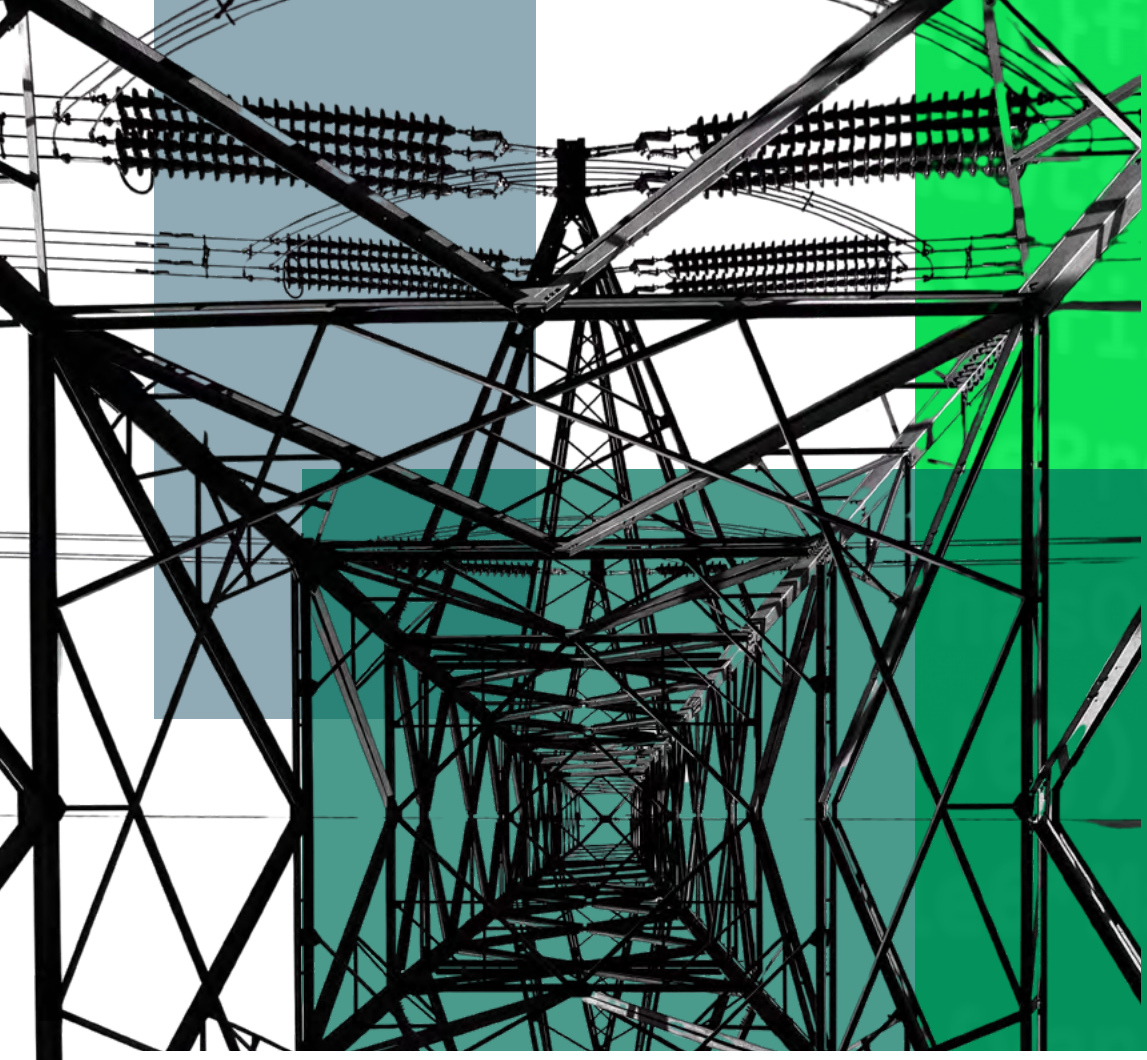


UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

CYBERINCIDENTS GÉOPOLITIQUES AU CANADA

ÉTAT DES LIEUX 2025

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, et notamment l'effet des technologies numériques sur celles-ci. 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 citoyen-ne-s.

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, la gestion américaine de la cyberconflictualité, les effets de la compétition géoéconomique sino-américaine sur les relations entre le Canada et les États-Unis, et la politique géoéconomique des États-Unis à l'égard du Canada.

Alexis Rapin est chercheur en résidence à l'Observatoire des conflits multidimensionnels. Il travaille notamment sur les transformations de la conflictualité, 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 docteur en science politique, diplômé de 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, axés 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.

Simon Hogue est professeur au Département de science politique de l'UQAM et chercheur en résidence à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand. Ses recherches, à l'intersection des études de la technologie, de la culture et du pouvoir, se penchent sur la sécurité et la guerre, le contrôle social et la démocratie dans les sociétés numérisées. Ses plus récents textes portent sur l'utilisation des technologies numériques dans la guerre en Ukraine et la résistance numérique.

Marie Lamensch est la chargée des affaires mondiales au Centre de Montréal sur la sécurité globale et membre associée à l'Observatoire de géopolitique et à l'Observatoire des conflits multidimensionnels de la Chaire Raoul Dandurand. Ses intérêts de recherche portent sur la sécurité internationale et les droits de la personne, la prévention des atrocités de masse, la désinformation genrée, l'extrémisme violent et la haine en ligne, les technologies émergentes, les répressions transnationales et l'autoritarisme numérique.

Laurence Michalski est candidate à la maîtrise en science politique à l'UQAM et chercheure en résidence à l'Observatoire des conflits multidimensionnels. Ses recherches portent principalement sur les services de renseignement américains. Elle s'intéresse également aux questions géoéconomiques qui marquent les relations entre les États-Unis, le Canada et la Chine.

Fanny Tan est chercheure en résidence 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.

Charlotte Vincent est stagiaire à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand. Finissante au baccalauréat en études internationales à l'Université de Montréal, elle s'intéresse aux enjeux de la sécurité internationale et aux questions de maintien de la paix.

2024 QUELQUES INCIDENTS MARQUANTS

JANVIER

BRÈCHE DE DONNÉES À AFFAIRES MONDIALES CANADA

Affaires mondiales Canada annonce avoir été victime d'une importante brèche de données. Celle-ci aurait notamment touché le service VPN du ministère et permis un accès non autorisé aux courriels et aux informations personnelles de certains employé-e-s. Aucun détail n'est livré sur les acteurs suspectés d'être à l'origine de la brèche.

MARS

CYBERINCIDENT AU CANAFE

Le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) annonce avoir été victime d'un cyberincident. Le système permettant de soumettre des déclarations d'opérations douteuses est mis temporairement hors ligne dans le cadre des mesures de remédiation. Aucun détail n'est livré sur la nature exacte ou l'origine de l'incident.

MAI

CAMPAGNE D'INFLUENCE PRO-ISRAÉLIENNE PAR LA FIRME STOIC

Une campagne d'influence visant à disséminer du contenu pro-israélien au sujet de la guerre à Gaza est repérée sur les plateformes Meta et X. Elle est attribuée à une firme israélienne de consulting électoral nommée STOIC et aurait touché des audiences au Canada, mais aussi aux États-Unis et en Israël, en exploitant entre autres des outils d'intelligence artificielle générative.

SEPTEMBRE

CONTENUS DE RRN VISANT JUSTIN TRUDEAU

Une enquête révèle que Reliable Recent News (RRN), un faux site web d'actualité lié à la Russie, a récemment publié plusieurs contenus relatifs à la politique canadienne. Ces publications visaient notamment à amoindrir le soutien au premier ministre Justin Trudeau. RRN est l'une des plateformes attribuées à un vaste réseau de désinformation russe baptisé Doppelganger.

OCTOBRE

ACTIVITÉS DE RECONNAISSANCE CHINOISES CONTRE DES SYSTÈMES CANADIENS

Le Centre canadien pour la cybersécurité révèle qu'un groupe de pirates lié à la Chine a conduit des activités de reconnaissance « à grande échelle » contre de nombreuses entités canadiennes au courant de l'année 2024. Parmi les cibles figurent notamment des ministères et partis politiques fédéraux, la Chambre des communes, le Sénat ou encore des acteurs de la société civile.

DÉCEMBRE

CAMPAGNE D'ESPIONNAGE VISANT DES ACTIVISTES TIBÉTAINS ET OUÏGHOURS

Un rapport révèle qu'un groupe de pirates, baptisé Earth Minotaur et vraisemblablement lié à l'État chinois, a conduit une vaste campagne de cyberespionnage visant des communautés ouïghoures et tibétaines dans plusieurs pays, dont le Canada. Les pirates ont notamment pu enregistrer des appels, prendre des photos et des captures d'écran des appareils compromis.

Le Canada et les cyberincidents géopolitiques à l'horizon 2025

Alors que ce début d'année 2025 consacre une actualité nord-américaine très chargée politiquement, l'espace numérique du Canada est de plus en plus marqué par les débats agitant gouvernements et opinions publiques au quotidien. En février dernier, on apprenait par exemple qu'Ottawa ordonnait au Centre de la sécurité des télécommunications — principale agence de cybersécurité canadienne — de déployer pour la première fois ses capacités cyber contre les acteurs transnationaux du trafic de stupéfiants. Réagissant manifestement aux pressions de l'administration Trump en matière de sécurité frontalière, les autorités canadiennes semblent désormais vouloir user de leurs outils de cybersurveillance (et potentiellement de cyberattaques) pour contrecarrer le trafic de fentanyl, l'un des sujets de tension actuels avec le voisin américain. Une démonstration de plus, s'il en fallait une, qu'il devient de plus en plus difficile de parler de politique sans parler de numérique au Canada.

C'est à ce lien, toujours plus étroit, qu'est consacré le rapport sur les cyberincidents géopolitiques au Canada, cinquième publication du genre produite par l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand. Entre campagnes de cyberespionnage et opérations d'influence en ligne, le Canada demeure année après année une cible significative de la cyberconflictualité agitant l'espace numérique mondial. À ce titre, l'analyse réalisée dans ce rapport (sans prétendre à l'exhaustivité) a permis de recenser **11 cyberincidents à caractère géopolitique au Canada en 2024**. Au total, le répertoire des cyberincidents canadiens de la Chaire Raoul-Dandurand, dont les données du présent rapport sont issues, dénombre aujourd'hui **125 cyberincidents géopolitiques ayant touché le Canada depuis 2010**. Or, il ne s'agit là que des données provenant de sources ouvertes, qui ne reflètent donc qu'une fraction des activités numériques malveillantes ayant cours au pays.

Que sait-on de ces incidents, de leur nature, de leurs cibles ou encore de leur origine ? Voici un aperçu global des données disponibles sur ces questions.

QU'ENTEND-ON PAR CYBERINCIDENTS ?

Nous définissons comme « cyberincident » 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, les brèches de données ou encore les actes de manipulation de l'information, entre autres exemples (pour plus de détails, voir la rubrique méthodologique). 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 remontent jusqu'à 2010.

Quels types de cyberincidents sont les plus fréquents ?

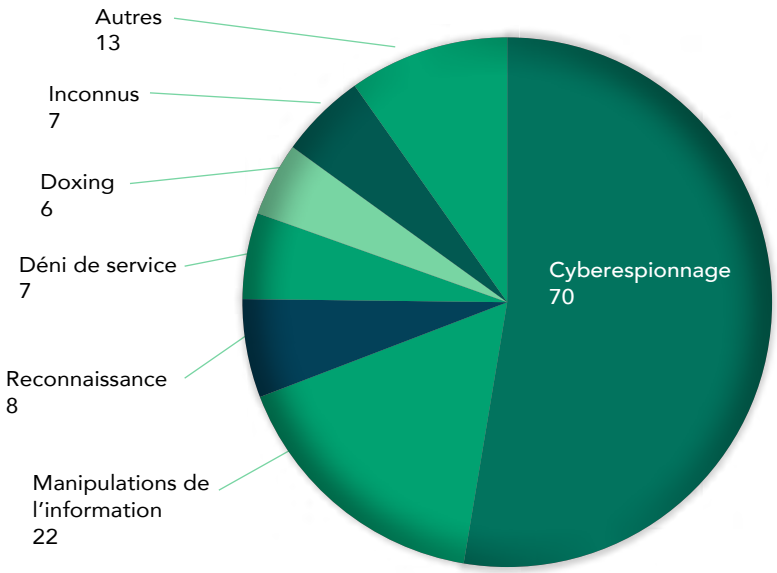
La très grande majorité des cyberincidents à caractère géopolitique touchant le Canada continue de relever de cyberespionnage. On pense notamment au vol de propriété intellectuelle et de secrets d'État ou encore à la surveillance clandestine d'individus. Sur les 125 incidents répertoriés depuis 2010, pas moins de 70 relèvent du cyberespionnage (soit 56 % du total). Les actes de manipulation de l'information (soit la diffusion intentionnelle, massive et coordonnée de nouvelles fausses ou biaisées à des fins politiques) sont le deuxième type de cyberincident le plus fréquent, au nombre de 22 depuis 2010 (soit 18 %). On peut noter que ces proportions sont restées remarquablement stables au fil des cinq années couvertes par les précédents rapports, suggérant ainsi qu'une tendance lourde est à l'œuvre.

De nouveau en 2024, le cyberespionnage et les manipulations de l'information représentent les deux catégories les plus prévalentes, avec 5 et 2 incidents respectivement. Il faut néanmoins noter que plusieurs incidents survenus en 2024 n'ont fait l'objet que de révélations partielles de la part des entités concernées, laissant ainsi planer un doute sur la nature exacte des activités malveillantes en question.

Quelles sont les cibles connues ?

En 2024 les entités gouvernementales canadiennes, particulièrement fédérales, ont été particulièrement ciblées. Affaires mondiales, la Gendarmerie royale du Canada (GRC) et le CANAFE ont tour à tour fait l'objet de cyberincidents — dont la nature reste nébuleuse — en janvier, février et mars 2024 respectivement. En avril, c'est le gouvernement de la Colombie-Britannique qui a déclaré avoir été pris pour cible, apparemment par des pirates affiliés à un État. En octobre, enfin, on apprenait que « des ministères et organismes du gouvernement du Canada, notamment des partis politiques fédéraux, la Chambre des communes et le Sénat » auraient été l'objet d'intenses activités

Types de cyberincidents les plus fréquents (depuis 2010)

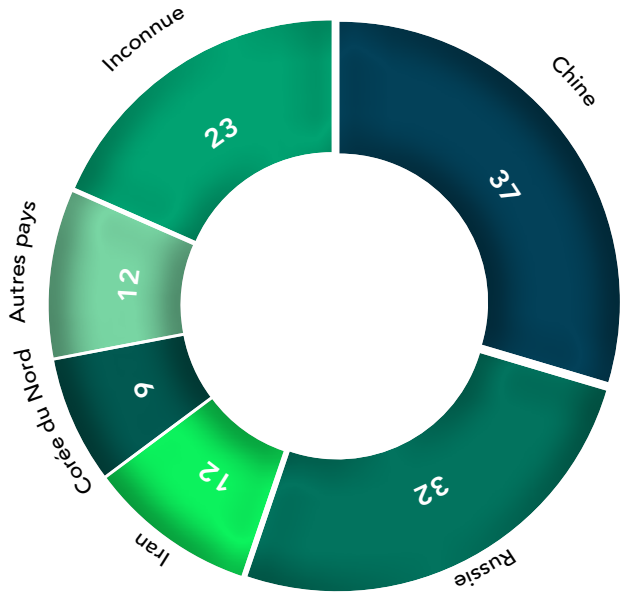


* Des cas peuvent cumuler simultanément plusieurs types d'incidents.
Source : Répertoire des cyberincidents canadiens

de reconnaissance par un groupe de pirates lié à l'État chinois. Une telle concentration de cyberincidents visant des organismes gouvernementaux est probablement sans précédent au Canada (voir chapitre).

Reste que les données globales issues de notre répertoire confirment la prééminence du secteur public parmi les cibles de cyberincidents géopolitiques : 56 % des incidents répertoriés depuis 2010 impliqueraient au moins une institution publique canadienne parmi les entités touchées, contre 37 % pour le secteur privé et 15 % pour la société civile[1]. Le degré de granularité des informations rendues publiques permet difficilement de ventiler ces données par secteurs d'activité spécifiques, mais il apparaît que les domaines de la défense, de l'énergie et des télécommunications figurent parmi les plus fréquemment visés au Canada.

Origine géographique des cyberincidents (depuis 2010)



Source : Répertoire des cyberincidents canadiens

D'où proviennent ces attaques ?

Depuis 2010, **quatre pays sont à l'origine de la grande majorité des cyberincidents géopolitiques recensés publiquement au Canada** : la Chine (37 incidents sur 125), la Russie (32), l'Iran (12) et la Corée du Nord (9). Ces données concernent l'origine *géographique* des cyberincidents et n'impliquent pas nécessairement une responsabilité des gouvernements des pays mentionnés (pour plus de détails, voir la rubrique méthodologie). Par ailleurs, du fait de l'absence de données probantes publiées en la matière, il apparaît que 23 des incidents recensés depuis 2010 n'ont pour le moment pas d'origine connue.

On peut noter qu'Israël a fait son entrée dans la liste des origines présumées l'année dernière. En mai 2024, on apprenait qu'une firme de consultation électorale israélienne (baptisée STOIC) a conduit une importante campagne de manipulation de l'information en ligne, dont plusieurs contenus ont spécifiquement visé des audiences canadiennes. La campagne de STOIC aurait été mandatée par le ministère israélien des Affaires de la Diaspora, afin de décrédibiliser les voix critiques de l'intervention à Gaza (voir étude de cas).

Quels groupes de pirates ont visé le Canada en 2024 ?

Plusieurs cyberincidents ayant touché le Canada en 2024 ont été attribués à des groupes de pirates informatiques déjà bien connus de la communauté de cybersécurité. Parmi eux figure par exemple Flax Typhoon (aussi appelé RedJuliett ou Ethereal Panda), un acteur vraisemblablement affilié au ministère de la Sécurité d'État de la République populaire de Chine. Ce groupe aurait notamment opéré un réseau de « machines zombies » (*botnet*) ayant infecté

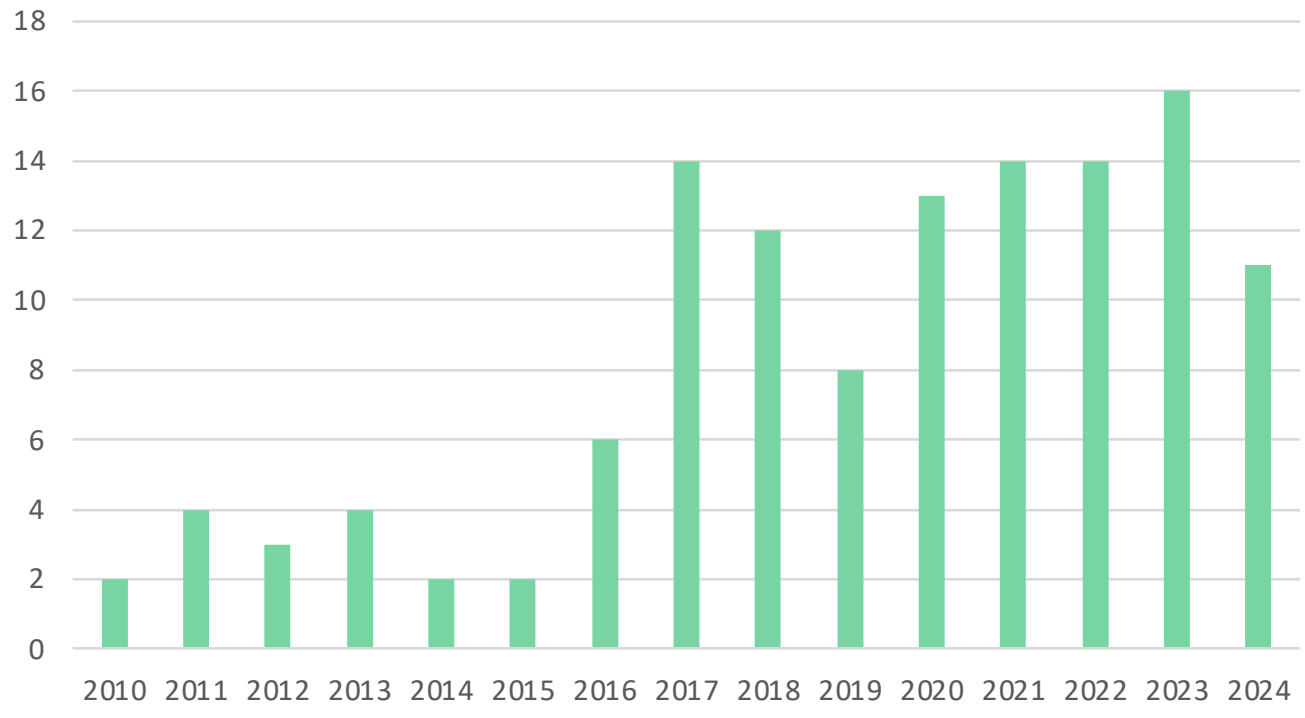
[1] À noter qu'un incident peut simultanément toucher différents types de cibles.

plus de 9000 appareils connectés situés en sol canadien (voir étude de cas).

Un autre groupe de pirates chinois, baptisé Earth Minotaur, aurait quant à lui conduit une importante campagne de cyberespionnage visant les communautés tibétaines et ouïgoures dans plusieurs pays, dont le Canada (voir étude de cas). Inconnu jusqu'alors, Earth Minotaur emploierait différents outils très similaires à ceux précédemment déployés par d'autres groupes chinois. On ne peut toutefois confirmer formellement son affiliation à des organes étatiques de la RPC.

Fin 2024, un groupe de pirates russes baptisé RomCom (aussi appelé CIGAR ou Storm-0978) a également visé des entités canadiennes, dont le nombre et la nature n'ont toutefois pas été spécifiés. Fait intéressant, RomCom mènerait à la fois des opérations de renseignement et des activités criminelles, répliquant ainsi un profil de « groupe hybride » observé de plus en plus fréquemment en Russie. Visant fréquemment des organes étatiques ukrainiens, RomCom entretient vraisemblablement des liens avec l'appareil sécuritaire russe, selon le Google Threat Intelligence Group. Les prochaines sections de notre rapport dressent un portrait détaillé des principaux cyberincidents géopolitiques ayant touché le Canada en 2024.

NOMBRE DE CYBERINCIDENTS RÉPERTORIÉS PAR ANNÉE



CYBERESPIONNAGE : type de cyberincident toujours le plus fréquent

Le cyberespionnage est un phénomène répandu au Canada depuis de nombreuses années. Les activités de cyberespionnage consistent à « obtenir par des moyens numériques de l'information sans l'accord préalable du détenteur de cette information », notamment pour subtiliser des données et renseignements sensibles pour les gouvernements, les entreprises ou encore les individus.

Comme l'indique notre répertoire des cyberincidents canadiens, il s'agit du type de cyberincident le plus fréquent dans notre base de données pour la période 2010-2025, dont pour l'année 2024. Nos observations rejoignent celles du rapport *Évaluation des cybermenaces nationales 2025-2026* du Centre canadien pour la cybersécurité, qui souligne, entre autres, que des pays comme la Chine et la Russie ont intérêt à intensifier leurs activités de cyberespionnage contre le Canada à l'avenir. Selon ce rapport, la Chine continue d'utiliser le cyberespionnage pour servir plusieurs objectifs de sa politique étrangère : vol de propriété intellectuelle ou de secrets industriels, influence sur l'opinion publique ou répression transnationale de groupes qu'elle considère comme une menace (diaspora ouïghoure, adeptes du Falun Gong, partisans de l'indépendance de Taïwan, etc.). De son côté, Moscou perçoit le Canada comme une « cible intéressante », notamment en raison de son statut de pays membre de l'OTAN, mais aussi de « son soutien de l'Ukraine contre l'agression russe et de sa présence dans l'Arctique ».

> \\ En l'état, ces incidents donnent parfois l'impression que les autorités canadiennes sont dépassées par les événements ou dans l'incapacité de fournir au public suffisamment d'informations pour le rassurer sur les risques cybernétiques auxquels la société canadienne est confrontée. \\

Au cours des dernières années, le groupe APT29 a par exemple mené des campagnes de cyberespionnage contre des centres de recherche canadiens pour tenter d'accélérer les découvertes russes sur le vaccin de la COVID-19. Un autre exemple majeur d'une campagne de cyberespionnage touchant le Canada a été révélé en 2018 : on apprenait alors que la Chine avait, sur une durée de 12 ans, mené une vaste campagne de cyberespionnage économique contre une douzaine de pays, dont le Canada, dans des secteurs comme la finance, les télécommunications, la santé, la biotechnologie, l'automobile ou encore les mines et le forage.

Organes gouvernementaux ciblés en série

L'année 2024 n'a pas fait exception à la règle alors que nous avons recensé au moins cinq campagnes de cyberespionnage visant spécifiquement le Canada. En janvier, des médias canadiens comme CBC et le *National Post* rapportaient qu'Affaires mondiales Canada avait été victime d'une importante brèche de données, pendant plus d'un mois, permettant à des pirates informatiques de consulter les courriels et de voler les informations personnelles de fonctionnaires œuvrant pour le ministère. Un mois plus tard, c'était au tour de la GRC de révéler qu'une brèche informatique d'une « ampleur alarmante » détectée dans ses systèmes aurait compromis des données essentielles et menacé la sécurité de l'organisation.

En avril, une campagne de cyberespionnage visant le gouvernement de la Colombie-Britannique rappelait que ce type de cyberincident peut autant cibler les gouvernements provinciaux que les institutions fédérales à Ottawa. Comme cela avait été le cas lors des attaques contre Affaires mondiales Canada et la GRC, les enquêtes entourant cet incident n'avaient pas permis de connaître l'identité des pirates ou encore l'étendue et la nature des données compromises. Emeline Manson, une experte en cybersécurité, rappelait toutefois que les « systèmes informatiques gouvernementaux sont particulièrement intéressants pour les pirates informatiques, puisqu'ils renferment des données confidentielles permettant un vol potentiel d'identité ».

Ce *modus operandi* a probablement été utilisé dans une autre opération de cyberespionnage ciblant le Canada en 2024, soit la campagne du groupe russe RomCom, découverte en novembre par l'entreprise informatique et de cybersécurité ESET. Soutenu par Moscou, le groupe de pirates a tiré profit de vulnérabilités de sécurité jusqu'alors inconnues dans les systèmes Windows et le navigateur Internet Mozilla Firefox pour installer des logiciels malveillants sur une foule d'ordinateurs en Europe et en Amérique du Nord. Le but (probable) était de collecter des informations personnelles sur les individus ou encore des secrets gouvernementaux dans des pays comme le Canada.

Des incidents entourés de mystère

L'année 2024 permet donc de réaffirmer trois conclusions sur le phénomène du cyberespionnage au Canada. Premièrement, le Canada n'est pas à l'abri d'une réalité désormais bien ancrée dans le système international contemporain : la tendance de divers États à tirer parti des moyens numériques pour mener des campagnes d'espionnage transnationales qui gagnent en ampleur, en fréquence et en sophistication. Deuxièmement, l'année 2024 confirme une fois de plus la diversité des auteurs, des cibles et des motifs des incidents de cyberespionnage visant le Canada. Dans un monde où les intérêts d'Ottawa divergent considérablement de ceux des gouvernements et régimes qui dirigent la Chine, la Russie, la Corée du Nord, l'Iran et même l'Inde, les campagnes de cyberespionnage risquent de se multiplier à l'avenir. Enfin, cette situation soulève la question de la capacité du Canada à prévenir de telles opérations, à les détecter précocement, à les déjouer et à tirer les leçons des attaques passées pour parfaire des stratégies de cyberdéfense.

En l'état, ces incidents donnent parfois l'impression que les autorités canadiennes sont dépassées par les événements ou dans l'incapacité de fournir au public suffisamment d'informations pour le rassurer sur les risques cybernétiques auxquels la société canadienne est confrontée. En effet, Ottawa a rarement été en mesure (ou a délibérément omis) de révéler à sa population l'identité des auteurs des opérations qui visaient spécifiquement le gouvernement canadien, ainsi que les objectifs des pirates. L'attaque de mars 2024 contre le CANAFE en est un exemple.

L'opération contre le CANAFE, campagne de cyberespionnage ou autre type de cyberincident ?

« Les systèmes de CANAFE ne sont pas disponibles pour le moment ». Voici le message qui s'affichait, le 5 mars 2024, sur le site du Centre d'analyse des opérations et déclarations financières du Canada, l'unité du gouvernement du Canada dont le mandat est « d'aider à la détection, à la prévention et à la dissuasion du blanchiment d'argent et du financement des activités terroristes ». Victime d'un cyberincident, le CANAFE avait mis en suspens son activité en ligne de manière à protéger l'intégrité de ses systèmes internes et la confidentialité de ses données. Bien que l'agence de renseignement se soit montrée peu communicative au regard des informations compromises, elle affirme que l'attaque n'a pas affecté « [s]es renseignements [et] [s]es systèmes protégés ». Pour autant, les pirates — dont l'origine n'a pas encore été établie publiquement — ont durablement perturbé les systèmes informatiques du CANAFE. En effet, ce n'est qu'en décembre 2024 que son système de soumission de déclarations a recommencé à fonctionner normalement.

Des observateurs extérieurs notent que les brèches créées lors de cette attaque auraient pu représenter « une aubaine inespérée pour les criminels », et ont probablement permis à des « transactions suspectes [de passer] sous le radar » de l'agence. Bien que les dirigeants du CANAFE n'aient pas souhaité divulguer « quelles tâches exactement ils [ont été] incapables d'effectuer » au cours des derniers mois, les retombées de cet incident sur la sécurité canadienne pourraient être considérables. En effet, le CANAFE reçoit chaque année quelque 20 millions de signalements d'opérations douteuses, provenant de 31 000 sources différentes. En fonction de leur pertinence, les informations sont communiquées aux forces de l'ordre ou à l'administration fiscale afin de prévenir divers crimes. À titre d'exemple, le CANAFE a joué un rôle déterminant dans une affaire de traite d'êtres humains en Saskatchewan en 2023. À l'issue de cette enquête, trois personnes ont été inculpées pour les mauvais traitements qu'ils avaient fait subir à une Bangladaise séjournant au Canada avec un permis de visiteur.

Le CANAFE peut également s'avérer une cible alléchante pour les cyberattaques du fait qu'il est non seulement un acteur clé dans la lutte contre le terrorisme, mais aussi un des organes veillant au respect des sanctions économiques imposées par Ottawa. Sans présumer de l'identité des responsables de l'incident, il importe de noter que des États cherchant à contourner des régimes de sanctions pourraient avoir un intérêt à conduire ce genre d'attaques. On peut rappeler à cet égard que le bureau du département de la Justice américain chargé du respect des sanctions (*Office of Foreign Assets Control*) a été visé par un groupe de pirates lié à l'État chinois en janvier 2025. Le fait que le CANAFE collabore étroitement avec des organes gouvernementaux similaires, responsables de détecter les crimes financiers ailleurs dans le monde, explique également pourquoi il peut être visé. Cet épisode démontre ainsi l'ampleur des conséquences qu'un cyberincident peut déclencher, en offrant à des acteurs criminels ou étatiques de nombreuses options pour affaiblir ou déstabiliser le Canada.

LA RÉPRESSION TRANSNATIONALE À L'ÈRE NUMÉRIQUE : une menace grandissante

Au Canada et dans le monde, la répression transnationale, employée par les gouvernements pour réprimer les exilés et leurs diasporas au-delà de leurs frontières, s'affirme avec force. Outre des méthodes « traditionnelles » de surveillance et d'intimidation, l'émergence de nouvelles technologies numériques amplifie la portée des menaces pesant sur les victimes. Profitant de la multiplication des outils de surveillance au sein d'une industrie débridée, les régimes autoritaires ont, plus que jamais, les capacités pour étendre leur contrôle à l'étranger. La nature clandestine des opérations, souvent peu exigeantes en termes de capital politique et financier, rend difficile toute forme de responsabilisation pour leurs auteurs, leur offrant ainsi la possibilité d'agir en toute impunité.

L'industrie mondiale de la surveillance

La croissance de l'industrie globale de la surveillance offre à ses clients — gouvernementaux comme privés — un arsenal toujours grandissant d'outils de répression. En dépit de l'onde de choc suscitée en 2021 par les révélations sur Pegasus, le puissant logiciel espion d'origine israélienne ayant été déployé contre au moins 180 victimes dans une vingtaine de pays (dont le Canada), l'industrie de la surveillance échappe toujours largement à la réglementation. Elle continue ainsi de doter les acteurs désirant exercer leur contrôle au-delà de leurs frontières d'outils sophistiqués de moins en moins onéreux.

Bien que les régimes autoritaires soient souvent critiqués pour leur persécution numérique des dissident-e-s, par le développement de leurs propres capacités étatiques de contrôle ou par le recours à des entreprises sous-traitantes, la découverte de nouveaux logiciels d'espionnage révèle le caractère global de l'industrie de la surveillance, à laquelle ni les entreprises ni les gouvernements occidentaux n'échappent. Par exemple, Israël et l'Italie, pays hôtes d'un nombre grandissant d'entreprises distributrices de logiciels espions, représentent aujourd'hui de véritables plaques tournantes de cette industrie préoccupante.

Au-delà des *espiogiciels*

Les logiciels espions ne sont qu'un des nombreux outils dont disposent les régimes autoritaires pour infiltrer les appareils des dissident-e-s à l'étranger. L'implantation de portes dérobées, octroyant un accès clandestin aux appareils des personnes ciblées, ou encore, la compromission de sites web par la technique du point d'eau — qui infecte les visiteurs via le téléchargement furtif d'un maliciel — représentent deux types d'attaques fréquemment utilisées pour garder un œil sur les diasporas jugées problématiques à l'étranger.

Contrairement aux logiciels espions plus puissants, capables d'infecter automatiquement les appareils des victimes, ces attaques font appel à l'ingénierie sociale, où les attaquants se font passer pour un proche ou pour un membre d'une organisation associée à leur domaine d'expertise afin d'inciter leurs victimes à cliquer sur un lien malveillant. Selon les chercheur-e-s, ces types d'attaques révèlent l'appétit croissant des acteurs de la menace pour infiltrer les téléphones cellulaires de leurs cibles, leur donnant accès à un ensemble de données personnelles, comme les messages textes et la liste d'appels. De plus, ces attaques leur permettent également d'épier leurs victimes par le biais de l'appareil photo, du microphone ou encore du GPS de leurs téléphones.

> \\ Si ces incidents hautement médiatisés représentent des cas extrêmes de menaces et de sévices physiques à l'encontre de victimes au Canada, la réalité de la répression transnationale au pays est beaucoup moins visible. \\

Les obligations de partage de données qu'ont certaines compagnies technologiques envers les services de sécurité et de renseignement étatiques, en Chine notamment, joueraient également un rôle dans le renforcement des capacités des États à espionner leurs diasporas à l'étranger, celles-ci dépendant des plateformes numériques pour communiquer entre elles et avec leurs proches dans leurs pays d'origine. La création d'accords de coopération juridique mutuelle quant aux enjeux de « cybercriminalité » pourrait également représenter une victoire pour les régimes autoritaires, en renforçant leurs capacités à identifier, traquer et exiger le retour des personnes dissidentes vivant en exil.

Au Canada

Au Canada, la répression transnationale entre dans la catégorie plus large de l'ingérence étrangère, une menace faisant l'objet d'une prise de conscience grandissante au sein de la population et du gouvernement. Cette prise de conscience a d'ailleurs mené à la tenue d'une enquête publique conclue en janvier 2025, présidée par la juge Marie-Josée Hogue. Bien que celle-ci ait admis dans son rapport final avoir seulement « effleur[é] la surface » de la répression transnationale, elle affirme toutefois que celle-ci représente « un véritable fléau », mettant à mal les institutions démocratiques et empêchant des membres de communautés opprimées de participer à la vie démocratique et à jouir pleinement de leurs droits et libertés.

Trois États en particulier y sont accusés d'être des auteurs de répression transnationale au Canada : l'Iran, la République populaire de Chine (RPC) et l'Inde. Le rapport met en lumière deux cas concrets de répression transnationale liés à ces deux derniers gouvernements : l'assassinat de l'activiste sikh Hardeep Singh Nijjar en Colombie-Britannique (qui aurait impliqué le

gouvernement indien, selon les agences de renseignement canadiennes), ainsi que les postes de police étrangers de la RPC en sol canadien.

Si ces incidents hautement médiatisés représentent des cas extrêmes de menaces et de sévices physiques à l'encontre de victimes au Canada, la réalité de la répression transnationale au pays est beaucoup moins visible. En effet, l'écrasante majorité des activités numériques de répression menées au Canada par des acteurs étrangers est effectuée par le biais d'outils et de techniques d'intrusion numérique difficiles à détecter. Notre répertoire des cyberincidents recense certains de ces cas « invisibles » de répression, comme le cyberespionnage de dissident-e-s d'Éthiopie établis ou de passage au Canada en 2017 ou encore, celui d'activistes iraniens basés au Canada en 2020. Et comme ailleurs dans le monde, les victimes de répression transnationale basées au Canada ne sont pas seulement épiées; elles sont également intimidées et menacées, notamment via la manipulation des caractéristiques des plateformes numériques utilisées dans la vie de tous les jours, comme Weibo, WhatsApp ou X.

Par exemple, les attaquants peuvent faire suspendre les comptes de réseaux sociaux des cibles en signalant leur profil en masse, ou encore, disséminer de fausses informations sur elles pour salir leur réputation en ligne, particulièrement auprès des membres de la même diaspora. Ces efforts servent notamment à créer des tensions au sein des communautés pour mieux les affaiblir et nuire à leurs efforts de mobilisation. Les attaques peuvent être perpétrées à la vue de tout un chacun ou de manière plus discrète, via l'envoi de menaces par messagerie privée.

L'angoisse au quotidien

Les récentes recherches s'intéressant aux conséquences sociales, professionnelles et psychologiques de la répression transnationale mettent en garde contre les effets démobilisateurs du phénomène. En effet, celle-ci peut inciter les victimes à s'isoler et à suspendre, voire à cesser complètement, leur activisme par peur ou par épuisement. Par extension, les tactiques d'intimidation en ligne ont également pour effet de terroriser les autres membres des diasporas et de les réduire au silence, sous peine d'être ciblés par des actes similaires. Depuis quelques années, les groupes de défense des libertés civiles focalisent de plus en plus sur l'aspect genré de la répression transnationale numérique, levant le voile sur les conséquences disproportionnées que vivent les femmes activistes visées par de telles tactiques, comparativement à leurs homologues masculins.

Pour les témoins entendus lors de l'enquête publique canadienne et les activistes interrogés par les groupes de défense des droits humains, la répression transnationale est un obstacle quotidien, une menace de l'ombre difficile à exposer et à endiguer compte tenu du manque de ressources disponibles pour celles et ceux qui la subissent. Alors que 22 % de la population canadienne est née à l'étranger et que les régimes autoritaires profitent d'un arsenal d'outils de surveillance numérique toujours plus grand, il ne fait nul doute que la propagation de l'oppression étatique à l'intérieur des frontières canadiennes continuera à représenter un enjeu important dans les années à venir.

Campagne d'Earth Minotaur contre des activistes tibétains et ouïghours

En décembre 2024, la firme de cybersécurité Trend Micro révélait qu'Earth Minotaur, un groupe de menace persistante avancée (APT) vraisemblablement lié à la Chine, a espionné des activistes tibétains et ouïghours dans plusieurs pays, dont le Canada.

Lors des attaques, il s'agit de contacter les cibles à l'intérieur de conversations de groupe sur des plateformes de messagerie instantanées, comme WhatsApp et WeChat. Pour les inciter à cliquer sur des hyperliens malveillants et augmenter leurs chances de réussite, les attaquants usurpent l'identité de différents individus. Leurs messages d'hameçonnage, « soigneusement élaborés », prétendent provenir d'organes officiels chinois ou affichent des nouvelles chinoises relatives à la COVID-19, aux religions, aux populations tibétaine ou ouïghoure, et aux voyages en Chine.

Une fois l'hyperlien consulté, la victime est redirigée vers un kit d'exploitation — sorte de boîte à outils visant des vulnérabilités spécifiques dans un système informatique — dénommé MOONSHINE par les chercheur-e-s en cybersécurité. MOONSHINE implante ensuite la porte dérobée DarkNimbus sur l'appareil de la cible, à son insu. Décrite par les chercheur-e-s comme un « outil complet de surveillance des téléphones Android », la porte dérobée permet aux attaquants de voler des informations privilégiées de ses cibles, comme les listes de contacts ou des appels téléphoniques, les SMS, le contenu du presse-papiers, les signets du navigateur et les conversations de plusieurs applications de messagerie instantanée. Les pirates ont également pu enregistrer des appels, prendre des photos et des captures d'écran ainsi qu'enregistrer certaines opérations des appareils visés.

Le kit d'exploitation MOONSHINE a déjà été utilisé dans le passé contre la communauté tibétaine par un autre acteur de menace lié à la Chine, nommé POISON CARP par le Citizen Lab. À ce moment, l'attaque représentait déjà « une escalade significative des tactiques d'ingénierie sociale et de la sophistication technique » par rapport à celles généralement utilisées contre la communauté tibétaine. Depuis, les capacités de MOONSHINE se sont améliorées, comportant désormais de nouvelles vulnérabilités et davantage de protections pour contrer les efforts de détection.

D'après les chercheur-e-s de Trend Micro, le kit d'exploitation MOONSHINE, utilisé par d'autres groupes de pirates informatiques sophistiqués, tels que POISON CARP et UNC5221, serait encore en cours de développement. Toutefois, aucun lien n'a pu être établi entre Earth Minotaur et les autres acteurs ayant exploité ce kit par le passé, ce qui laisse supposer qu'il s'agit d'un nouveau protagoniste dans le paysage des cybermenaces.

MANIPULATION DE L'INFORMATION ET IA GÉNÉRATIVE : évolution ou révolution ?

À l'horizon 2025, les campagnes de manipulation de l'information se suivent, mais ne se ressemblent pas : l'utilisation de l'intelligence artificielle (IA) générative à des fins frauduleuses connaît en effet une tendance à la hausse, au Canada et ailleurs. Déjà à la fin 2023, Microsoft révélait l'existence d'une opération d'influence iranienne basée sur un faux reportage vidéo créé par IA générative, à laquelle des internautes canadiens auraient été exposés. D'autres cas du genre sont venus s'ajouter à la liste en 2024 (voir encadré plus bas).

L'utilisation de l'intelligence artificielle pour générer du contenu sur les médias sociaux est maintenant pratique courante. Au Sud de la frontière, les élections présidentielles américaines ont permis d'observer cette tendance croissante. Selon la firme Thales, aux États-Unis, le trafic généré par des automates représentait en 2022 pas moins de 32 % du trafic Internet et se situait autour de 35 % pour 2023. Alors que la population canadienne est appelée aux urnes en 2025, il importe de s'interroger sérieusement sur le potentiel de manipulation de l'information découlant de la révolution de l'IA, dont les capacités d'imitation se révèlent de plus en plus réalistes.

Brouillard informationnel

En septembre 2024, on apprenait qu'une vaste campagne d'influence russe baptisée « Doppelganger », démantelée par la justice américaine, incluait des contenus portant sur le Canada. Un faux site d'information aurait notamment publié plus d'une douzaine d'articles cherchant à tourner Justin Trudeau en ridicule, tout en mettant en valeur le chef de l'opposition conservatrice, Pierre Poilièvre. Bien que ce ne soit apparemment pas le cas des contenus canadiens, la campagne Doppelganger incluait plusieurs contenus générés par IA. Notons au passage que, dans la boîte à outils d'Ottawa pour lutter contre la désinformation, il n'existe pour l'instant pas de loi couvrant la manipulation artificielle des voix et des images, l'apanage des acteurs malveillants créateurs d'hypertrucages. Stéphane Perrault, directeur général d'Élections Canada, demande d'ailleurs d'urgence une réforme des lois existantes en la matière.

En octobre 2024, un groupe cybercriminel algérien baptisé FunkSec a prétendu avoir intercepté une conversation entre Donald Trump et Benjamin Netanyahu. La supercherie a été rapidement repérée : le soi-disant enregistrement était en fait une conversation générée par l'intelligence artificielle, le groupe cherchant probablement à gagner en visibilité pour attirer l'attention de clients potentiels. Bien que cet incident ne concerne pas le Canada spécifiquement, il suggère néanmoins que des groupes de pirates privés cherchant simplement à promouvoir leurs services pourraient contribuer eux aussi à épaissir le brouillard informationnel en ligne.

Modération des contenus en recul

Si le secteur privé et les géants technologiques ont pu jouer un rôle majeur dans la lutte contre la désinformation ces dernières années, les nouvelles récentes ont de quoi inquiéter. Meta annonçait par exemple en janvier 2025 qu'elle mettait fin à ses opérations de vérifications des faits. Tout comme sur X depuis l'arrivée d'Elon Musk, Mark Zuckerberg passe le flambeau à la communauté d'utilisateur-trice-s, qui n'est pas forcément la mieux outillée, pour effectuer ce travail. Il reste à voir quel impact aura cette décision alors que le retour de Donald Trump à la Maison-Blanche semble annoncer une ère de déréglementation chez certains chefs de file des GAFAMs qui ont réagi positivement à sa victoire. Le vice-président

JD Vance a d'ailleurs déclaré le 11 février 2025 que les États-Unis ne participeraient pas à un régime international de régulation de l'IA, le Paris AI Action Summit, qui, selon lui, entraverait l'innovation.

Autre phénomène préoccupant, l'intelligence artificielle semble de plus en plus agir de manière autonome. En effet, la firme américaine de vérification de l'information NewsGuard a récemment publié des chiffres inquiétants au sujet de la prolifération de sites Internet créés en utilisant l'IA générative, mais qui s'administrent avec une intervention humaine minimale, voire de manière complètement autonome. Alors qu'aucun site du genre n'était répertorié dans la première moitié de 2023, la firme en dénombre maintenant environ 1150, qui opèrent en 16 langues différentes et qui publient des articles parfois entièrement écrits par des automates. Une variété de sujets y sont discutés, notamment la politique et la guerre en Ukraine, qui semble être l'un des sujets particulièrement populaires pour 2024. Il n'est pas difficile d'imaginer comment ces mécanismes pourraient contribuer à une croissance des manipulations de l'information en ligne.

Une technologie en phase ascendante

Parmi les avancées récentes dans le domaine de l'IA, on remarque que les réseaux antagonistes génératifs (GAN), ont fait des progrès majeurs depuis leur apparition en 2014. Ces programmes opposent deux réseaux de neurones artificiels qui entrent en quelque sorte en compétition pour créer, par exemple, une image. À tour de rôle, une IA crée une image et une autre tente de déterminer si elle est authentique. Les deux systèmes se relancent et s'entraînent ainsi pour créer des images toujours de plus en plus convaincantes.

\\ Le contenu créé par l'intelligence artificielle est sans aucun doute toujours plus persuasif, mais il ne suscite pas nécessairement davantage d'interactions sur les médias sociaux. \\

Dans une étude publiée en 2022, des centaines de participant-e-s avaient pris part à une expérience où ils devaient déterminer à partir d'une série de visages ceux qui étaient véritables et ceux qui étaient générés par l'IA. Les résultats étaient loin d'être rassurants : non seulement les participant-e-s n'arrivaient pas à faire la différence, mais dans une large proportion, les visages générés par l'IA étaient jugés plus susceptibles d'être authentiques. Avec les progrès fulgurants de l'IA générative, 2022 semble maintenant lointain. Bien que les faux comptes créés par l'utilisation de telles technologies soient pour l'instant peu nombreux, une étude récente démontre qu'ils sont principalement utilisés pour parfaire les campagnes d'hameçonnage et pour amplifier la diffusion de messages inauthentiques sur les réseaux sociaux.

Cela ne veut pas dire que nous naviguons à l'aveugle dans la tempête. Le contenu créé par l'intelligence artificielle est sans aucun doute toujours plus persuasif, mais il ne suscite pas nécessairement davantage d'interactions sur les médias sociaux. Et s'il permet de propulser les campagnes d'influence de manière plus systématique en occupant de plus en plus d'espace sur les plateformes, il échoue souvent, jusqu'ici, à convaincre les utilisateur-trice-s visés. Enfin, pour l'heure, rien ne prouve qu'une exposition à du contenu généré par l'IA ou la réception de messages de robots conversationnels provoquent des changements d'allégeances politiques ou idéologiques en conséquence.

Campagne d'influence pro-israélienne par la firme STOIC

En mars 2024, le DFRLab, un organisme américain qui étudie la désinformation et les campagnes d'influence, met à jour une opération visant à disséminer du contenu islamophobe aux États-Unis, le tout en lien avec la guerre à Gaza. L'enquête expose du contenu factice, rédigé en anglais et en hébreu, propagé par plus de 130 faux comptes sur la plateforme X appartenant à de soi-disant étudiant-e-s d'origine juive, des Afro-Américain-e-s et des citoyen-ne-s préoccupés. Ces comptes appellent à la libération des otages enlevés par le Hamas le 7 octobre 2023, critiquent les manifestations sur les campus universitaires et dénoncent les activités de l'Office de secours et de travaux des Nations unies pour les réfugiés de Palestine dans le Proche-Orient (UNRWA) dépeint comme de mèche avec le Hamas.

Alors que Meta se saisit des résultats de l'enquête du DFRLab, une analyse interne permet non seulement de repérer 510 faux profils sur Facebook et 32 sur Instagram, tous créés dans un très court laps de temps, mais aussi d'établir des liens avec des campagnes dans d'autres pays, dont une campagne d'influence menée sous l'égide du compte United Citizens for Canada. OpenAI, la firme américaine derrière la création de ChatGPT, confirme que ses services, notamment ChatGPT, ont été utilisés pour créer du contenu écrit. Les différentes enquêtes permettent aussi de démontrer que l'IA générative a permis de créer des visages pour agrémenter les faux profils afin de les rendre plus crédibles.

L'acteur derrière l'opération est la firme de marketing israélienne STOIC. Elle aurait vraisemblablement reçu une somme de deux millions de dollars du ministère israélien des Affaires de la Diaspora pour mener à bien l'opération. Quel rôle a joué United Citizens for Canada de son côté ? Le faux compte a principalement été utilisé pour partager du contenu antimusulman auprès de journalistes, de politicien-ne-s ainsi que de véritables utilisateur-trice-s. Le compte mettait en garde la population contre l'imposition de la charia au Canada tout en critiquant le laxisme des politiques d'immigration canadiennes qui permettraient l'implantation de groupes islamistes violents. Selon Mike Dvilyanski, responsable de l'enquête chez Meta, la campagne aurait cependant généré peu de réactions : bien que les faux profils ont été utilisés pour mousser la campagne et générer plus de partages, les interactions authentiques se sont faites rares et les faux profils ont été relativement faciles à repérer et à suspendre.

Ce cas n'est pourtant pas insignifiant. D'abord, si les campagnes d'influence n'ont rien de nouveau, les liens entre Tel-Aviv et STOIC laissent entrevoir une étroite collaboration entre les États et le secteur privé pour sous-traiter ces opérations, rendant le repérage et l'attribution de celles-ci de plus en plus difficiles. Les États acquièrent ainsi une couche de « déni plausible » permettant d'occulter leur implication, ce qui pourrait les rendre davantage disposés à entreprendre de telles campagnes. Par ailleurs, l'implication probable de l'État israélien dans l'opération vient également démontrer que les campagnes d'influence au Canada ne sont vraisemblablement plus uniquement l'apanage des puissances adverses « traditionnelles » (Russie, Chine, Iran, etc.), mais pourraient à l'avenir provenir aussi de pays considérés comme des partenaires.

BOTNETS ET INFRASTRUCTURES OFFENSIVES : quand les cyberopérations génèrent des « victimes collatérales »

Peut-on pâtir d'une cyberattaque sans en être la cible directe ? Bien que l'enjeu ne soit pas le plus discuté par la communauté de la cybersécurité, la réponse est clairement affirmative. De fait, dans le cadre d'activités malveillantes, les pirates informatiques sont fréquemment amenés à instrumentaliser des cibles « intermédiaires », dont les systèmes informatiques doivent servir de tremplin à une opération plus vaste. Il s'agit le plus souvent d'accaparer discrètement un morceau de réseau (un serveur ou un routeur par exemple), en vue de constituer une « infrastructure offensive ». Sans être elle-même victime de vol de données ou de déni de service, l'entité concernée voit néanmoins son système informatique partiellement dévoyé — le plus souvent à son insu.

L'année 2024 a rappelé que ce genre d'incident touche, au moins occasionnellement, le Canada. En septembre, les États membres du Groupe des cinq (*Five Eyes*) annonçaient avoir démantelé un réseau de « machines zombies » (un *botnet*) opéré par un groupe de pirates étatiques chinois, regroupant près de 260 000 appareils connectés et incluant plus de 9000 appareils canadiens. Appartenant à des petites entreprises ou même à des particuliers, ces machines étaient discrètement contrôlées à distance par les pirates et servaient de vecteur à d'autres opérations, de cyberespionnage par exemple (voir encadré ci-dessous). Cet événement n'est toutefois pas une première au Canada. En mars 2022, un rapport publié par la firme de cybersécurité Trend Micro révélait qu'un *botnet* de routeurs, constitué clandestinement par le groupe de pirates Sandworm, affilié au renseignement militaire russe, instrumentalisait les équipements de plusieurs entités canadiennes.

Détourner et obfusquer

Pour bien comprendre l'enjeu de la constitution clandestine d'infrastructures offensives, on pourrait comparer les victimes collatérales à des propriétaires d'automobiles, dont les véhicules sont discrètement subtilisés la nuit pour commettre des vols et des cambriolages. Bien qu'ils ne soient pas eux-mêmes la cible des délits en question, les propriétaires voient leurs biens utilisés contre leur gré, à des fins néfastes de surcroît. Ce contrôle à distance est généralement acquis à travers l'installation d'un logiciel malveillant ou d'une porte dérobée (*backdoor*) sur les appareils en question et peut perdurer de quelques jours à plusieurs mois suivant le type d'activité entrepris. Fréquemment déployés par les cybercriminels, de tels procédés sont aussi occasionnellement utilisés par les groupes de pirates étatiques — et des cas de partage d'infrastructures entre les deux sphères ont déjà été documentés.

Dans le cas de pirates affiliés à des États, les infrastructures informatiques détournées peuvent servir différents objectifs. Un serveur d'entreprise discrètement contrôlé à distance peut par exemple être utilisé pour stocker temporairement des données dérobées à la cible principale, dans l'attente de leur exfiltration finale. Un ordinateur personnel, une fois rattaché à un *botnet* de plusieurs milliers d'autres appareils, peut contribuer à une attaque par déni de service contre un site web en inondant celui-ci de requêtes inauthentiques. Un routeur domestique peut quant à lui servir de nœuds de transit aux pirates, afin d'allonger et de complexifier le chemin emprunté pour pirater une cible dans l'idée de masquer l'origine réelle d'une cyberattaque. En d'autres termes, ces appareils compromis peuvent fournir aux pirates aussi bien de l'espace de stockage que de la puissance de traitement et un mécanisme d'obfuscation.

**\\ La révolution IoT implique donc que la surface d'attaque à disposition des pirates s'accroît actuellement de manière exponentielle et que les barrières posées pour sécuriser ces nouveaux territoires numériques s'avèrent souvent vétustes. **

Victimes collatérales, dommages réels

Si ces victimes collatérales sont le plus souvent choisies au hasard, elles répondent à certaines caractéristiques spécifiques : ce sont généralement de petites organisations disposant d'un personnel informatique très modeste et dont l'infrastructure est sujette à peu de contrôles de sécurité. Il peut s'agir, par exemple, de petites entreprises, de municipalités ou d'institutions scolaires de taille modeste, et parfois même de particuliers. L'enquête publiée en 2022 par Trend Micro révélait par exemple que le *botnet* constitué par les pirates du renseignement russe comptait parmi ses victimes une petite compagnie locale de plomberie aux États-Unis. Qui plus est, de telles organisations utilisent souvent des appareils connectés bon marché ou vieillissants, dont les vulnérabilités ne sont pas ou plus réparées par les entreprises conceptrices. Une vaste campagne de cyberespionnage chinoise publicisée en 2023 reposait par exemple sur l'exploitation de vieux routeurs non mis à jour, vraisemblablement détenus par de petites entreprises ou des particuliers. Le groupe de pirates Fancy Bear, lié au renseignement militaire russe, a récemment fait de même au Royaume-Uni et aux États-Unis.

Les pirates veillant habituellement à maintenir un niveau d'activité limité sur les appareils dévoyés, les personnes visées ne se rendent que rarement compte qu'une partie de leur réseau est furtivement exploitée à des fins illégitimes. Cela ne veut pas pour autant dire qu'aucun tort n'est causé aux victimes intermédiaires. L'accaparement de la puissance de traitement d'un appareil peut par exemple porter temporairement atteinte à la performance d'un système et ralentir ainsi les activités menées en parallèle par l'utilisateur-trice légitime. Dans des cas extrêmes, des manipulations imprudentes ou maladroites de la part des pirates pourraient même faire tomber le réseau dévoyé, forçant son propriétaire à entreprendre des mesures de remédiation parfois coûteuses. Dans une étude publiée en 2018, des chercheurs de l'Université Princeton envisageaient même la possibilité qu'un *botnet*

regroupant de nombreux appareils ménagers connectés puisse un jour être utilisé pour déstabiliser la grille électrique d'une collectivité en ordonnant subitement une mise en marche massive d'appareils à haute consommation énergétique.

> \\ L'instauration de normes de cybersécurité minimales pour les appareils commercialisés au Canada pourrait représenter une piste à explorer. De telles initiatives pourraient encourager d'autres États à faire de même et ainsi stimuler une forme de sécurité collective. \\

Tendre vers la sécurité collective

De fait, une évolution actuelle contribue significativement à accroître les inquiétudes vis-à-vis de la constitution clandestine d'infrastructures : l'essor de l'Internet des objets (*Internet of Things*, IoT), qui voit des millions d'objets connectés rejoindre chaque jour l'Internet global, du cadre photo numérique au grille-pain « intelligent ». Souvent petits, bon marché et conçus à la hâte, ces appareils présentent fréquemment d'importantes failles de sécurité, qui peuvent facilement livrer des accès à des pirates cherchant à se bâtir une infrastructure offensive. À titre d'exemple, le *botnet* Mirai, l'un des plus vastes observés à ce jour, comptait parmi ses « machines zombies » de nombreux petits appareils bon marché et faiblement sécurisés — notamment des caméras connectées. La révolution IoT implique donc que la surface d'attaque à disposition des pirates s'accroît actuellement de manière exponentielle et que les barrières posées pour sécuriser ces nouveaux territoires numériques s'avèrent souvent vétustes.

Au plan sécuritaire et stratégique, il est tentant de voir le problème des infrastructures informatiques compromises comme un enjeu secondaire. Après tout, les utilisateur-trice-s concernés sont bien davantage des instruments que des victimes directes des groupes de pirates étatiques. Reste que le détournement d'appareils numériques constitue une source de menaces pour d'autres acteurs à travers le monde. Alors que le Canada aspire officiellement à promouvoir un « comportement responsable des États dans le cyberespace », prévenir l'utilisation clandestine d'infrastructures informatiques canadiennes à des fins malveillantes apparaît important. À cet égard, l'instauration de normes de cybersécurité minimales pour les appareils commercialisés au Canada pourrait représenter une piste à explorer. De telles initiatives pourraient encourager d'autres États à faire de même et ainsi stimuler une forme de sécurité collective. Les récents développements en la matière dans l'Union européenne pourraient également pousser les manufacturiers à adopter de meilleures pratiques. Dans le cyberespace, probablement plus qu'ailleurs, protéger les autres équivaut bien souvent aussi à se protéger soi-même.

Démantèlement du botnet « *Raptor Train* »

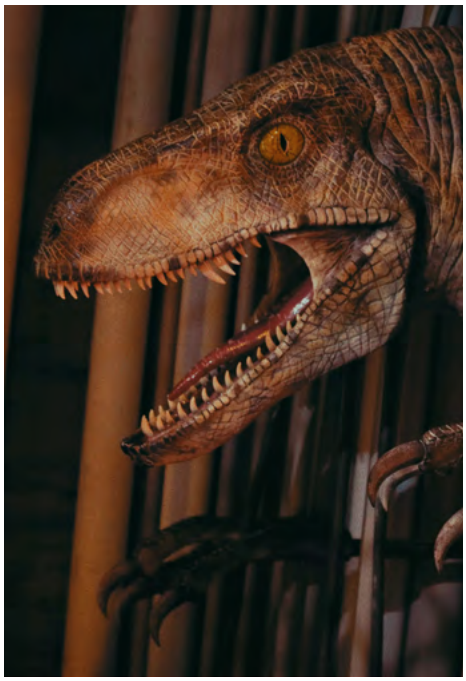
Le 18 septembre 2024, les agences de cybersécurité des cinq pays membres du *Five Eyes* publient un communiqué conjoint qui fait rapidement grand bruit dans le secteur numérique. Celui-ci annonce le démantèlement réussi d'un vaste réseau de « machines zombies » (*botnet*) opéré par un groupe de pirates lié à la République populaire de Chine. Baptisé Raptor Train, ce *botnet* aurait compromis jusqu'à 260 000 appareils numériques, parmi lesquels des routeurs et des caméras connectées, pour la plupart domestiques ou de bureau. Avec près de 9200 appareils compromis, le Canada totaliserait 3,5 % de l'infrastructure du *botnet* — occupant ainsi la 6e place parmi la vingtaine de pays touchés.

Si l'on en croit le communiqué, le *botnet* pouvait notamment servir de proxy pour masquer l'origine de cyberopérations menées par la Chine ainsi que de vecteur à des attaques par déni de service distribué (DDoS). Surnommé Flax Typhoon dans l'industrie de la cybersécurité, le groupe ayant bâti et opéré ce *botnet* serait lié au ministère de la Sécurité d'État chinois par l'entremise d'un contractant gouvernemental nommé Integrity Technology Group. D'après certains rapports de firmes de cybersécurité, le *botnet* aurait fait ses premiers pas en mai 2020 et atteint son pic de croissance mi-année 2023.

La liste des appareils compromis pour assembler le *botnet*, le plus grand attribué à la Chine jusqu'alors, est variée. Celle-ci incluait des routeurs et modems résidentiels ou de bureau, des serveurs de stockage en réseau (*network-attached storage*), des caméras connectées ainsi que des enregistreurs vidéo numériques (généralement utilisés pour des systèmes de vidéosurveillance). Black Lotus Labs, première entreprise ayant repéré l'existence du *botnet*, estime que ces appareils auraient été infectés durant des périodes allant typiquement de 17 à 75 jours, selon leur rôle dans l'infrastructure de Raptor Train.

C'est le FBI, sur autorisation des tribunaux américains, qui aurait conduit l'opération de remédiation — d'une durée d'une quinzaine de jours — ayant permis le démantèlement de Raptor Train. Les pirates de Flax Typhoon auraient toutefois tenté de faire obstacle à ce grand nettoyage en lançant parallèlement une attaque par déni de service contre l'infrastructure opérationnelle du FBI — sans succès. En janvier 2025, le département du Trésor a annoncé des sanctions à l'encontre d'Integrity Technology pour avoir participé à des cyberopérations visant des entités américaines.

Le Canada, pour sa part, n'a pas adopté de mesures similaires. En octobre 2024, en marge de la publication de son *Évaluation des cybermenaces nationales 2025-2026*, le Centre canadien pour la cybersécurité a déclaré que la Chine représente actuellement la cybermenace « la plus active et la plus sophistiquée » à laquelle fait face le Canada.



CONCLUSION

Pour la fin du mutisme d'Ottawa : le Canada doit faire preuve de transparence sur les cyberincidents

Pour la première fois depuis son lancement en 2020, le rapport observe une baisse des recensions de cyberincidents au Canada. De 16 cyberincidents en 2023, le Canada n'aurait été ciblé par des acteurs étrangers que 11 fois cette année, selon les données disponibles. Ce constat surprend au regard d'une actualité internationale chargée qui tend à suggérer une intensification des cyberincidents à caractère géopolitique à travers le monde : de l'ingérence électorale aux États-Unis et en Roumanie, à l'infiltration des réseaux des géants des télécommunications américains, en passant par le sabotage de câbles Internet sous-marins dans la mer Baltique. Plus choquant, ce constat détonne avec l'*Évaluation des cybermenaces nationales 2025-2026* publiée par le Centre canadien pour la cybersécurité, qui note, sans aucune ambiguïté, que le pays « affronte un environnement de cybermenaces complexe et en pleine expansion » et fait face à des « États adversaires […] plus agressifs ». Plutôt qu'une diminution, « [a]u cours des deux dernières années, » le Centre a observé « une forte augmentation du nombre et de la gravité de cyberincidents, dont plusieurs ciblent nos services essentiels ».

Si la conclusion du Centre canadien pour la cybersécurité est inquiétante, elle a, à tout le moins, le mérite de disqualifier tout discours de complaisance. Le Canada n'échappe pas à cette tendance mondiale. Ni sa vertu ni sa diplomatie ne le protègent, pas plus que le « grand retour » du Canada sur la scène internationale annoncé par le gouvernement Trudeau en 2015. Le Canada est bien ancré dans des réseaux d'alliances occidentaux, anglo-saxons et nord-américains qui constituent des cibles de choix pour la Chine, la Russie, l'Iran et la Corée du Nord. Mais alors, comment pouvons-nous expliquer le décalage qui existe entre le répertoire de l'OCM et cette tendance mondiale ?

À notre avis, le mutisme et le secret entretenus par Ottawa expliquent la difficulté à brosser un portrait d'ensemble du phénomène au Canada. Comme la Commission sur l'ingérence étrangère au Canada le note dans son rapport final, « le gouvernement s'est révélé être un mauvais communicateur et insuffisamment transparent en ce qui a trait à l'ingérence étrangère ». Cette observation vaut pour les autres sphères de la sécurité nationale.

Pour qui suit les activités des institutions de sécurité canadiennes, la critique n'est pas surprenante. Les cyberincidents frappant le Canada s'accompagnent souvent de communiqués laconiques, comme ceux annonçant la campagne de salissage chinoise ciblant des parlementaires canadiens et les cyberattaques contre le Parlement, le Conseil national de la recherche du Canada, Affaires mondiales, Rideau Hall et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. Les communiqués étant excessivement généralistes, le lecteur ne peut en tirer d'information pertinente. C'est plutôt à travers le travail d'acteurs privés, issus d'entreprises ou de la société civile, qu'il devient possible de reconstituer les événements — bien qu'il faille reconnaître que plusieurs firmes au sein de l'industrie de la cybersécurité se montrent également de plus en plus évasives dans ce qui s'apparente à une volonté de préserver leurs intérêts corporatifs.

Or, il ne faudrait pas y voir une simple répartition de la tâche. Le manque de transparence du gouvernement canadien a des conséquences. Il nuit à la recherche, c'est-à-dire à l'approfondissement des connaissances sur une « menace existentielle » à la sécurité du Canada, selon les mots de la Commission sur l'ingérence étrangère. En outre, en limitant la transmission d'information au public canadien, le gouvernement omet les éléments factuels et contextuels ayant permis au gouvernement de tirer sa conclusion sur les événements. Les conclusions du gouvernement doivent être acceptées sur la base d'un argument d'autorité — parce qu'Ottawa le dit — plutôt que partagées et comprises par le public.

Cette forme de non-communication favorise la contestation — incluant celle aux fondements douteux — et nuit au sain débat public sur la gestion gouvernementale. Ainsi, alors que Washington annonçait en décembre 2024 avoir été victime de la plus grande cyberattaque de son histoire, Ottawa est resté silencieux. Pourtant, Salt Typhoon, le groupe responsable de l'attaque, est actif depuis quelques années et s'est attaqué au Canada, parmi d'autres cibles de choix. Plusieurs expert-e-s rappellent également que les réseaux de communication canadiens partagent les mêmes vulnérabilités que ceux déployés aux États-Unis. S'il s'avérait exact que le Canada ait été épargné, l'attaque aurait pu à tout le moins servir d'occasion pour expliquer pourquoi il l'a été.

Certes, la transparence peut imposer des contraintes opérationnelles pour les institutions de sécurité, en dévoilant par exemple les tactiques et stratégies des autorités, ce dont le gouvernement canadien se réclame pour justifier son mutisme. Toutefois, cette contrainte existe également ailleurs. La responsable du centre américain de cybersécurité, la CISA, n'était nullement enthousiaste à l'idée de révéler l'existence de la cyberattaque de Salt Typhoon. Cela n'a pas empêché le gouvernement américain de faire preuve de transparence, avec tous les risques et contraintes que cette décision imposait.

Le partage d'information est fondé sur une relation de confiance entre les interlocuteur-trice-s. En s'enfermant dans le secret, les institutions de sécurité montrent qu'elles font peu, voire pas, confiance au public canadien. Ce manque de confiance, qui frisait la condescendance, chez le rapporteur spécial sur l'ingérence étrangère David Johnston, est délétère pour la recherche, le débat public et, plus largement, la consolidation de la cohésion sociale au Canada. Or, à l'heure où la légitimité des gouvernements est constamment remise en question, il faut se joindre à la Commission sur l'ingérence étrangère pour appeler à une plus grande transparence du gouvernement : « L'expérience de la Commission démontre qu'il est possible de rendre publiques beaucoup d'informations sans porter préjudice à la sécurité nationale ». Nous ne pouvons qu'espérer qu'Ottawa s'engagera à l'avenir à un meilleur dialogue avec la société civile.

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.

Typologie des incidents et leurs définitions

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

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

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

Montage couverture : Françoise Conea