républiques soviétiques. En effet, la désinformation est une réalité quotidienne pour les soldats allemands stationnés en Lituanie et les soldats britanniques en Estonie. Les Forces armées canadiennes doivent rapidement apprendre à composer avec un terrain informationnel miné. Une douzaine de soldats sont immédiatement affectés à des tâches de veille pour identifier les campagnes de propagande les visant.

Photo @Diego Delso

La fin d'une bataille,
mais pas de la guerre

Au courant de l'automne 2017, un nombre impressionnant de fausses nouvelles fait surface, toujours sur des sites d'information russophones. Parmi celles-ci, une allégation, affirmant que les soldats canadiens seraient logés dans des appartements de luxe aux frais des contribuables lettons, est rapidement démentie. D'autres histoires accompagnées de photos fallacieuses mettent en scène des soldats achetant de grandes quantités d'alcool ou des sites d'entraînement en forêt jonchés de déchets. Or, les images représentent en vérité des soldats d'autres pays dans d'autres théâtres d'opérations, ou simplement des photos hors contexte. Le but de ces diverses opérations semble toujours le même : attiser la colère des populations locales en présentant les soldats canadiens comme des parasites ou des fauteurs de trouble.

La vague de manipulation de l'information qui vise les Forces armées canadiennes à leur arrivée en Lettonie prend progressivement fin vers l'été 2018. Les Forces canadiennes en ont tiré des leçons importantes. Les soldats sont maintenant sensibilisés au phénomène de la désinformation, et ils organisent des évènements publics pour tisser des liens avec les populations locales et leur permettre d'observer et de mieux comprendre la nature des opérations canadiennes. Les campagnes russes n'ont toutefois pas complètement cessé : en avril 2020, plusieurs contenus fallacieux accusent le contingent canadien de propager la COVID-19 et présentent la

base lettonne d'Adazi comme un important foyer de cas actifs. La fausse nouvelle émerge au moment même où les soldats canadiens terminent les préparatifs pour une simulation militaire de l'OTAN, l'opération Steele Crescendo, qui doit amener ceux-ci à opérer hors des limites de leur base. Les autorités lettonnes démentent rapidement l'information, mais le mal est déjà fait.

En avril 2020, plusieurs contenus fallacieux accusent le contingent canadien de propager la COVID-19.

Petits coups de pied, mais fourmilière agitée

De prime abord, de telles informations peuvent sembler inoffensives, mais elles sont néanmoins prises au sérieux par les autorités canadiennes. La Lettonie est un pays divisé entre une population tournée vers l'Occident et une minorité russophone culturellement et politiquement plus proche de Moscou. En 2017, le ministre de la Défense Harjit Sajjan partage donc sa crainte que les troupes canadiennes puissent être la cible de violences de la part de groupuscules prorusses harangués par Moscou. En 2014, des heurts isolés entre Lettons et soldats de l'OTAN ont par exemple été instrumentalisés par des médias russes pour attiser davantage les tensions.

On voit donc que la présence des troupes de l'OTAN en Lettonie soulève les passions. Les autorités de la république balte sont inquiètes des visées territoriales de son voisin russe et la majorité de la population voit d'un bon oeil la présence de l'Alliance atlantique. La communauté russophone de l'est du pays, qui représente environ 37 % de la population, a toutefois une vision différente : l'OTAN est davantage perçue comme une force d'occupation. Cette minorité se montre passablement favorable à l'annexion de la Crimée par la Russie en 2014, et à la politique de Vladimir Poutine envisageant l'usage de la force pour défendre les populations russophones d'Europe. Riga craint ainsi que la Russie instrumentalise les populations russophones de Lettonie pour déstabiliser le pays, peut-être en vue d'une intrusion territoriale. Ce type de stratégie a d'ailleurs précédé les interventions militaires russes en Géorgie en 2008, et en Crimée en 2014.

En plus de ces enjeux géopolitiques régionaux, les campagnes de désinformation visant le contingent canadien en Lettonie soulèvent d'autres défis pour Ottawa. La campagne de désinformation de 2017, par exemple, s'est déroulée à moins d'un an d'élections parlementaires lettonnes (une « coïncidence » récurrente dans le cadre de campagnes de désinformation). En semant la controverse sur la présence des troupes canadiennes au pays, ces campagnes cherchent, en outre, à faire de cette question un enjeu électoral et à forcer la classe politique locale à prendre position. De telles opérations, en plus d'influencer les opinions publiques des pays en question, peuvent donc nuire à la collaboration entre le Canada et des gouvernements alliés.


Photo @ Jason Thibault

Internationale mais basée à Montréal : la cyberattaque contre l'OACI en 2016

L'Organisation de l'aviation civile internationale, dont le siège se trouve à Montréal, se présente comme un organe des Nations unies plus technique que politique. Tout porte donc à croire qu'une telle instance n'est pas une cible prioritaire du cyberespionnage interétatique. Néanmoins, en 2016, elle est victime de la pire cyberattaque de son histoire, mettant potentiellement à risque les données personnelles de Canadiennes et Canadiens.

Siégeant à Montréal, l'Organisation de l'aviation civile internationale (OACI) est une institution spécialisée des Nations unies (ONU) où coopèrent chaque jour 193 pays membres. Créée en 1944, elle est chargée d'établir le cadre réglementaire de la sécurité de l'aviation civile internationale. Elle met en œuvre le transport aérien de personnes et de biens au niveau mondial, et a un fort impact en ce qui concerne l'élaboration des politiques et des normes internationales pour la standardisation du transport aéronautique. Elle compte entre 800 et 1000 fonctionnaires internationaux dont la plupart sont basés à Montréal.

Organisation internationale éminemment technique, elle ne présente a priori pas d'intérêt stratégique particulier pour des pirates informatiques à la solde d'un État. En 2016 toutefois, l'OACI est avertie que deux de ses serveurs ont fait l'objet d'une intrusion. Loin de s'en douter sur le moment, elle était sur le point de subir la cyberattaque la plus grave de son histoire.

Un « point d'eau » contaminé

L'alerte est lancée le 22 novembre 2016 par un analyste en cyberintelligence travaillant pour l'entreprise américaine Lockheed Martin, spécialisée en défense et sécurité. Ne pesant point ses mots, il qualifie l'attaque de « menace importante pour l'industrie aéronautique ». Cette cyberattaque vise deux des serveurs de l'organisation internationale, et met à risque les nombreux utilisateurs et institutions transitant chaque heure sur la plateforme digitale de l'OACI. Un site du gouvernement turc a aussi été infecté, ce qui a trahi l'existence de la cyberattaque.

La brèche étant désormais détectable, l'enquête est transférée à l'interne pour permettre une analyse du cas par la firme SecureWorks, une entreprise américaine spécialisée en cybersécurité employée par l'ONU. L'analyse se révèle préoccupante ; les pirates semblent s'être introduits dans deux serveurs de messageries de l'organisation et y hibernent depuis une longue période. Technique bien connue des analystes en cybersécurité, les pirates sont passés sous les radars grâce à une cyberattaque de type watering hole.

Comme son nom l'indique, une attaque par « point d'eau » consiste à piéger le système d'un premier utilisateur, afin d'infecter ensuite les visiteurs ou utilisateurs externes de ce système (qui viennent « s'abreuver » au point d'eau contaminé). Plus précisément, cela revient à placer un *malware* dans un site, généralement en dehors des protections

Photo @Jeangagnon

de sécurité relatives à l'entreprise, qui sera visité par les personnes visées. Les victimes s'infectent alors d'elles-mêmes et propagent le virus plus loin. Ces attaques sont complexes : les sites web infectés sont généralement des entités de confiance, des partenaires commerciaux par exemple, dont la sécurité des serveurs n'est pas sujette à suspicion.

Comme son nom l'indique, une attaque par « point d'eau » consiste à piéger le système d'un premier utilisateur, afin d'infecter ensuite les visiteurs ou utilisateurs externes de ce système (qui viennent « s'abreuver » au point d'eau contaminé).

Des attaquants armés de patience

Bien que connu, ce type d'attaque n'est pas particulièrement fréquent, notamment parce qu'il exige énormément de patience de la part des pirates informatiques. Les attaques par *watering hole* constituent toutefois une menace importante puisqu'elles sont difficiles à détecter. Un autre problème majeur dans la gestion de ce type de cyberattaque touche à la formation des employés : il est facile de former des employés à reconnaître et à éviter les courriels d'*hameçonnage*[1], mais il n'y a aucun moyen pour un utilisateur ordinaire d'identifier un site web compromis sans l'aide d'un outil conçu à cet effet.

C'est ce qui semble s'être produit lors de la cyberattaque envers l'OACI, dont les serveurs de messageries ont servi de point d'eau principal. Les pirates se sont infiltrés discrètement et se sont tapis dans les serveurs pendant des mois avant qu'on ne les identifie. Générateur d'un abondant trafic internet en provenance de nombreux pays, l'OACI était la cible idéale d'une attaque par point d'eau. Selon toute vraisemblance, le but de l'infiltration était le cyberespionnage. L'OACI représentait ainsi un choix logique notamment puisqu'elle sert de porte d'entrée vers d'autres acteurs de l'industrie aérospatiale, ce qui permettait aux pirates d'accéder à une plus grande quantité de données à des fins de vol de propriété intellectuelle.

Un schéma habituel pour Emissary Panda

À qui convient-il d'attribuer cette cyberattaque ? Une analyse préliminaire effectuée par la firme SecureWorks conclut qu'elle est imputable au groupe de pirates informatiques chinois Emissary Panda. Actif depuis 2010 et aussi connu sous les noms d'APT27, Lucky-Mouse, Threat Group 3390 et Bronze Union, le groupe n'en était donc pas à ses premières armes. Par le passé, Emissary Panda avait déjà réalisé de grandes opérations de vol de propriété intellectuelle, en ciblant des organisations importantes en Amérique du Nord et

1 L'hameçonnage est une technique utilisée par des fraudeurs informatiques pour obtenir des accès ou des renseignements personnels à des fins d'usurpation d'identité ou pour pénétrer un système informatique. Il se présente le plus souvent sous la forme de courriels frauduleux cherchant à duper l'utilisateur en imitant un courriel légitime.

du Sud, en Europe et au Moyen-Orient. On sait, en outre, que ce groupe vise régulièrement les secteurs de l'aérospatiale, de la défense, de la technologie, de l'énergie et de la finance.

Un rapport de SecureWorks affirme qu'Emissary Panda se situe sur le territoire de la République populaire de Chine, et il apparaît plausible qu'il soit subventionné et cautionné par le gouvernement chinois. Le groupe se distingue par sa tendance à compromettre les serveurs Microsoft Exchange notamment par l'utilisation de *backdoors*[2] et d'informations d'identification. Il est aussi réputé pour ses campagnes de cyberespionnage de longue haleine où il passe une longue période dans un serveur avant d'en exfiltrer les données, qui fut le schéma suivi dans le cas de l'OACI. Le groupe utilise ce laps de temps pour trouver d'autres points d'accès, apprendre comment le réseau est structuré et identifier les données importantes.

Une cyberattaque de longue haleine et des dégâts encore méconnus

Bien que l'OACI n'ait pas confirmé précisément ce qui a été dérobé, il est probable que la cyberattaque ait compromis un certain nombre de documents d'aviation couramment utilisés sur son site web, permettant ainsi aux pirates d'accéder à un grand nombre d'organisations aériennes et gouvernementales à travers le monde. De nouveaux détails sur l'attaque ont par ailleurs fait surface en 2019, suggérant que les comptes des serveurs de messagerie ainsi que les comptes des administrateurs de domaines et de systèmes aient été touchés. La manœuvre aurait permis aux pirates d'accéder aux identifiants et aux mots de passe de plus de 2000 utilisateurs et utilisatrices du système.

Fait notable pour le Canada : les pirates auraient également eu accès aux dossiers personnels des employées et employés, aux dossiers médicaux des patients ayant utilisé la clinique du siège de l'OACI, aux relevés de transactions financières d'entreprises traitant avec l'OACI, ainsi qu'aux informations personnelles de toute personne ayant visité physiquement les bâtiments de l'OACI à Montréal.

La manœuvre aurait permis aux pirates d'accéder aux identifiants et aux mots de passe de plus de 2000 utilisateurs et utilisatrices du système.

Il est donc plausible d'imaginer que certaines données de résidentes et résidents canadiens aient été compromises durant l'attaque. L'incident montre donc l'importance du statut de « pays hôte » du Canada en termes de cybersécurité : bien que visant une organisation internationale, une cyberattaque peut en parallèle induire des effets collatéraux pour le Canada.

2 Une backdoor, ou porte dérobée en français, est une fonctionnalité offrant un accès clandestin à un système informatique, à l'insu de son utilisateur légitime.

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 origine 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.

Pour aller plus loin...

Les « chroniques des nouvelles conflictualités » de l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand analysent, sur une base bimensuelle, des événements d'actualité se rapportant aux mutations stratégiques contemporaines : cybersécurité, désinformation, ingérences électorales ou encore géoéconomie.

Autres bases de données et ressources en ligne sur les cyberincidents :

Cyber Operations Tracker : Très complète, cette base de données présente de manière habile une vaste part des cyberopérations étatiques ayant eu lieu à travers le monde depuis 2005. Elle est entretenue par le Digital and Cyberspace Policy Program du *think tank* américain Council on Foreign Relations. Sa méthodologie a inspiré celle du répertoire des cyberincidents canadiens.
https://www.cfr.org/cyber-operations/

Significant Cyber Incidents : Se présentant davantage comme une frise chronologique que comme une base de données, ce registre en ligne constitue néanmoins une archive très utile des cyberincidents majeurs ayant eu lieu depuis 2006. Il est entretenu par le *think tank* américain Center for Strategic and International Studies.
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Live Cyber Threat Map : De nombreuses firmes de cybersécurité entretiennent des cartes en temps réel des cyberattaques (ou tentatives de) ayant lieu à travers le monde. Celle de l'entreprise ThreatCloud n'est pas nécessairement la plus avancée ou la plus détaillée, mais elle s'avère toutefois très complète et intuitive pour observer instantanément les coups qui s'échangent à travers l'internet global.
https://threatmap.checkpoint.com/

Quelques médias de référence sur les enjeux cyber :

Wired : La section « sécurité » du célèbre média en ligne américain offre une couverture de grande qualité de l'actualité cyber américaine mais aussi internationale, par le biais d'articles de fond et d'enquêtes poussées mettant à contribution parmi les meilleures plumes du domaine.
https://www.wired.com/category/security/

CyberScoop : Comparable à une « agence de presse de la cybersécurité », CyberScoop offre au lecteur un traitement rapide, accessible et rigoureux de l'actualité cyber, qu'il s'agisse de sécurité internationale, de cybercriminalité, ou de l'élaboration des politiques de cybersécurité. https://www.cyberscoop.com/

IT World Canada : Très prisé des professionnelles et professionnels des technologies de l'information, ce petit média spécialisé offre un bon traitement de l'actualité cyber sous un angle spécifiquement canadien.
https://www.itworldcanada.com/

Vygl le balado : Cette baladodiffusion produite par l'agence de cybersécurité québécoise Vygl offre un survol régulier, à la fois pointu et décontracté, de l'actualité en matière de cybersécurité. L'une des rares du genre en français. https://vyglbalado.libsyn.com/

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