UQÀM

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

CYBERINCIDENTS GÉOPOLITIQUES AU CANADA

État des lieux 2026

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, et Simon Hogue, professeur de science politique à l'UQAM, l'OCM rassemble des chercheur-e-s étudiant les transformations de la conflictualité internationale. Les cyberattaques, les manipulations de l'information, la géoéconomie, et les ingérences politiques ou électorales figurent parmi les principaux thèmes étudiés par l'OCM. Contribuant au développement d'une réflexion canadienne sur ces enjeux au moyen de publications scientifiques et grand public, de conférences et colloques et d'interventions médiatiques, l'OCM informe et sensibilise sur la manière dont les mutations sécuritaires contemporaines, notamment l'usage malveillant des technologies numériques, affectent des États comme le Canada, leur gouvernement, la société civile, le secteur privé et les citoyennes et citoyens.

Les auteur-e-s

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

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

Walid Ferguen est chercheur en résidence à l'Observatoire des conflits multidimensionnels et coordonnateur à l'Observatoire sur le Moyen-Orient et l'Afrique du Nord de la Chaire Raoul-Dandurand. Candidat à la maîtrise en science politique à l'UQAM, il s'intéresse aux conflits contemporains, aux dynamiques sécuritaires au Moyen-Orient, en Afrique du Nord, ainsi qu'aux enjeux de renseignement, d'ingérence étrangère et de guerre informationnelle. Il est également chercheur émergent au Réseau d'analyse stratégique (RAS).

Philippe Marchand est chercheur en résidence et coordonnateur à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand. Étudiant à la maîtrise en science politique à l'UQAM, il se spécialise sur les technologies de communication numériques en temps de guerre et sur les cyberattaques sur les infrastructures physiques.

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.

Avec des contributions de

Alexis Rapin est chercheur associé 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. il est également membre du comité éditorial du Rubicon, une plateforme francophone d'analyse des questions internationales.

Danny Gagné est professeur adjoint au Département des humanités et sciences sociales du Collège Militaire Royal de St-Jean où il enseigne la science politique dans le programme d'études internationales. Il est également chercheur associé à la Chaire de recherche sur la Force de réserve du CMR St-Jean, au réseau CRITIC et à l'Observatoire des conflits multidimensionnels de la Chaire Raoul Dandurand, où il travaille sur les questions de cybersécurité et de désinformation.

Quelques incidents marquants 2025

COMPROMISSION D'APPAREILS CISCO PAR SALT TYPHOON

Février

Entre décembre 2024 et janvier 2025, le groupe de cyberespionnage Salt Typhoon, aligné sur les intérêts de l'État chinois, aurait mené six attaques contre des opérateurs de télécommunication et des universités. Plus de 1000 appareils localisés dans plusieurs pays, dont le Canada, auraient été visés grâce à l'exploitation de vulnérabilités connues dans des équipements réseau Cisco.

CONTENU GÉNÉRÉ PAR INTELLIGENCE ARTIFICIELLE SUR YOUTUBE LORS DE L'ÉLECTION FÉDÉRALE DE 2025

Mars

En avril 2025, pendant les élections fédérales canadiennes, 42 chaînes YouTube auraient diffusé 771 vidéos à caractère politique générées par intelligence artificielle (IA). Selon le DFRLab, ces contenus reprenaient la facture visuelle de médias canadiens pour paraître plus crédibles. L'équipe de recherche estime que les chaînes étaient probablement coordonnées et observent un biais en faveur de Pierre Poilievre au détriment de Mark Carney.

CYBERATTAQUE CONTRE LA CHAMBRE DES COMMUNES

Août

Le 8 août 2025, un acteur malveillant inconnu aurait obtenu un accès non autorisé à une base de données de la Chambre des communes du Canada. Selon CBC News, les données compromises incluraient des informations sur du personnel et des appareils informatiques du gouvernement. L'attaque survient peu après la divulgation de deux failles *zero-day* touchant des produits Microsoft.

OPÉRATION D'INFLUENCE DE COPYCOP PORTANT SUR LE SÉPARATISME ALBERTAIN

Septembre

Insikt Group affirme, dans un rapport diffusé le 9 mai, que le groupe COPYCOP, lié à Moscou, mène des opérations d'influence appuyées par l'IA. Actif en Europe et aux États-Unis, le réseau aurait aussi ciblé le Canada dès septembre, notamment via des faux médias et des sites web favorisant le séparatisme albertain après l'élection fédérale de 2025.

ABUS DE SYSTÈMES DE CONTRÔLE INDUSTRIELS ACCESSIBLES DEPUIS INTERNET PAR DES HACKTIVISTES

Octobre

En octobre dernier, le Centre canadien pour la cybersécurité a recensé trois cyberattaques visant des infrastructures canadiennes utilisant des systèmes de contrôle industriels accessibles en ligne. Les incidents ont touché une usine de traitement de l'eau, une entreprise pétrolière et gazière ainsi qu'une ferme. Aucun responsable n'a été identifié, mais les autorités soulignent les risques liés aux hacktivistes exploitant ces vulnérabilités.

CAMPAGNE DE FRAUDE ET DE CYBERESPIONNAGE DE FAMOUS CHOLLIMA

Décembre

Depuis 2018, des membres du groupe de menace persistante avancé nord-coréen Famous Chollima infiltrent des grandes entreprises internationales en se faisant embaucher par celles-ci, sous de fausses identités américaines. Les salaires obtenus seraient transférés à Pyongyang tandis que les membres du réseau mèneraient aussi des vols de données sensibles. L'usage accru de modèles d'IA comme ChatGPT et Claude aurait amplifié cette pratique en 2025.

Le Canada et les cyberincidents géopolitiques à l'horizon 2026

Entre la démission de son ex-premier ministre et une élection fédérale marquée par des menaces d'annexion américaine, en passant par son appui continu à l'Ukraine et son rapprochement avec la Chine, le Canada a vécu une foule de rebondissements politiques et géopolitiques majeurs en 2025. Les tensions provoquées par ces nouvelles fractures, tant nationales qu'internationales, revêtent une dimension cyber plus significative que jamais. Dans un paysage numérique marqué par la sophistication des outils d'intelligence artificielle générative et une multiplication des attaques contre les infrastructures critiques à l'échelle mondiale, le Canada demeure une cible importante de la cyberconflictualité. Le **désinvestissement** massif de l'Agence de cybersécurité et de sécurité des infrastructures par le gouvernement Trump laisse le Canada d'autant plus vulnérable dans un environnement numérique fortement intégré.

Désinformation, cyberespionnage et cybersabotage : voici quelques-uns des thèmes abordés dans ce sixième rapport de l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand sur les cyberincidents à caractère géopolitique ciblant le Canada. Cette publication brosse un portrait des campagnes cyber qui se sont déroulées en 2025, année où notre équipe a recensé le plus d'événements de ce genre. Sans prétendre à l'exhaustivité, nous avons recensé au cours de la dernière année 20 incidents de cyberespionnage, de manipulation de l'information, de doxing, et de reconnaissance contre des individus, la société civile, le secteur public et le secteur privé au Canada.

Depuis 2010, le répertoire des cyberincidents canadiens de la Chaire Raoul-Dandurand — dont sont tirées les données de ce rapport — a recensé 145 cyberincidents à caractère géopolitique ayant visé le Canada. Ces chiffres reposent uniquement sur des sources ouvertes et ne représentent qu'une partie des activités numériques malveillantes observées au pays.

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

Les incidents décrits 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.

Que nous apprennent ces incidents sur leur nature, leurs cibles ou encore leur provenance ? Voici un aperçu général des phénomènes abordés dans ce rapport.

Quels types de cyberincidents sont les plus fréquents ?

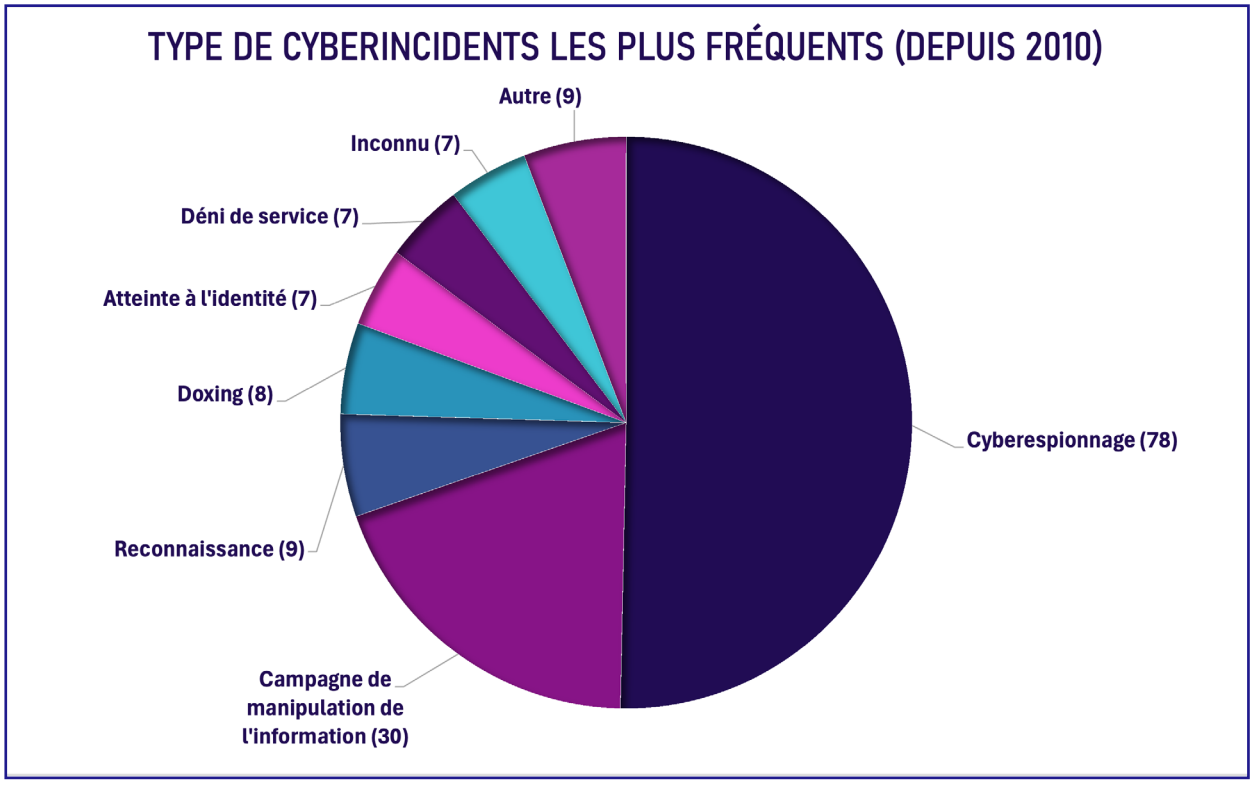
En 2025, le cyberespionnage et les campagnes de manipulation de l'information ont atteint le sommet du palmarès des types d'incidents les plus souvent perpétrés au Canada, avec neuf et huit cas, respectivement.

Si le nombre total de cas de cyberespionnage recensés en 2025 n'augmente que légèrement par rapport à 2024, les campagnes de manipulation de l'information, elles, ont été multipliées par quatre en un an. Cette recrudescence peut s'expliquer en partie par le contexte électoral chargé en 2025 au Canada : la course à la chefferie du Parti libéral en mars et l'élection fédérale en avril ont suscité leur lot de tentatives d'influence prenant la forme de campagnes de manipulation de l'information.

La progression du nombre de campagnes de manipulation de l'information peut aussi s'expliquer par l'utilisation croissante des outils d'intelligence artificielle générative pour créer, entres autres, des images synthétiques par IA. Parmi les huit cas d'opérations de ce type répertoriés en 2025, au moins trois ont reposé sur l'utilisation de l'IA pour la production de contenu diffusé en sol canadien. L'un de ces cas de désinformation, en marge de l'élection fédérale canadienne d'avril, a consisté à utiliser l'IA pour créer des hypertrucages à caractère sexuel visant une influenceuse politique issue de la diaspora chinoise, une première au Canada.

En plus de faciliter la création et d'accélérer la diffusion de contenu fallacieux, l'IA agit comme un multiplicateur de forces pour d'autres types d'opérations. Par exemple, lors des deux campagnes de cyberespionnage nord-coréennes recensées en sol canadien en 2025, l'IA a été utilisée en prélude aux intrusions informatiques pour appâter des victimes à l'aide de fausses offres d'emploi.

Fait intéressant, 2025 représente également la première entrée dans le répertoire d'un cas de cybersabotage, perpétré par un groupe hacktiviste contre trois entités basées au Canada, dont une entreprise pétrolière et gazière. Même si nous disposons de peu d'informations sur l'incident, notamment sur son origine et les motivations de l'attaquant, l'émergence de ce type d'événement au pays — surtout dans les secteurs critiques — suggère que les adversaires du Canada deviennent de plus en plus actifs dans le cyberespace.



* Des cas peuvent cumuler simultanément plusieurs types d'incidents.

Source : Répertoire des cyberincidents canadiens

Quelles sont les cibles connues ?

Année après année, le secteur public reste la cible la plus fréquente au Canada pour les acteurs malveillants liés, directement ou indirectement, à des intérêts étatiques étrangers. L'année 2025 ne fait pas exception.

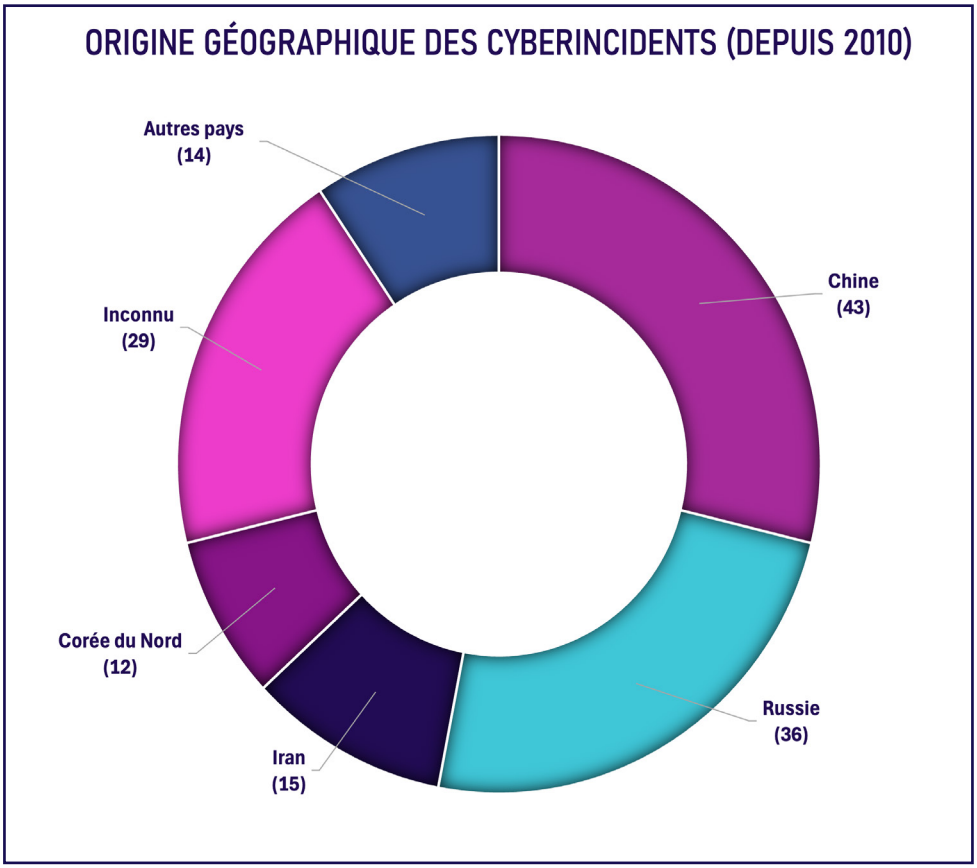
Secoué par une série de bouleversements politiques, incluant la démission du premier ministre Justin Trudeau, la course à la chefferie du Parti libéral et une élection fédérale sous la menace d'annexion du Canada formulée par le président des États-Unis, le gouvernement fédéral a été la cible d'attaques majeures en 2025. À l'été, la Chambre des communes a été visée par une campagne de **cyberespionnage**. En octobre, le gouvernement s'est également retrouvé parmi les nombreux États victimes d'une large opération de **reconnaissance** menée par un groupe originaire d'Asie afin d'identifier les failles potentielles au sein de ses infrastructures numériques.

Des acteurs majeurs de la classe politique canadienne ont aussi été ciblés par des efforts de déstabilisation étrangère. L'ex-vice première ministre **Chrystia Freeland** a fait l'objet d'une opération d'influence chinoise sur la plateforme WeChat alors qu'elle se portait candidate à la chefferie du Parti libéral en février. Le premier ministre **Mark Carney** a été visé par une opération d'influence chinoise en avril, dans le contexte de l'élection fédérale. De façon plus générale, l'électorat canadien a été pris pour cible lors de diverses campagnes d'influence autour d'enjeux comme le **séparatisme albertain** en septembre ou encore **l'élection fédérale** dès le mois de janvier. Malgré tout, le **gouvernement canadien** a confirmé qu'aucun acte d'ingérence étrangère n'est parvenu à miner l'intégrité du déroulement des élections.

La société civile n'a pas été épargnée en 2025. En plus de la campagne de salissage visant l'influenceuse politique chinoise mentionnée précédemment, l'activiste ouïghour-canadien Mehmet Tohti a été victime d'une tentative de vol d'identifiants de la part d'un groupe lié à la Chine en avril 2025, tandis qu'un journaliste iranien a été ciblé par une campagne pro-iranienne de doxing à l'été 2025. Tel que nous l'indiquions dans notre **rapport de 2024**, la répression transnationale représente une menace grandissante à la démocratie canadienne — une conclusion partagée par la juge Marie-Josée Hogue, qui a présidé la Commission d'enquête sur l'ingérence étrangère et qui a qualifié cette menace de « véritable fléau » au pays.

D'où proviennent ces attaques ?

Selon nos données, la Chine reste au sommet du palmarès des États perpétrant le plus d'opérations cyber au Canada, avec un total de 43 cas depuis 2010, suivie de la Russie (36 cas), de l'Iran (15 cas) et de la Corée du Nord (12 cas). Ces données portent sur l'origine géographique des cyberincidents, ce qui ne signifient pas nécessairement que les gouvernements des pays concernés en sont responsables (voir la section méthodologie pour plus de précisions).



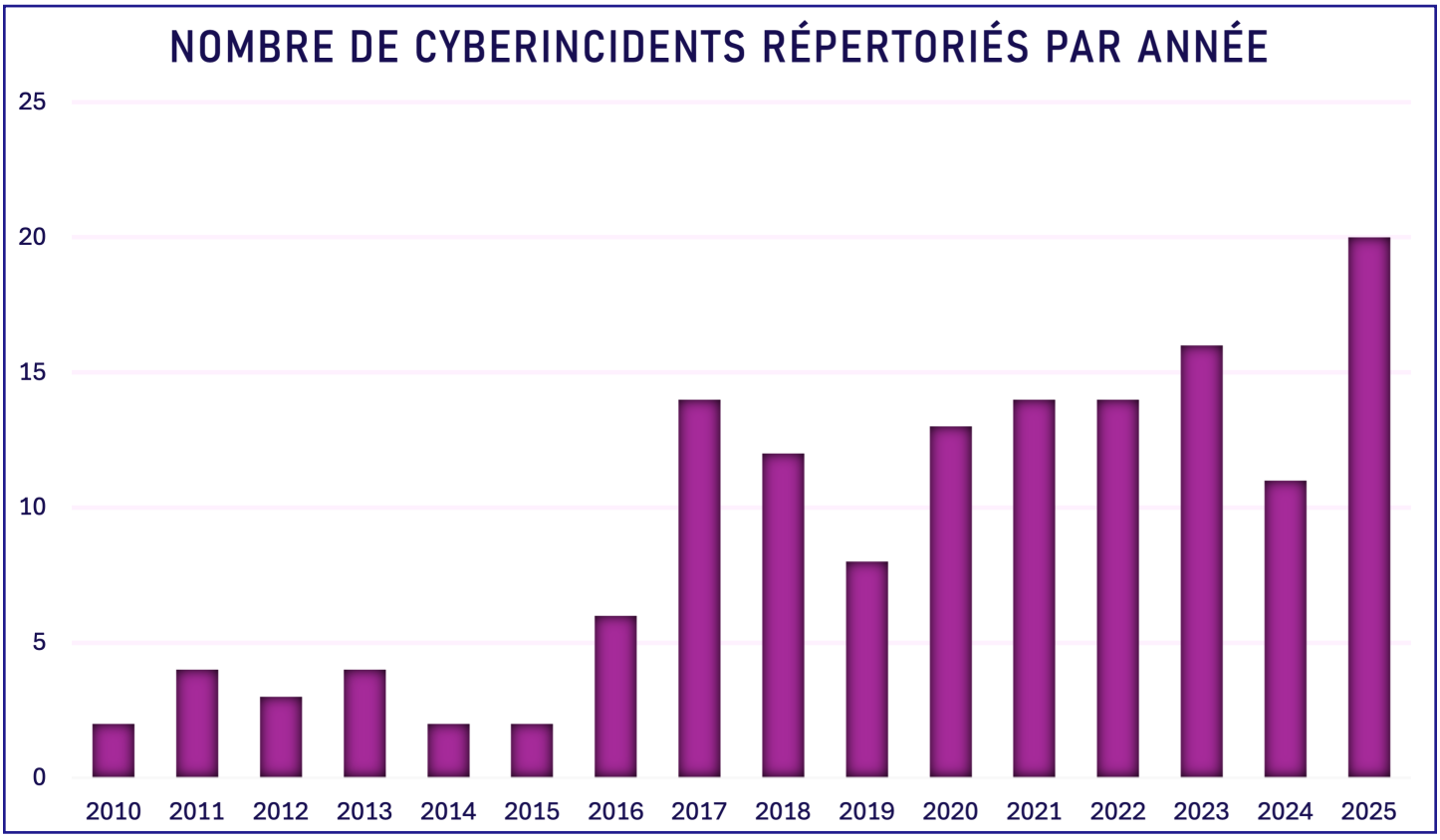
*À noter qu'un incident peut simultanément être perpétré par plusieurs acteurs d'origines différentes

Au-delà des quatre acteurs susmentionnés, nous notons, pour la deuxième année d'affilée, une opération d'influence **israélienne** ayant visé le Canada. Bien que son ampleur ait été nettement inférieure à celle observée **en 2024**, cet incident illustre néanmoins une tendance : même des États alliés peuvent chercher à influencer l'opinion publique au pays.

L'attribution de campagnes cyberoffensives à un groupe de pirates informatiques ou à un État reste une question délicate et résolument politique. Certains articles de presse dévoilent des indices quant à l'origine des acteurs malveillants qui perpétuent des cyberattaques en sol canadien. Par exemple, l'attaque par rançongiciel contre le fournisseur d'énergie **Nova Scotia Power** en avril 2025 aurait, selon son PDG, été menée par un groupe basé **en Russie**. Toutefois, en l'absence d'attribution officielle de la part de firmes de cybersécurité ou du gouvernement canadien, nous restons prudents et nous nous abstenons, pour l'heure, d'ajouter ce cas à notre répertoire. Il en va de même pour les **campagnes d'influence** coordonnées et inauthentiques dont l'origine et les motivations des auteurs demeurent inconnues à ce jour.

Finalement, il arrive que tous les signes d'une attaque pointent vers un acteur étatique précis, mais que des contraintes politiques ou de sécurité érigent des barrières à l'attribution. Tel fut le cas pour la campagne « asiatique » de **reconnaissance** de TGR-STA-1030 ayant ciblé le gouvernement canadien en octobre 2025. La firme de cybersécurité Palo Alto, qui a découvert l'existence de la campagne, aurait décidé de ne pas attribuer la responsabilité de l'opération à la Chine, par crainte de **représailles** de la part de Pékin.

Les sections suivantes du rapport proposent une analyse détaillée des principaux cyberincidents géopolitiques ayant affecté le Canada en 2025.



CYBERESPIONNAGE: toujours la principale menace pour le Canada

Comme lors des années précédentes, le cyberespionnage, soit le vol d'information par des moyens numériques, se hisse au sommet des cyberincidents géopolitiques les plus fréquents au Canada en 2025. Au total, neuf cas de cyberespionnage ont été recensés par l'OCM au courant de cette année, contre six cas pour l'année 2024.

Alors que les campagnes de cyberespionnage identifiées en 2024 visaient particulièrement le secteur public et la société civile, c'est le secteur privé qui a été la cible principale de ce type d'activité malveillante en 2025. Parmi les victimes canadiennes, on compte notamment des compagnies technologiques, au moins un opérateur de télécommunications et une entreprise du secteur manufacturier, dont les identités demeurent confidentielles.

Parmi les principaux auteurs de ces campagnes, on retrouve en tête de file la Chine, toujours considérée par le gouvernement fédéral comme « la cybermenace la plus active et la plus **sophistiquée** » contre le Canada. L'ampleur des capacités cyber de Pékin résulte devl'intégration de divers acteurs corporatifs, gouvernementaux et académiques à l'appareil stratégique chinois déployé dans le cyberespace.

> « Alors que la cybermenace chinoise était, pendant bien des années, concentrée sur le vol de propriété intellectuelle, le ciblage de Salt Typhoon et sa capacité de persister à long terme dans les systèmes de télécommunications peut porter à croire que la Chine recourt désormais à une stratégie cyber plus offensive. »

La Russie, entrée dans sa troisième année de guerre contre l'Ukraine en février 2025, poursuit elle aussi ses opérations de cyberespionnage au pays. Selon la firme de cybersécurité **Recorded Future**, Moscou aurait intensifié ses opérations cyber aux États-Unis et au Canada en 2025.

Finalement, le phénomène grandissant des fraudes à l'emploi par des acteurs nord-coréens a également été observé à au moins **deux reprises** au Canada en 2025. Mêlant escroquerie financière et vol de données auprès de particuliers et de compagnies privées, ces campagnes, menées par le groupe de menace persistante avancée Famous Chollima, utilisaient l'IA pour créer des leurres convaincants. Par exemple, lors d'une campagne visant des personnes travaillant dans le **secteur de la technologie**, des offres d'emploi de compagnies fictives générées par IA ont été publiées en ligne. Elles invitaient à répondre à un «test d'entrée» qui, une fois téléchargé sur un appareil, lançait une attaque destinée à voler les données de la victime.

Le tournant Salt Typhoon

L'enjeu du cyberespionnage étatique a également été propulsé aux devants de la scène médiatique américaine à la fin de 2024 et au début 2025 alors que l'on révélait la campagne d'espionnage massive menée par Salt Typhoon visant de multiples services de télécommunications américains, dont les géants Verizon et AT&T. Les spécialistes interrogés par les journalistes suggéraient que l'opération semblait d'une ampleur telle qu'une **douzaine** de pays auraient pu être touchés par le groupe affilié au ministère de la Sécurité d'État chinois. Les révélations subséquentes ont finalement mis en lumière un nombre de victimes beaucoup plus élevé. L'opération de longue durée — amorcée dès 2019 — aurait touché plus de **80 pays**, y compris le Canada. Le gouvernement canadien a **confirmé** à l'été 2025 la compromission de « trois dispositifs réseau enregistrés à une entreprise de télécommunications canadienne » survenue à la mi-février 2025.

Si aucune information précise n'a été dévoilée sur les données dérobées en sol canadien, les révélations

de la presse américaine sur le *modus operandi* de Salt Typhoon aux États-Unis donnent un aperçu des informations qui auraient pu être exfiltrées au Canada. En pénétrant dans les réseaux de télécommunications américains, le groupe de menace persistante avancée aurait réussi à mettre la main sur les **données** de géolocalisation et les métadonnées de millions d'individus, en plus d'espionner le contenu des communications de hauts fonctionnaires américains, dont le président Donald Trump et son vice-président J.D. Vance.

Selon un **communiqué conjoint** des États-Unis, de l'Australie et du Canada, Salt Typhoon aurait également ciblé, au courant de sa campagne, les réseaux des administrations publiques, des transports, de l'hébergement et des infrastructures militaires dans les pays touchés. Les informations ainsi dérobées permettraient aux services de renseignement chinois « d'identifier et de suivre les communications et les déplacements de leurs cibles partout dans le monde ».

Alors que la cybermenace chinoise était, pendant bien des années, concentrée sur le vol de propriété intellectuelle, le ciblage de Salt Typhoon et sa capacité de persister à long terme dans les systèmes de télécommunications peut porter à croire que la Chine recourt désormais à une stratégie cyber plus offensive. Selon le professeur Michael Poznansky et la professeure Erica Lonergan, spécialistes américains en études stratégiques, les récentes opérations cyber des groupes de menace persistante avancée chinois illustrent une volonté de la Chine de se **pré-positionner** au sein des infrastructures critiques des pays visés dans l'objectif de nuire aux structures de commandement et de contrôle en cas de crise.

Le secteur public également visé

Malgré la prédominance des entités du secteur privé parmi les victimes au Canada, le secteur public n'a pas été épargné par les campagnes de cyberespionnage orchestrées par des acteurs étatiques en 2025.

Le 8 août, un groupe de pirates informatiques toujours inconnu du grand public a réussi à obtenir un accès non autorisé à une base de données de la **Chambre des communes**, exfiltrant les noms, les titres de poste, les emplacements des bureaux et les adresses courriel de membres du personnel fédéral, ainsi que des

données liées à la gestion des ordinateurs et des appareils mobiles. Bien que la vulnérabilité spécifique qui a permis le vol de données à la Chambre des communes n'ait pas été divulguée, l'attaque survenait peu de temps après la divulgation des **failles** *zero-day* de Microsoft[1].

Des failles irrémédiables ?

L'exploitation de vulnérabilités *zero-day* est toutefois loin de représenter la seule porte d'entrée pour les acteurs malveillants affiliés à des États. Dans une majorité de cas, les groupes de menace persistante avancée exploitent des vulnérabilités « n-day », c'est-à-dire des failles de sécurité pour lesquelles il existe des correctifs, mais qui n'ont toujours pas été mis en œuvre par les utilisateurs et utilisatrices.

De telles failles ont été exploitées à de nombreuses reprises au Canada, comme lors de la campagne opportuniste de cyberespionnage du groupe de pirates étatiques russes **Sandworm**, révélée en février 2025, ou encore lors de la campagne de cyberespionnage de Salt Typhoon mentionnée précédemment. En effet, le Centre canadien pour la cybersécurité a certes dévoilé la vulnérabilité (2023-20198 CVE) exploitée par le groupe de menace persistante avancée chinois, mais l'agence gouvernementale omet toutefois de mentionner qu'un **correctif** pour cette faille était disponible depuis octobre 2023. Cela signifie qu'une période de deux ans et quatre mois s'est écoulée entre la possibilité de corriger la vulnérabilité et son exploitation par l'acteur malveillant, témoignant de la négligence de l'opérateur de télécommunications visé par l'attaque.

Dans un **rapport** d'octobre 2025 sur la cybersécurité des réseaux et des systèmes gouvernementaux, la vérificatrice générale du Canada souligne que le gouvernement fédéral n'est pas davantage à l'abri des vulnérabilités connues. D'importantes lacunes persistent dans la cyberdéfense du gouvernement canadien. Ont notamment été pointés du doigt le manque de coordination entre les différentes agences responsables de la cybersécurité au sein de l'appareil fédéral — une faille importante ayant permis à un attaquant « d'accéder de façon prolongée à des renseignements personnels » lors d'un incident survenu en janvier 2024 — ainsi que l'absence d'un inventaire complet de l'ensemble des biens en technologie de l'information du gouvernement, alors même que près de dix ans se sont écoulés depuis le lancement de l'initiative visant à les répertorier. De telles lacunes font état d'une vulnérabilité évidente face à la menace du cyberespionnage étatique pourtant reconnue depuis des années au Canada.

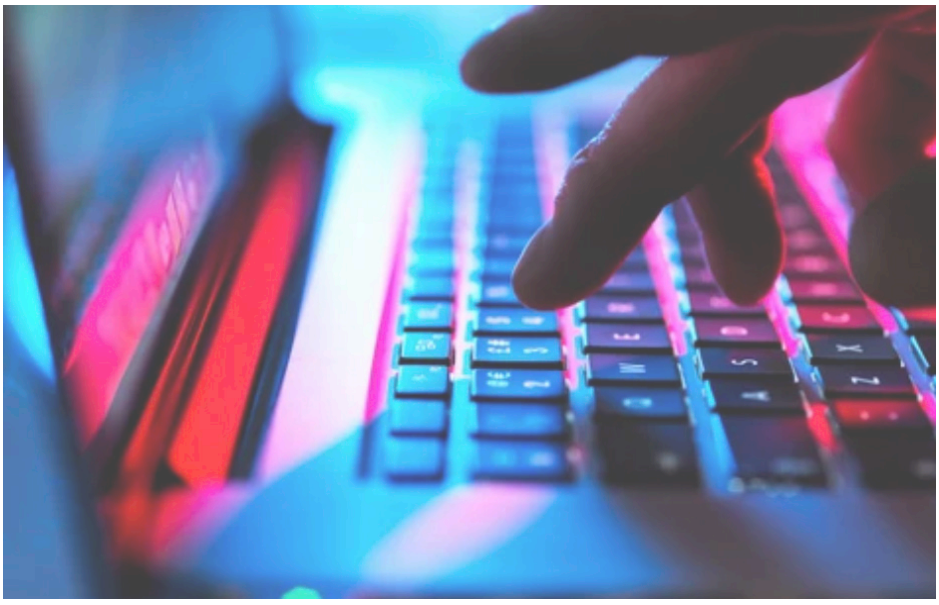
1 Un type de vulnérabilité rare, mais extrêmement efficace, vu qu'aucune mise à jour de sécurité n'existe pour la corriger au moment de sa découverte.

La campagne de cyberespionnage de RomCom contre une entreprise du secteur manufacturier

Une campagne de cyberespionnage a visé une entreprise canadienne du secteur manufacturier **à l'été 2025**, après qu'un employé de celle-ci ait téléchargé une fausse candidature reçue dans un courriel à l'apparence anodine.

Derrière l'attaque se trouve le groupe de menace persistante avancée RomCom, affilié à la Russie, qui a également réussi à s'introduire dans les systèmes d'entreprises financières, manufacturières, de défense et de logistique basées en Europe durant sa campagne. En convainquant du personnel des organisations ciblées de télécharger de fausses candidatures, RomCom parvenait à faire lancer par les victimes elles-mêmes, via un simple clic, la chaîne d'attaque, déployant à leur insu un fichier malveillant dans leurs systèmes informatiques. La faille exploitée par RomCom ciblait le logiciel de compression de données très répandu WinRAR, pour lequel le développeur a rapidement déployé un correctif de sécurité après en avoir été informé.

Bien qu'il soit complexe de déterminer les liens exacts entre le Kremlin et le groupe de pirates informatiques visant le Canada, l'exploitation par RomCom de multiples failles zero-day au cours des dernières années porte l'équipe d'ESET, une firme de cybersécurité, à croire que le groupe possède d'importants moyens financiers[2]. S'adonnant à des activités cybercriminelles financièrement motivées comme des attaques par rançongiciel, l'organisation, aussi connue sous les noms Storm-0978, Tropical Scorpius et UNC2596, a également commencé à mener des opérations d'espionnage contre des organisations ukrainiennes à partir de 2022, ce qui étaye la thèse d'une collaboration avec Moscou.



RomCom avait déjà mené une campagne d'espionnage au Canada **en 2024** en exploitant des vulnérabilités précédemment inconnues dans des produits Mozilla et Microsoft. Les tactiques utilisées par RomCom durant son attaque à l'été 2025 laissent présager que son objectif était de subtiliser de l'information stratégique au bénéfice de Moscou.

Fanny Tan

2 Entrevue avec Damien Schaeffer, chercheur sénior chez ESET (19 août 2025).

DÉSINFORMATION AUGMENTÉE: le Canada à l'ère de l'ingérance par IA

L'année 2025 marque une intensification des ingérences informationnelles visant le Canada. Dans ce rapport, neuf cas de manipulation de l'information ont été recensés, contre seulement deux l'an dernier. Toutefois, ce qui distingue 2025 n'est pas l'existence du phénomène, documenté depuis plusieurs années, mais la convergence simultanée de trois dynamiques qui en transforment l'échelle et la nature.

La première dynamique est technologique : la démocratisation des outils d'intelligence artificielle générative a atteint un niveau d'accessibilité tel qu'elle facilite aujourd'hui la production massive de désinformation. Textes automatisés, images manipulées et hypertrucquées imitant des médias établis peuvent désormais être produits à coût marginal. L'IA agit à la fois comme outil de production et comme multiplicateur de diffusion, en augmentant le volume et la vitesse de circulation des contenus trompeurs, tout en en renforçant la plausibilité et en réduisant les indices permettant d'en détecter le caractère artificiel.

La deuxième dynamique est politique : la démission du premier ministre Justin Trudeau, le retour de Donald Trump à la présidence des États-Unis et ses menaces d'annexion du Canada, ainsi qu'une élection fédérale se déroulant dans un climat d'incertitude, ont ouvert des espaces d'exploitation à des acteurs extérieurs désireux d'exacerber certaines tensions et inquiétudes au sein de la population canadienne.

La troisième dynamique est géopolitique : les conflits en Ukraine et à Gaza, les tensions entre Israël, les États-Unis et l'Iran ou encore les rivalités entre la Chine et Taïwan donnent lieu à une intensification des opérations d'influence à travers le monde, marquée, entre autres, par la diffusion de contenus trompeurs et l'amplification de narratifs clivants. En raison de ses positions diplomatiques et de son alignement avec ses alliés, le Canada est directement touché par ces phénomènes et figure parmi les cibles de certaines campagnes d'influence.

L'automatisation de la désinformation

Une augmentation marquée des campagnes d'influence reposant sur l'intelligence artificielle a d'ailleurs a été observée dans ce rapport.

Lors de l'élection fédérale d'avril 2025, le **Digital Forensic Research Lab (DFRLab)** a identifié 42 chaînes YouTube coordonnées ayant publié 771 vidéos générées par IA, imitant la facture visuelle de médias canadiens établis et affichant un biais systématique contre le chef libéral Mark Carney. La coordination de ces chaînes, dont trois publiaient simultanément des vidéos au titre identique, révèle une architecture de diffusion automatisée orientée vers un objectif politique précis, notamment en faveur du chef conservateur Pierre Poilievre et du mouvement séparatiste en Alberta.

> « Le problème ne repose pas uniquement sur la capacité des individus à distinguer le vrai du faux, mais sur celle des institutions à réguler un environnement informationnel en mutation rapide. »

Plus tôt dans l'année, TikTok a détecté **76 comptes inauthentiques** ciblant l'élection canadienne ont été détectés. Ceux-ci se faisaient passer pour des utilisateurs et utilisatrices de plusieurs pays afin de promouvoir des contenus associés à des idéologies extrémistes, sans que leur identité précise ne soit rendue publique.

Par ailleurs, le groupe russe COPYCOP a attiré l'attention de la firme de cybersécurité Insikt Group en mai 2025 en raison de ses activités en Europe et aux États-Unis. En septembre, il étend **ses opérations au Canada** en créant de faux sites médiatiques et des pages promouvant notamment le séparatisme albertain. Ce cas illustre la facilité avec laquelle une

infrastructure d'influence peut être redéployée d'un contexte à un autre en fonction de l'actualité. Ces trois opérations partagent des traits communs révélateurs. Elles exploitent des fractures politiques préexistantes au Canada, qu'il s'agisse des tensions partisanes autour de l'élection fédérale, de la méfiance envers certaines institutions ou du débat sur l'unité nationale. Elles mobilisent toutes l'IA comme outil de production à grande échelle et ciblent des plateformes à fort trafic pour maximiser leur portée. Leurs origines géographiques diffèrent, mais leur logique converge vers l'intention de saturer l'espace informationnel canadien avec des contenus clivants pendant une période de vulnérabilité politique.

Ces incidents mettent en évidence un défi qui dépasse la simple question technique de la détection des contenus. Ils révèlent un enjeu institutionnel plus large : dans quelle mesure les sociétés démocratiques disposent-elles des mécanismes nécessaires pour anticiper, encadrer et répondre à une production massive et automatisée de désinformation ? Le problème ne repose pas uniquement sur la capacité des individus à distinguer le vrai du faux, mais sur celle des institutions à réguler un environnement informationnel en mutation rapide.

Le recul de la modération sur les grandes plateformes — entre autres avec **le démantèlement de certains programmes de vérification des faits** chez Meta en janvier 2025 — ne marque pas la fin du *fact-checking*, mais son repositionnement vers des mécanismes plus décentralisés, reposant davantage sur les personnes utilisatrices. Dans un contexte marqué par le retour au pouvoir de Donald Trump et par le **refus américain** de participer à tout régime international de régulation de l'intelligence artificielle, cela contribue à créer un environnement où les acteurs malveillants agissent avec une latitude et une impunité croissante.

Le Canada, bien qu'il dispose déjà de mécanismes encadrant les propos mensongers et diffamatoires en contexte électoral, ne s'est pas encore doté d'un dispositif législatif explicitement adapté aux usages de l'IA, notamment en matière de manipulation des voix et des images. Cette situation contraste avec **certaines initiatives internationales** visant à encadrer plus directement ces pratiques et contribue à maintenir une zone d'incertitude dans la réponse institutionnelle à ces nouvelles formes de désinformation.

Le ciblage politique du débat public canadien

Deux incidents impliquant des opérations présumément chinoises sur WeChat révèlent une stratégie persistante d'ingérence visant des processus politiques distincts au Canada, soit une course à la chefferie partisane et une élection générale. En février 2025, le **Mécanisme de réponse rapide (MRR) d'Affaires mondiales Canada** révèle qu'une trentaine de comptes coordonnés ont ciblé Chrystia Freeland, candidate à la chefferie libérale, générant plus de 140 000 interactions et exposant 2 à 3 millions de comptes à des contenus dénigrants envers la politicienne. Quelques semaines plus tard, en pleine campagne électorale au Canada, le **Bureau du Conseil privé** confirme une opération similaire visant Mark Carney, exposant entre 1 et 3 millions d'internautes à des narratifs ciblant la diaspora chinoise canadienne. La réapparition de profils qui avaient déjà été mobilisés contre le député conservateur Michael Chong en 2023 — en particulier le canal WeChat Youli-Youmian — confirme l'existence d'une infrastructure d'influence entretenue sur plusieurs années et activée ponctuellement d'une élection à l'autre.

Ces opérations révèlent une logique d'ingérence structurée qui ne vise pas à convaincre l'ensemble de l'opinion publique canadienne, mais à cibler des communautés spécifiques en exploitant les canaux numériques qui leur sont propres, comme en témoigne la dissémination de contenus fallacieux sur WeChat. Cette plateforme constitue un espace clé pour une partie de la diaspora chinoise au Canada qui s'y informe, y échange et y entretient des liens avec son

pays d'origine, puisqu'elle constitue souvent l'un des rares moyens de communiquer avec des proches restés en Chine. Diffuser des contenus malveillants de manière coordonnée dans cet espace permet d'intervenir au sein d'un environnement communautaire relativement fermé et perçu comme fiable. Cet espace est par ailleurs marqué par des barrières linguistiques et une visibilité limitée pour les acteurs extérieurs, ce qui peut nuire à la détection de ces campagnes par les autorités canadiennes.

Cette forme d'ingérence met en évidence la vulnérabilité de la souveraineté démocratique du Canada, Ottawa n'étant pas toujours en mesure de contrer les atteintes à l'intégrité des processus politique et électoral canadiens.

« Le choix de cibler un aéroport n'est pas anodin, car il s'agit d'un espace hautement régulé, associé à la sécurité, à la mobilité et à la présence de l'État. »

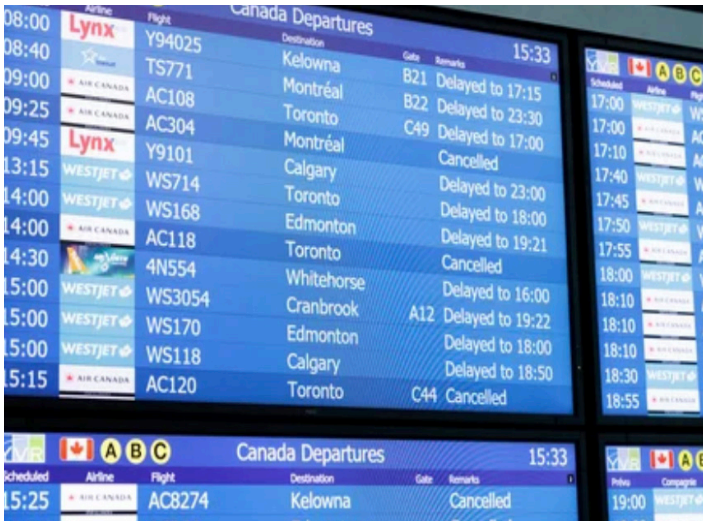
L'hybridation entre intrusion numérique et manipulation de l'information

Le 14 octobre 2025, les systèmes de sonorisation et les écrans d'information de plusieurs aéroports canadiens, notamment ceux de **Windsor**, Kelowna et Victoria, ont été piratés afin de diffuser des messages pro-Hamas et des allusions à un « deuxième 11 septembre ». Même si le contenu précis des messages n'a pas pu être confirmé dans l'ensemble des aéroports concernés, l'attaque a été revendiquée par le groupe de pirates informatiques Mutariff Siberislam et n'a pas eu de conséquence directe sur la sécurité aérienne.

Cet incident se distingue toutefois des précédents cas évoqués : il ne repose pas sur la fabrication de contenus trompeurs diffusés en ligne, mais sur l'exploitation d'infrastructures physiques comme vecteurs de diffusion d'un message politique transnational. Il s'inscrit ainsi dans une hybridation croissante entre cyberattaques à visée technique et opérations informationnelles à portée psychologique, où l'objectif ne semble pas tant de convaincre que d'intimider et de marquer les esprits.

Le choix de cibler un aéroport n'est pas anodin, car il s'agit d'un espace hautement régulé, associé à la sécurité, à la mobilité et à la présence de l'État. Y diffuser des messages hostiles revient à exploiter un lieu de confiance et hautement sécurisé pour en faire un vecteur de perturbation symbolique. Cette intrusion, même limitée sur le plan technique, produit un effet psychologique notable en exposant la vulnérabilité apparente d'infrastructures critiques et en semant le doute sur la capacité des autorités à en assurer la protection.

Cet incident met en lumière l'élargissement des modes d'action des acteurs malveillants, capables non seulement de s'introduire dans des systèmes numériques, mais aussi d'exploiter leur visibilité pour produire un effet informationnel amplifié. Il renforce également les analyses portant sur les logiques de prépositionnement, où l'accès préalable à certaines infrastructures peut être mobilisé de manière opportuniste pour générer un impact politique ou symbolique, sans nécessiter une perturbation majeure des fonctions techniques des lieux visés.



Enfin, cet événement montre que les conflits mondiaux ont des répercussions informationnelles en sol canadien, bien au-delà de leur lieu d'origine, certains groupes n'hésitant pas à utiliser des espaces du quotidien au Canada pour diffuser des messages à portée internationale.

Campagne de Spamouflage contre des membres de la diaspora chinoise

« C'est la première fois que le MRR Canada observe des agents de la campagne de spamouflage utilisant l'IA générative pour lancer et diffuser du contenu sexuellement explicite sur une personne habitant au Canada. »

Affaires mondiales Canada, 27/02/2025

Les événements **documentés** remontent à mai 2024 et ont notamment été signalés entre le 16 et le 19 septembre, période durant laquelle plusieurs individus ont été ciblés au Canada. Ce n'est qu'en février 2025 que le **Mécanisme de réponse rapide du Canada** en révèle l'ampleur, en les rattachant à une campagne menée par Spamouflage, un réseau d'influence prochinois actif depuis plusieurs années et reposant sur l'utilisation de comptes inauthentiques afin de diffuser et d'amplifier des contenus trompeurs en ligne.

Parmi les cibles figure une militante des droits de la personne basée au Canada, dont les activités de sensibilisation sur la situation des Ouïghours et de la diaspora chinoise lui avaient valu une visibilité publique croissante. Les auteurs recourent à des hypertrucages sexuellement explicites générés par IA : l'image et la voix de la militante ciblée sont manipulées pour la faire apparaître dans des situations compromettantes. En parallèle, d'autres contenus de la **même campagne** utilisent l'image d'un commentateur critique pour lui faire prononcer de fausses accusations contre des personnalités canadiennes — Justin Trudeau, Mélanie Joly, Pierre Poilievre — postées massivement dans les commentaires de comptes gouvernementaux et médiatiques. Ces vidéos sont diffusées sur plusieurs plateformes par un réseau de comptes automatisés, à un rythme de 100 à 200 publications par jour.

Les impacts sur la personne ciblée sont **multiples**. Sur le plan réputationnel, les contenus ont miné la confiance de membres de la diaspora chinoise envers la militante, certains choisissant de rompre les liens avec elle. Sur le plan personnel, l'exposition à un volume quotidien de vidéos compromettantes génère une pression continue et délibérée : la personne ciblée doit constamment surveiller, signaler et tenter de contredire des contenus qui se renouvellent plus vite qu'ils ne peuvent être supprimés. Selon Affaires mondiales Canada, l'objectif explicite de la campagne est de « discréditer, dénigrer et harceler » les individus visés afin de les décourager de s'exprimer publiquement.

Sur le **plan civique**, la campagne vise explicitement à réduire au silence une voix critique, en rendant le coût de l'activisme suffisamment élevé pour décourager toute prise de parole publique. Malgré les efforts de suppression des plateformes concernées réalisés par Affaires mondiales Canada, certains contenus continuaient de circuler au moment des révélations, illustrant les limites structurelles de la réponse réactive.

L'effet de cette campagne dépasse par ailleurs les tendances décrites dans cette section. Il ne s'agit pas seulement d'automatiser la désinformation, de cibler le débat électoral ou de compromettre des infrastructures, mais aussi d'exercer une intimidation informationnelle personnalisée contre des individus ordinaires, en mobilisant délibérément des contenus sexuellement explicites comme arme d'intimidation. Cette tactique s'inscrit dans une forme documentée de violence numérique genrée : selon **Reporters sans frontières**, 74 % des hypertrucages ciblant des journalistes et militantes visent des femmes, et selon **ONU Femmes**, ce type de contenu est utilisé spécifiquement pour réduire au silence les femmes qui s'expriment dans l'espace public.

La campagne Spamouflage démontre que l'ingérence étrangère au Canada ne se limite pas aux institutions ou aux figures politiques, mais vise également des individus engagés dans l'espace public. Elle s'attaque ainsi aux personnes qui tentent, depuis la société civile, de maintenir des espaces d'expression indépendants au sein des diasporas, prolongeant des pratiques existantes tout en les adaptant à des formes plus visibles et plus coercitives.

Walid Ferguen

CYBERSABOTAGE ET HACKTIVISME: des menaces croissantes pour les infrastructures critiques canadiennes

Le Canada a été la cible d'actes de cybersabotage notables en 2025. Ceux-ci ont visé une installation de traitement de l'eau, une entreprise pétrolière ainsi qu'une ferme. Les informations publiées laissent entendre qu'il s'agirait d'incidents de gravité mineure. La nouvelle n'en est pas moins préoccupante. Parmi les types de cyberattaques étudiés dans ce rapport, le cybersabotage d'infrastructures critiques est celui qui suscite **les plus grandes inquiétudes auprès des instances décisionnelles publiques**. L'annonce de 2025 risque d'accroître les angoisses des agences de sécurité du pays.

Retour sur l'évolution du cybersabotage

En 2010, une nouvelle a rapidement fait le tour de la planète : les États-Unis et Israël se seraient attaqués aux **centrifugeuses iraniennes** d'enrichissement d'uranium afin de perturber leur capacité à développer l'arme nucléaire.

Fait notable : l'attaque destructrice a été perpétrée via un ver informatique, logiciel malveillant capable de se reproduire par lui-même, développé conjointement par la National Security Agency, la Central Intelligence Agency et l'unité israélienne 8200, une agence spécialisée en renseignement, en cyberguerre et en contre-espionnage. Le virus, aussi connu sous le nom de Stuxnet, était à ce moment le premier cas répertorié publiquement d'une cyberattaque cherchant à compromettre une infrastructure physique.

Depuis cet événement, le nombre de cas de cybersabotages a augmenté à l'échelle mondiale. Pensons, par exemple, à l'attaque du groupe russe Sandworm sur les **infrastructures énergétiques ukrainiennes** en 2014, à la cyberattaque sur l'entreprise d'oléoduc américaine **Colonial Pipeline en 2021**, à l'attaque sur la compagnie publique lithuanienne **Ignitis** en 2022 ou à celle conduite par le groupe **Sandworm** contre diverses entreprises polonaises en 2025.

Ces attaques, peu communes comparativement à d'autres cyberattaques comme le cyberespionnage ou les attaques par déni de service, ont généralement des conséquences bien concrètes qui sont facilement identifiables, notamment le sabotage d'une fonctionnalité de l'infrastructure visée ou encore l'interruption de ses opérations. Elles sont fréquemment motivées par une volonté géopolitique et s'alignent avec les objectifs du pays dont elles proviennent, qu'ils soient pécuniers ou stratégiques. Elles peuvent ainsi prendre diverses formes : cyberattaques sur une entreprise pétrolière afin d'affecter la production énergétique d'un pays ; modification d'une valve de pression d'une station de traitement d'eau afin de suspendre ses services ; abaissement de la température d'une ferme connectée via un système de contrôle industriel dans le but d'en perturber le fonctionnement.

Au cours des dernières années, la Russie a été particulièrement active sur ce plan. Historiquement, son attention s'est surtout portée vers l'Ukraine. Depuis 2014, année de la prise de la Crimée par Moscou, les infrastructures critiques ukrainiennes sont fréquemment ciblées. En parallèle aux moyens de destruction conventionnels déployés dans la guerre, comme les frappes d'artilleries et aériennes, la Russie s'attaque aux infrastructures ukrainiennes par des moyens non conventionnels comme des actes de cybersabotage. Le géant eurasiatique cherche ainsi à créer de l'instabilité chez son voisin afin d'atteindre ses objectifs stratégiques, soit la prise de possession du territoire ukrainien.

Cependant, depuis 2022, on peut voir une évolution dans la stratégie russe. En effet, Moscou ne semble plus seulement se contenter d'agresser son voisin à l'aide de tactiques numériques, mais étend désormais ses assauts sur les pays soutenant l'Ukraine, tant militairement que financièrement. En témoignent les multiples attaques contre les infrastructures du domaine de l'énergie en **Pologne** en 2025 et 2026,

son exploitation des **logiciels Cisco** afin de s'infiltrer au sein des infrastructures critiques aux États-Unis de 2023 à 2025, ou encore les attaques de **Sandworm** contre les infrastructures du domaine de l'énergie, principalement, de multiples pays occidentaux, tant américains qu'européens.

> « On constate donc que divers pays, dont la Russie, utilisent les groupes d'hacktivistes à travers leur financement pour camoufler des actions dont ils ne veulent pas être tenus responsables sur la scène internationale. »

Ces attaques de grande ampleur et coordonnées sont généralement réalisées par des groupes de menace persistante avancée, comme Sandworm, Fancy Bear (affiliés à la Russie) ou WageMole (affilié à la Corée du Nord). Ces groupes de pirates informatiques sont capables de mener des opérations sophistiquées d'envergure perdurant dans le temps. Généralement, ces groupes sont financés par un gouvernement et possèdent donc des ressources importantes pour réaliser leurs activités.

L'hacktivisme en collaboration avec les États

Cependant, il arrive que certains individus ou collectifs recourent à des formes de désobéissance civile sans lien avec un État précis, afin de défendre des idéologies particulières, notamment par le biais de cyberattaques, à l'image du groupe Anonymous, toujours actif aujourd'hui. Comme nous l'avions déjà mentionné dans notre **rapport de 2024**, des groupes d'hacktivistes ciblent régulièrement les intérêts canadiens ou encore aux alliés d'Ottawa. À titre d'exemple, le groupe NoName057(16) s'en était pris à l'Agence canadienne des services frontaliers, provoquant de multiples pannes au sein d'aéroports partout dans le pays. NoName057(16) avait fait parler de lui par l'ampleur et l'assiduité de ses attaques. Le groupe avait effectivement recouru aux attaques par déni de service distribué pour déstabiliser le Canada, parfois à hauteur de 15 attaques par jour sur la même institution, et ce, pendant environ un an.

Bien qu'en 2024, aucun indice ne suggérait de lien direct entre ce « hacker patriotique » russophone et l'appareil gouvernemental russe, de **nouvelles informations publiées en 2025** confirment aujourd'hui cette collaboration. Les groupes NoName057(16), Cyber Army of Russia Reborn, Z-Pentest ainsi que Sector16 ne sont pas directement sous une égide gouvernementale comme les autres groupes de menaces persistantes, mais ils reçoivent tout de même un soutien, direct ou indirect, de la part de l'État russe. Par exemple, le groupe NoName057(16) aurait été créé par le Centre russe d'étude et de surveillance en ligne du milieu de la jeunesse. Divers et complexe, l'écosystème de la cybermenace russe fonctionne un peu à la manière d'une **mosaïque** avec à sa tête le gouvernement qui chapeaute les opérations sans pour autant contrôler dans les détails les actions de ses membres. Ainsi, si certains groupes travaillent directement pour les services de renseignement russes (FSB, GRU ou SVR), d'autres agissent de manière plus indépendante, ayant un accord tacite avec le gouvernement pour cibler des acteurs extérieurs en échange d'une sorte de laissez-passer de Moscou pour agir malgré la nature illégale de leurs opérations. On constate donc que divers pays, dont la Russie, utilisent les groupes d'hacktivistes à travers leur financement pour camoufler des actions dont ils ne veulent pas être tenus responsables sur la scène internationale.

Ciblage de systèmes de contrôle industriels par des hacktivistes

Le 29 octobre 2025, le Centre canadien pour la cybersécurité (CCCS) a émis une alerte faisant état de trois incidents de cybersabotage survenus au Canada : le premier visait les paramètres de pression de l'eau dans une installation de traitement de l'eau, le deuxième concernait une jauge magnétique à lecture directe au sein d'une entreprise pétrolière et gazière, et le troisième portait sur la manipulation des niveaux de température et d'humidité dans le silo de séchage à grain d'une exploitation agricole. Dans les trois cas, les hacktivistes ayant commis les actes ont exploité les vulnérabilités des systèmes de contrôle industriel accessibles depuis Internet afin d'obtenir un accès et un contrôle sur certaines fonctionnalités des institutions et entreprises visées, perturbant leurs activités régulières.

Bien qu'aucun groupe n'ait revendiqué les attaques, le CCCS estime que des actes de ce genre sont à anticiper de la part d'hacktivistes qui chercheraient à attirer l'attention des médias ou encore à discréditer les organisations visées pour porter atteinte à la réputation du Canada.

Comme mentionné précédemment, ce type d'attaque contre des infrastructures critiques est un phénomène récent au Canada et qui s'inscrit dans le contexte géopolitique actuel. Bien que le Canada ne soit engagé dans aucun conflit direct avec un autre État, son soutien financier à certains pays — notamment à l'Ukraine dans sa guerre contre la Russie — peut en faire une cible pour des individus sympathisant avec cette dernière. Dans les trois cas cités plus haut, le Canada n'a cependant pas été en mesure d'attribuer la responsabilité des attaques à des hacktivistes ou un État en particulier.

Pour conclure, la croissance continue de la connectivité à Internet des infrastructures critiques soulève de sérieux enjeux de sécurité. Le gouvernement canadien recommande plusieurs mesures pour renforcer la **sécurité du réseau**, notamment l'isolement des appareils connectés sur des réseaux distincts, l'utilisation de phrases secrètes plutôt que de mots de passe pour accéder aux systèmes informatiques, le recours à l'authentification à deux facteurs, ainsi que l'adoption de technologies intégrant le principe de « **sécurisation dès la conception** ». Non obligatoires, ces recommandations ne sont toutefois pas systématiquement mises en œuvre par les entreprises et les autorités publiques, y compris au sein du gouvernement fédéral.

Philippe Marchand

Conclusion

Entre transparence limitée et menaces croissantes : le Canada dans la tempête des cyberincidents géopolitiques

Des opérations d'influence visant la diaspora chinoise lors des élections fédérales d'avril 2025, des campagnes de cyberespionnage ciblant les secteurs canadiens de l'énergie, des télécommunications et de la défense, ainsi que la diffusion de fausses informations par des groupes russes sur les tensions liées au séparatisme en Alberta ou par des comptes associés à Israël concernant la position d'Ottawa sur le Proche-Orient, illustrent la diversité et la fréquence des cyberincidents géopolitiques ayant touché le Canada en 2025.

Cette année, notre rapport sur les cyberincidents géopolitiques au Canada recense le plus grand nombre d'incidents jamais identifiés par notre équipe de recherche. Loin de constituer un cas isolé, cette tendance montre que le Canada s'inscrit pleinement dans les dynamiques conflictuelles de la géopolitique mondiale actuelle, marquée par une multiplication des affrontements interétatiques, comme en Ukraine et en Iran. Cette conclusion examinera certaines vulnérabilités propres au Canada et dont les autorités canadiennes devront tenir compte au cours des prochaines années.

Transparence opaque sur les cyberincidents au Canada

Sur le plan méthodologique, tirer des conclusions générales sur la base du recensement des cyberincidents à caractère géopolitique est toujours délicat. La principale qualité de notre rapport — mais aussi sa limite — tient à la capacité de notre équipe à compiler et analyser des données en sources ouvertes sur lesquelles nous n'avons aucun contrôle. Nos chercheures et chercheurs scrutent scrupuleusement les annonces, mises à jour et autres rapports rendus publics par le gouvernement canadien — au premier chef, le Centre canadien pour la cybersécurité —, des firmes de cybersécurité et des forums spécialisés concernant les cyberincidents impliquant le Canada. Notre rapport demeure ainsi tributaire d'informations tirées de sources ouvertes.

À ce titre, on observe une augmentation des annonces sur les cyberincidents touchant le Canada, ce qui pourrait indiquer une plus grande transparence dans la divulgation des risques pour le pays. Cependant, cette dynamique est contrebalancée par un mouvement inverse : nos gouvernements et les entreprises se limitent à partager un minimum d'informations, insuffisant pour analyser en profondeur les événements, éclairer les décideurs en matière de sécurité publique et anticiper l'avenir. Les déclarations laconiques, justifiées au nom de la sécurité nationale ou afin de ne pas nuire à des intérêts économiques privés, se résument souvent à une ou deux phrases, comme en témoigne par exemple la courte **déclaration officielle** du Mécanisme de réponse rapide du Canada suite à la détection d'une opération de manipulation de l'information ciblant l'élue libérale Chrystia Freeland en février 2025. Les firmes privées traditionnellement volubiles s'engagent également sur cette voie. D'ailleurs, les demandes d'accès à l'information que nous avons réalisées ont requis des efforts et une énergie disproportionnés par rapport à la faible quantité d'informations pertinentes obtenues.

Bref, la transparence quant aux menaces de cyberincidents au Canada demeure bien opaque. Au risque de répéter une partie de la conclusion de notre rapport de 2024, il convient de rappeler le constat sans équivoque auquel en est venue la **Commission sur**

l'ingérence étrangère au Canada dans son rapport final :

> « *Une plus grande transparence permettrait au Canadiennes et aux Canadiens de ne pas dépendre entièrement des médias et des fuites d'informations (qui peuvent facilement être trompeuses ou mal comprises) pour être informés des tentatives ou des actes d'ingérence étrangère. […] Le risque de fuites augmente si les agences gouvernementales gardent ces incidents presque entièrement secrets, et la dépendance à l'égard du journalisme d'enquête persistera.* »

Pour la Commission, l'obligation de transparence du gouvernement canadien dépasse l'objectif noble du « bon gouvernement ». Il s'agit d'une considération pratique. La transparence évite le recours à des sources de moins bonne qualité « trompeuses ou mal comprises » et permet, en outre, à chacun de « contribuer à défendre la démocratie canadienne ». Ce constat porté dans le cadre de l'ingérence étrangère est tout aussi pertinent dans celui des cyberincidents à caractère géopolitique qui, comme la première, concernent la cybersécurité et la guerre informationnelle.

Notre équipe qui prépare le Rapport sélectionne méticuleusement ses sources. Toutefois, la compréhension des cyberincidents au Canada dépend moins d'une connaissance fine des opérations que de la capacité à les replacer dans leur contexte mondial. Les cas particuliers prennent leur sens à travers leur mise en relation avec les événements similaires vécus par d'autres États, dont les alliés du Canada. Que ceux-ci nous permettent-ils d'apprendre ?

Le Canada, au coeur de tendances mondiales

Trois tendances se dégagent. Premièrement, la plupart des cyberattaques prenaient encore récemment la forme de rançongiciels. En verrouillant l'accès à des données, ceux-ci rendaient les systèmes informatiques inopérables, déstabilisant les opérateurs et institutions ciblés. Ils étaient aussi instrumentalisés comme outils de financement par les régimes malicieux collectant des rançons importantes en échange du déchiffrement des systèmes. La Corée du Nord constitue un exemple typique de pays à l'origine récurrente de ce type d'attaques visant le Canada, comme l'illustre la **campagne d'espionnage et de vol de données personnelles** menée en 2025 par le groupe Famous Chollima contre des individus présents sur le territoire canadien. Or, de nouveaux cas de cyberespionage, comme celui de Salt Typhoon, démontrent que les cyberattaques visent de plus en plus le pré-positionnement au sein des systèmes, sans mener dans l'immédiat à un incident — déstabilisation, vol de données, etc. — concret. Ce prépositionnement témoigne par ailleurs d'une aggravation des tensions géopolitiques mondiales, alors que les principaux acteurs semblent se préparer à intervenir advenant l'émergence d'un nouveau conflit militaire direct. Traditionnellement perçus comme des instruments de guerre en zone grise, les rançongiciels représentent désormais de véritables armes de guerre en cas de future déflagration entre États.

Deuxièmement, en tant que joueur international important et membre de la communauté occidentale, proche allié des États-Unis, le Canada et sa population se retrouvent directement et indirectement au cœur des efforts d'influence menés par les belligérants des grands conflits internationaux actuels : de l'invasion russe en Ukraine à la guerre de Gaza et son prolongement au Liban, en passant par les guerres israélo-américaines contre l'Iran. Certains de ces efforts sont menés publiquement, comme l'**opération de diplomatie publique du gouvernement ukrainien** portée par l'**organisation United24** ou **la campagne iranienne** de dérision représentant le président Trump sous la forme d'un jouet Lego. D'autres sont menés en catimini, comme en témoignent les campagnes russes ciblant les **franges radicales de la population canadienne** et de l'**écosystème médiatique nord-américain**, celles du **gouvernement israélien**, ou encore les **images générées par intelligence artificielle produites par Téhéran** magnifiant la gravité des frappes iraniennes contre les pays du Golfe.

Ces conflits montrent que les campagnes de communication en ligne, attribuées par le passé à la créativité des acteurs privés, sont de plus en plus menées par des **États qui se réapproprient les codes de la culture numérique**. Pour les États ciblés, ces exemples soulèvent également l'enjeu de la réponse adéquate : comment les gouvernements doivent-ils réagir face à la guerre informationnelle ? Si le gouvernement

canadien, parmi d'autres, est souvent critiqué pour sa réticence à intervenir, à l'inverse, **la criminalisation du partage de contenu associé à la désinformation iranienne par les Émirats arabes unis** est inconcevable au Canada. La zone d'intervention est difficile à établir, et son opérationnalisation est parsemée d'embuches. Enfin, ces campagnes d'influence sonnent un signal d'alarme quant à la banalisation de la guerre et la normalisation de la violence portée par des discours humoristiques dépolitisés.

Troisièmement, la dernière tendance mondiale qui se dégage est, sans surprise, l'intégration croissante de l'intelligence artificielle générative à l'ensemble des pratiques de la cyberconflictualité. L'IA ne crée pas les cyberattaques ni la guerre informationnelle, mais elle en démultiplie la portée tout en en réduisant considérablement les coûts. L'IA générative permet, en effet, de produire la désinformation à grande échelle tout en diminuant les charges de la production, et d'inonder les systèmes informatiques et les plateformes de médias sociaux. **Pour plusieurs, elle représente dès lors une menace à venir considérable**. Les prochaines années permettront de départager les risques réels de l'angoisse momentanée..

Les spécificités canadiennes

Les cyberincidents canadiens s'inscrivent dans ces tendances mondiales. En même temps, la position canadienne s'est considérablement transformée au cours de l'année 2025, sans qu'Ottawa y soit pour grand-chose. La rhétorique belliqueuse et l'approche **ouvertement néo-impérialiste** adoptées par le gouvernement Trump à l'égard des États des Amériques placent le Canada dans une situation inconfortable. La fiabilité et l'honnêteté du gouvernement américain ne peuvent plus être tenues pour acquises, comme en témoignent, entre autres, les déclarations de la Maison-Blanche sur le projet d'annexion du Canada ou encore la publication, en novembre 2025, d'une **Stratégie de sécurité nationale américaine** (*National Security Strategy*) où l'administration Trump indique qu'elle voit les Amériques comme sa chasse-gardée, sa région prioritaire et un territoire où elle n'hésitera pas à utiliser tous les moyens pour favoriser l'alignement des gouvernements et des régimes voisins sur les intérêts nationaux américains. Avec la tenue probable ou projetée de référendums sur l'indépendance de l'Alberta et du Québec, le gouvernement américain respectera-t-il l'intégrité des processus électoraux canadiens ? Les conséquences envisageables de telles campagnes d'ingérence dépasseraient la composition d'un gouvernement et affecteraient la constitution même de la Confédération canadienne.

« Bref, face à l'ingérence américaine, le Canada pourrait bien y trouver sa plus grande menace, et la plus distinctive. »

Bien que cela puisse sembler invraisemblable, il est important de rappeler les précédents du trumpisme : son appui aux putschistes brésiliens qui contestèrent la défaite de Bolsonaro, son **soutien public au parti d'extrême droite allemand AfD** lors des dernières élections fédérales, ses **menaces de sanctions financières contre l'Argentine** en cas de défaite électorale de l'ami Milei, son implication dans l'**enlèvement manu militari du président vénézuélien**, ainsi que son **soutien au populiste Orbán** lors de la récente élection hongroise. En plus de Trump, d'autres acteurs politiques américains influents n'hésitent plus à s'immiscer dans les débats publics canadiens pour tenter d'influencer les processus politiques et les élections au Canada, comme en témoignent, par exemple, l'appui d'Elon Musk au candidat conservateur Pierre Poilièvre lors du dernier scrutin fédéral canadien ou encore les critiques virulentes de la vedette médiatique Tucker Carlson à l'égard des gouvernements de Justin Trudeau et de Mark Carney. Bref, face à l'ingérence américaine, le Canada pourrait bien y trouver sa plus grande menace, et la plus distinctive. Il est désormais attendu que des adversaires géopolitiques cherchent à fragiliser les assises démocratiques d'un pays. Il est plus difficile de se préparer à affronter l'ingérence d'un pays aussi étroitement lié au Canada que les États-Unis, surtout si elle continue de gagner en importance autant dans l'espace public que cyber.

Rubrique méthodologique

Comment ce rapport a-t-il été établi ?

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

www.dandurand.uqam.ca/cyberincidents

Le répertoire des cyberincidents canadiens a pour objectif de recenser et classer les cyberincidents à caractère géopolitique ayant touché le Canada, qu'il s'agisse de sa population, de ses pouvoirs publics, de ses entreprises, de sa société civile, de ses infrastructures ou des entités y étant basées. Le répertoire se veut une source de référence, régulièrement mise à jour, mais ne prétend pas à l'exhaustivité. Ses données remontent pour l'heure jusqu'à 2010. Un incident manquant ? Vous pouvez nous le signaler à l'adresse chaire.strat@uqam.ca.

Ce que ce rapport traite et ne traite pas

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

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

UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

Typologie des incidents et leurs définitions

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

CYBERESPIONNAGE : Fait d'obtenir par des moyens numériques de l'information sans l'accord préalable du détenteur 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 investigué un incident donné : rapports de firmes de cybersécurité, communiqués d'agences gouvernementales, etc. Nous invitons les lectrices et lecteurs à parcourir le répertoire en ligne pour plus de détails sur l'origine attribuée à chaque incident.

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

Les données du répertoire des cyberincidents canadiens, sur lequel ce rapport s'appuie, sont établies à partir des types de sources suivants : contenus produits par des médias professionnels respectant les principes énoncés par la Charte de Munich; études et rapports d'institutions gouvernementales, universitaires ou privées (entreprises de cybersécurité, think tanks, ONG, etc.) ; communiqués d'organes gouvernementaux canadiens et étrangers; publications scientifiques et autres bases de données, soumises à une évaluation par les pairs. Ces sources sont autant que possible soumises à recoupement entre elles. Nous invitons les lectrices et lecteurs à parcourir le répertoire en ligne afin de consulter les sources propres à chaque cas.

Chaire Raoul-Dandurand
en études stratégiques et diplomatiques

Université du Québec à Montréal

dandurand.uqam.ca

Révision
Daphné St-Louis Ventura

Graphisme
Françoise Conea et Daphné St-Louis Ventura

Montage couverture : Françoise Conea