

ÉVALUATION DES CYBERMENACES NATIONALES



2025
2026



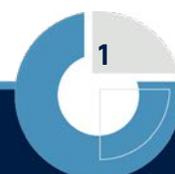
Centre de la sécurité des télécommunications Canada
1929, chemin Ogilvie
Ottawa (Ontario) K1J 8K6
cse-cst.gc.ca

ISSN 2816-9190
CAT D98-4F-PDF

© Sa Majesté le Roi du chef du Canada, représenté par le ministre
de la Défense nationale, 2024

Table des matières

À propos du Centre pour la cybersécurité	2
Avant-propos du ministre	3
Message du dirigeant principal du Centre pour la cybersécurité	4
Sommaire	5
Principaux avis	5
À propos de la présente évaluation des menaces	7
Sources	7
Processus d'évaluation	7
Restrictions	7
Lexique des estimations	7
Introduction	8
Cybermenace provenant d'États adversaires	9
Le Canada affronte un cyberécosystème étatique plus complexe et en pleine expansion	10
République populaire de Chine	11
Fédération de Russie	14
République islamique d'Iran	16
République populaire démocratique de Corée	18
République de l'Inde	18
Menaces émanant de la cybercriminalité	19
Un écosystème de cybercriminalité virtuel et interconnecté facilite la cybercriminalité comme service	20
La fraude et les escroqueries sont toujours une menace pour les Canadiennes et Canadiens	21
La menace de rançongiciel au Canada continue de croître et d'évoluer	22
Les rançongiciels affectent les infrastructures essentielles du Canada	25
Les opératrices et opérateurs de rançongiciel peaufinent leurs tactiques pour maximiser les profits et éviter la détection	28
Tendances qui influencent le contexte des cybermenaces du Canada	31
Contexte	32
Tendance no 1 : Les technologies d'intelligence artificielle amplifient les menaces dans le cyberspace	33
Tendance no 2 : Le savoir-faire des auteures et auteurs de cybermenace évolue pour échapper à la détection	35
Tendance no 3 : Les auteures et auteurs de cybermenace non étatiques inspirés par des intérêts géopolitiques sont source d'imprévisibilité	36
Tendance no 4 : La concentration des fournisseurs augmente la vulnérabilité en matière de cybersécurité	37
Tendance no 5 : Les services commerciaux à double usage se retrouvent sur le champ de bataille numérique	38
Conclusion	39
Notes de fin de texte	40



À propos du Centre pour la cybersécurité

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) est l'autorité technique canadienne en matière de cybersécurité. Relevant du Centre de la sécurité des télécommunications Canada (CST), le Centre pour la cybersécurité est la seule source unifiée d'avis, de conseils, de services et de soutien spécialisés en matière de cybersécurité pour les Canadiennes et Canadiens et pour les organisations canadiennes.

Le Centre pour la cybersécurité travaille étroitement avec les ministères du gouvernement du Canada, les secteurs des infrastructures essentielles, les entreprises canadiennes et les partenaires internationaux pour se préparer et réagir aux cyberévénements, pour en atténuer les conséquences et pour s'en remettre. Il est à l'écoute des entités externes et favorise les partenariats visant un cyberspace canadien fort et résilient. Conformément à la Stratégie nationale de cybersécurité, le Centre pour la cybersécurité représente une approche plus collaborative à la cybersécurité dans notre pays.

À titre de spécialistes en cybersécurité dignes de confiance, nous aidons à assurer la sécurité du Canada et des Canadiennes et Canadiens comme suit :

- en étant une source claire et fiable de renseignements pertinents sur la cybersécurité pour les Canadiennes et Canadiens, les entreprises canadiennes ainsi que les propriétaires et les exploitants d'infrastructures essentielles;
- en fournissant des avis et des conseils adaptés sur la cybersécurité afin de protéger les plus importants cybersystèmes canadiens;
- en travaillant en collaboration avec les gouvernements provinciaux, territoriaux et autochtones, les administrations municipales et les partenaires du secteur privé pour résoudre les défis les plus complexes du Canada en matière de cybersécurité;
- en développant et en diffusant nos technologies et connaissances spécialisées de cyberdéfense;
- en défendant les cybersystèmes, notamment les réseaux du gouvernement du Canada, grâce au développement et au déploiement d'outils et de technologies de cyberdéfense sophistiqués;
- en agissant à titre de chef de file opérationnel du gouvernement du Canada lors de cyberévénements et en tirant parti de notre expertise et de nos accès de manière à fournir de l'information opportune et utile à la gestion des incidents.

Grâce à son travail et à ses partenariats, le Centre pour la cybersécurité relève le niveau de la cybersécurité au Canada afin que les Canadiennes et Canadiens puissent vivre et travailler en ligne en toute confiance et sécurité.

Avant-propos du ministre

Les cybermenaces visant le Canada sont de plus en plus complexes et sophistiquées, compromettant notre sécurité nationale et notre prospérité économique. À titre de pays ayant une présence importante dans le monde, le Canada est une cible intéressante pour les cybercriminelles et cybercriminels qui cherchent à réaliser des gains et pour les États adversaires qui cherchent à perturber les systèmes sur lesquels nous comptons.

Au cours des deux dernières années, nous avons observé une forte augmentation du nombre et de la gravité de cyberincidents, dont plusieurs ciblent nos services essentiels. Des auteures et auteurs qui mènent leurs activités à l'extérieur du pays ont également tenté d'influencer l'opinion publique et d'intimider la population, notamment la diaspora canadienne, au moyen de cybercampagnes coordonnées.

L'Évaluation des cybermenaces nationales 2025-2026 du Centre canadien pour la cybersécurité est un outil essentiel à notre compréhension des cybermenaces qui guettent le Canada. L'évaluation des menaces fait fond sur les rapports publics et le renseignement classifié pour brosser un tableau global du contexte actuel des menaces, tout en prévoyant les futures tendances. En offrant des renseignements fiables et opportuns, le rapport permet à la population et aux organisations canadiennes de se préparer aux menaces actuelles et émergentes et de les contrer.

En approfondissant notre compréhension des cybermenaces, nous renforçons également notre préparation et, à mesure que les menaces évoluent, le Centre pour la cybersécurité continuera de chercher de nouvelles façons de les combattre. Son équipe est à la pointe des efforts déployés pour accroître la cybersécurité et ainsi mieux protéger les Canadiennes et Canadiens. Notre gouvernement appuie son travail inestimable, et le Budget 2024 prévoit 917,4 millions de dollars à l'enrichissement des programmes de renseignement et de cyberopérations dans le but de contrer les menaces pour la sécurité nationale qui ne cessent d'évoluer.

Les renseignements fournis dans cette évaluation des menaces s'avèrent essentiels alors que nous travaillons à renforcer la sécurité du Canada dans un monde de plus en plus numérique.

L'honorable Bill Blair
Ministre de la Défense nationale

Message du dirigeant principal du Centre pour la cybersécurité

Il est difficile de croire que deux ans se sont déjà écoulés depuis notre dernier rapport. Au premier abord, on dirait que le contexte des cybermenaces n'a pas beaucoup changé. La cybercriminalité constitue toujours une menace, les attaques par rançongiciel continuent de cibler nos infrastructures essentielles et les activités de cybermenace parrainées par des États continuent de toucher la population canadienne.

Ce qui a changé, par contre, c'est que les États adversaires deviennent plus audacieux et plus agressifs. Les cybercriminelles et cybercriminels motivés par le profit tirent parti de nouveaux modèles opérationnels illicites pour accéder à des outils malveillants et utilisent l'intelligence artificielle pour accroître leurs capacités. Les auteures et auteurs non étatiques exploitent les grands conflits mondiaux et les controverses politiques pour mener des activités perturbatrices.

Ces nouvelles réalités et autres tendances sont présentées en détail dans la présente édition de l'Évaluation des cybermenaces nationales. Le rapport de cette année va plus loin que les éditions précédentes : il offre des exemples plus concrets d'activités de cybermenace au Canada et dans le monde, de même que nos propres statistiques sur les cyberincidents.

Bien que nos évaluations dépeignent des tendances qui devraient préoccuper quiconque lit à leur sujet, vous pouvez tenir pour certain que le Centre pour la cybersécurité continue de lutter contre ces menaces. En travaillant étroitement avec le secteur privé, l'industrie, le gouvernement et les infrastructures essentielles, nous aidons à protéger les systèmes nécessaires à notre vie quotidienne.

Que vous soyez une nouvelle lectrice ou un nouveau lecteur, une consommatrice ou un consommateur passionné, une Canadienne ou un Canadien, ou encore membre d'une petite, moyenne ou grande organisation, je suis convaincu que vous trouverez l'information contenue dans le présent rapport pertinente. J'espère qu'il vous encouragera également à réfléchir à ce que vous pouvez faire pour contribuer à notre résilience collective. Après tout, nous avons toutes et tous un rôle à jouer pour faire du Canada un pays plus sûr et plus sécuritaire.

Bien cordialement,

Rajiv Gupta
Dirigeant principal, Centre canadien pour la cybersécurité

Sommaire

Le Canada affronte un environnement de cybermenaces complexe et en pleine expansion comptant un éventail croissant d'auteurs et auteurs de cybermenace étatiques et non étatiques malveillants et imprévisibles, comme les cybercriminelles et cybercriminels et les hacktivistes, qui ciblent ses infrastructures essentielles et compromettent sa sécurité nationale. Ces auteurs et auteurs de cybermenace développent leur métier, adoptent de nouvelles technologies et collaborent dans le but d'améliorer et d'intensifier leurs activités malveillantes.

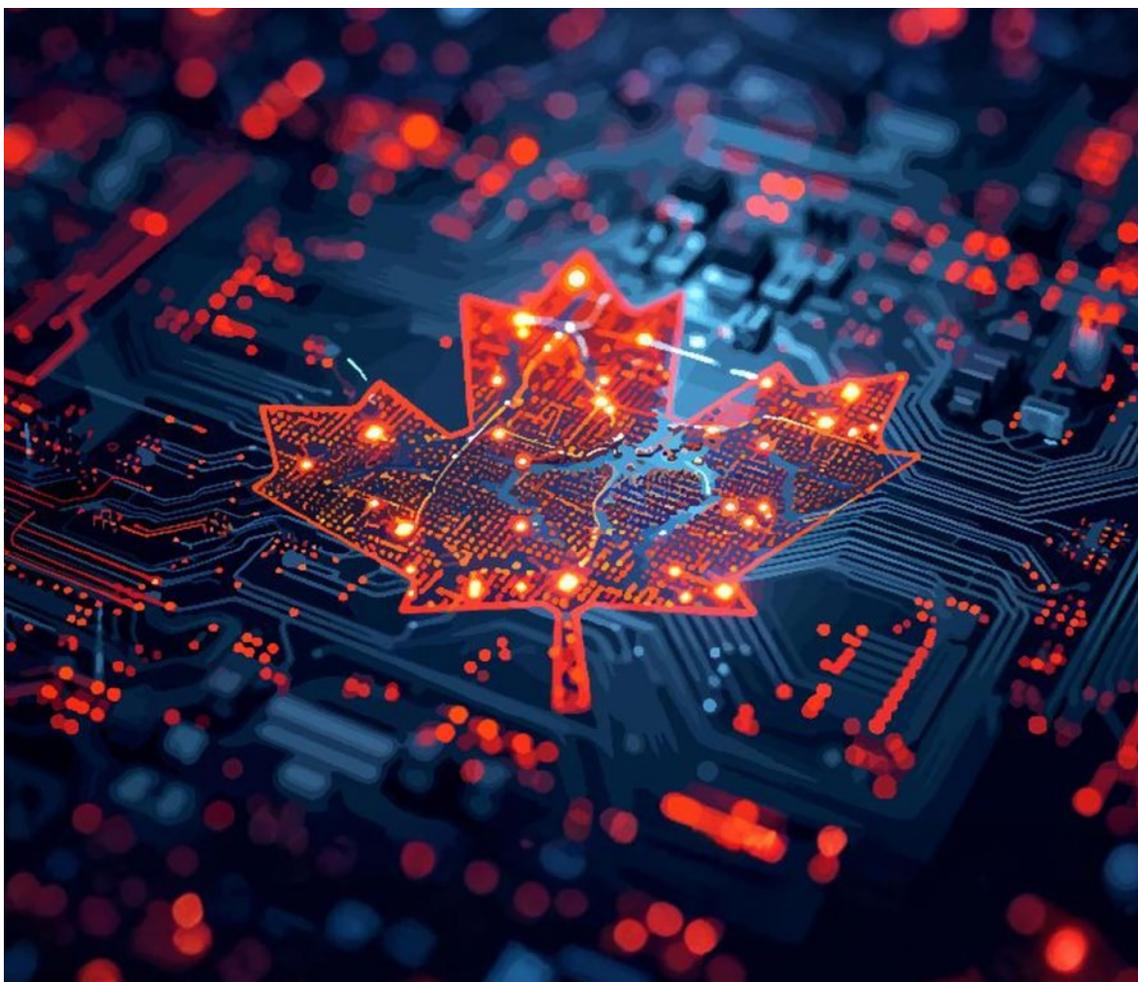
Les États adversaires du Canada sont plus agressifs dans le cyberspace. Les cyberopérations parrainées par des États visant le Canada et ses alliés ne se limitent certainement pas à l'espionnage. Les auteurs et auteurs de cybermenace parrainés par des États tentent sans doute d'être perturbateurs, par exemple, en rendant un service inaccessible, en supprimant ou en divulguant des données et en manipulant des systèmes de contrôle industriels, afin de favoriser la réalisation d'objectifs militaires ou de campagnes d'information. Nous estimons que nos adversaires considèrent très probablement les infrastructures civiles essentielles comme une cible légitime de cybersabotage advenant un conflit militaire.

Parallèlement, la cybercriminalité constitue toujours pour les particuliers, les organisations et tous les ordres de gouvernement au Canada une menace généralisée et perturbatrice appuyée par un écosystème de cybercriminalité mondial prospère et résilient. Selon nous, les motivations financières qui sous-tendent la cybercriminalité inciteront sans doute l'écosystème de cybercriminalité à évoluer et à se diversifier continuellement alors que les cybercriminelles et cybercriminels tentent d'échapper aux autorités.

Principaux avis

- **Les États adversaires du Canada recourent à des cyberopérations pour causer des perturbations et créer des divisions.** Les auteurs et auteurs de cybermenace parrainés par des États conjuguent presque certainement des attaques de réseau informatique perturbatrices et des campagnes d'information en ligne pour intimider la population et influencer l'opinion publique. Ils ciblent fort probablement les réseaux d'infrastructures essentielles au Canada et dans les pays alliés afin de se préparer à d'éventuelles cyberopérations perturbatrices ou destructrices.
- **Le vaste et vigoureux programme de cyberactivité de la République populaire de Chine (RPC) représente pour le Canada à l'heure actuelle la cybermenace la plus active et la plus sophistiquée.** La RPC mène des cyberopérations contre les intérêts canadiens pour servir de grands objectifs politiques et industriels, dont l'espionnage, le vol de propriété intellectuelle (PI), l'influence malveillante et la répression transnationale. Parmi nos adversaires, la portée, la capacité et la visée du programme de cyberactivité de la RPC dans le cyberspace sont inégales.
- **Le programme de cyberactivité de la Russie renforce l'ambition de Moscou de vouloir confronter et déstabiliser le Canada et ses alliés.** Le Canada est fort probablement une cible intéressante pour l'espionnage pour les auteurs et auteurs de cybermenace parrainés par la Russie, notamment par la compromission de la chaîne d'approvisionnement, compte tenu de son statut de pays membre de l'Organisation du Traité de l'Atlantique Nord, de son soutien de l'Ukraine contre l'agression russe et de sa présence dans l'Arctique. Des auteurs et auteurs non étatiques pro-Russie, dont certains, selon nous, ont probablement des liens avec le gouvernement russe, ciblent le Canada dans le but d'influencer sa politique étrangère.

- **L'Iran se sert de son programme de cyberactivité pour contraindre, harceler et réprimer ses adversaires et gérer les risques d'escalade.** La volonté grandissante de l'Iran à lancer des cyberattaques destructrices au-delà du Moyen-Orient et ses efforts soutenus en vue de suivre et de surveiller les adversaires du régime dans le cyberspace donnent de plus en plus de fil à retordre au Canada et à ses alliés pour assurer leur cybersécurité.
- **Le modèle opérationnel de cybercriminalité comme service (CaaS) contribue sans doute au fait que la cybercriminalité se poursuit au Canada et dans le monde.** L'écosystème CaaS est soutenu par des marchés en ligne florissants où des auteurs et auteurs de cybermenace spécialisés vendent des données volées et divulguées de même que des outils malveillants prêts à l'emploi à d'autres cybercriminels et cybercriminels. Cela a presque certainement permis à un nombre croissant d'auteurs et auteurs possédant diverses capacités et connaissances techniques de lancer des attaques de cybercriminalité et d'échapper aux organismes d'application de la loi.
- **Les rançongiciels constituent la principale menace émanant de la cybercriminalité à laquelle font face les infrastructures essentielles du Canada.** Les rançongiciels perturbent directement la capacité des entités des infrastructures essentielles à offrir des services critiques, ce qui peut nuire au bien-être physique et émotionnel des victimes. Au cours des deux prochaines années, les auteurs et auteurs de rançongiciels intensifieront presque certainement leurs tactiques d'extorsion et perfectionneront leur capacité d'accroître la pression exercée sur les victimes pour qu'elles paient des rançons et d'échapper aux organismes d'application de la loi.



À propos de la présente évaluation des menaces

L'Évaluation des cybermenaces nationales 2025-2026 (ECMN 2025-2026) fait état des cybermenaces auxquelles font face les personnes et les organisations au Canada. Elle constitue une mise à jour de l'[Évaluation des cybermenaces nationales 2018](#)¹ (ECMN 2018), de l'[Évaluation des cybermenaces nationales 2020](#)² (ECMN 2020) et de l'[Évaluation des cybermenaces nationales 2023-2024](#)³ (ECMN 2023-2024), et fournit une analyse des années intermédiaires et des prévisions d'ici 2026. Nous recommandons de lire l'ECMN 2025-2026, l'[Introduction à l'environnement de cybermenaces](#)⁴ et les avis et conseils que nous avons publiés comme compléments d'information à la présente évaluation.

Nous avons préparé la présente évaluation pour aider les Canadiennes et Canadiens à façonner et à maintenir la cyberrésilience de notre pays. Ce n'est que lorsque le gouvernement, le secteur privé et la population travaillent ensemble que nous pouvons instaurer une résilience face aux cybermenaces au Canada.

Sources

Les avis formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise du CST en matière de cybersécurité. Le rôle que joue le CST dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans l'environnement de cybermenaces, ce qui lui a permis par la même occasion d'éclairer son évaluation. Le volet du mandat du CST touchant le renseignement étranger lui procure de précieuses informations sur le comportement des adversaires dans le cyberspace. Bien que le CST soit toujours tenu de protéger les sources et méthodes classifiées, il fournira aux lectrices et lecteurs, dans la mesure du possible, les justifications qui ont motivé ses avis.

Processus d'évaluation

Les évaluations des cybermenaces sont effectuées selon une méthode d'évaluation qui comprend l'évaluation de la qualité des renseignements disponibles, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. On emploiera des termes comme « on considère que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « possiblement », « probablement » et « très probablement » pour exprimer les probabilités.

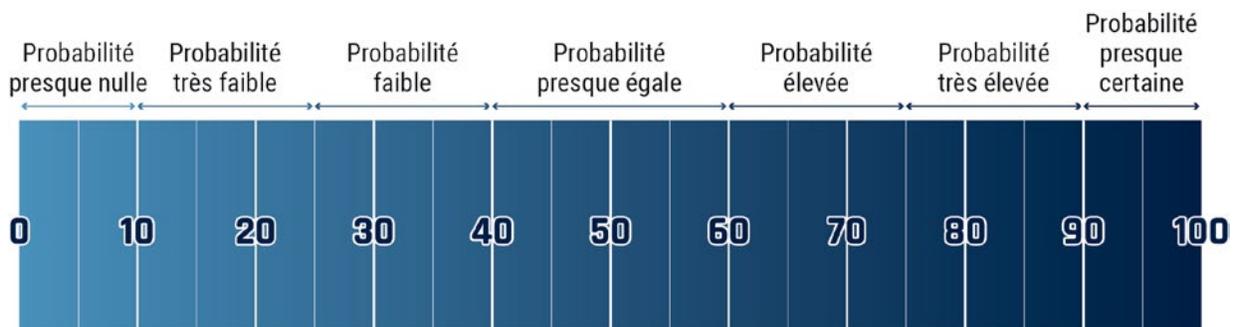
La présente évaluation des menaces se fonde sur des renseignements disponibles en date du **20 septembre 2024**.

Restrictions

La présente évaluation n'a pas pour objet de fournir une liste exhaustive des activités de cybermenace ciblant le Canada ou des conseils en matière d'atténuation. Son objectif est plutôt de décrire et d'évaluer les menaces visant le Canada. Elle cherche à comprendre la nature de l'environnement de cybermenace actuel et la façon dont les activités de cybermenace peuvent toucher la population et les organisations canadiennes. Pour obtenir des conseils sur la cybersécurité, prière de consulter le site Web du Centre pour la cybersécurité et le [site Web de Pensez cybersécurité](#)⁵.

Lexique des estimations

Le tableau ci-dessous fait coïncider le lexique des estimations à une échelle de pourcentage approximative. Ces nombres ne proviennent pas d'analyses statistiques, mais sont plutôt basés sur la logique, les renseignements disponibles, des jugements antérieurs et des méthodes qui accroissent la précision des estimations.



Introduction

Le Canada se retrouve dans une nouvelle ère de cybervulnérabilité, où les cybermenaces sont omniprésentes et où les Canadiennes et Canadiens ressentiront de plus en plus les répercussions des cyberincidents qui s'enchaînent et perturbent leur vie quotidienne.

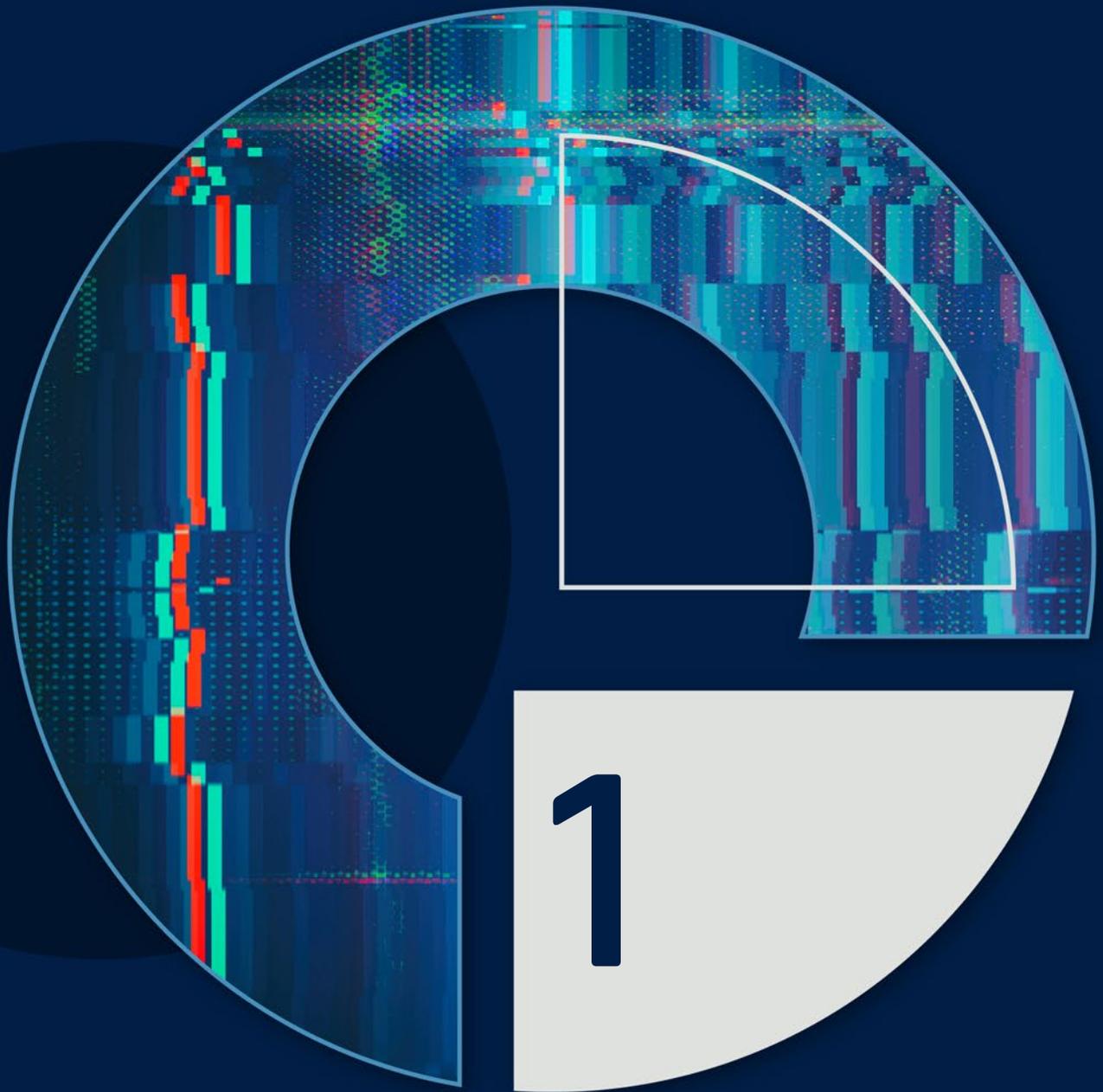
Les progrès réalisés au chapitre des technologies informatiques et des communications ont ouvert la voie à un monde de connectivité omniprésente pour la population canadienne. Dans cet environnement, les plateformes en ligne et les technologies numériques continuent de façonner et d'influencer les interactions des Canadiennes et Canadiens avec le monde physique – leur façon de travailler, de faire des courses, de voyager, de se rencontrer, de s'informer et d'accéder à des services critiques⁶. Ces systèmes enregistrent et traitent de grandes quantités de données à leur sujet, souvent sur des réseaux numériques mal sécurisés ou non fiables⁷. Ces systèmes sont également interconnectés et fragiles : les cyberincidents, qu'il s'agisse de cyberattaques ou de mises à jour logicielles déficientes, peuvent faire en sorte que les compagnies aériennes, les hôpitaux, les banques et les détaillants partout dans le monde se retrouvent hors ligne⁸.

Le CST et ses partenaires au Canada et au sein de la collectivité des cinq sont à l'affût des cybermenaces qui pèsent sur le Canada de la part d'auteurs et auteurs de cybermenace étatiques et non étatiques et les surveillent au fur et à mesure qu'elles évoluent. L'ECMN 2025-2026 fournit au public canadien des données actuelles du CST sur les auteurs et auteurs de cybermenace étatiques et non étatiques qui mènent des activités de cybermenaces malveillantes contre le Canada, et la façon d'évaluer le contexte des cybermenaces évoluera au cours des deux prochaines années. La présente évaluation est divisée en trois sections qui sont conçues pour être prises en compte indépendamment et collectivement.

- **Section 1 – Cybermenace provenant d'États adversaires** : Cette section présente l'écosystème des cybermenaces parrainé par des États et porte sur les cybermenaces visant le Canada qui proviennent des pays suivants :
 - la République populaire de Chine (RPC);
 - la Fédération de Russie (Russie);
 - la République islamique d'Iran (Iran);
 - la République populaire démocratique de Corée (RPDC);
 - la République de l'Inde (Inde).
- **Section 2 – Menaces émanant de la cybercriminalité** : Cette section porte sur l'interconnectivité de l'écosystème de la cybercriminalité comme service (CaaS) et des menaces émanant de la cybercriminalité auxquelles fait face le Canada, en particulier la fraude, les escroqueries et les rançongiciels. Elle porte également sur la menace de rançongiciel visant les infrastructures essentielles du Canada.
- **Section 3 – Tendances qui influencent le contexte des cybermenaces du Canada** : Cette section présente cinq tendances qui influenceront le contexte des cybermenaces du Canada et qui guideront les activités de cybermenace touchant la population canadienne jusqu'en 2026.

Nous invitons les lectrices et lecteurs qui souhaitent en savoir davantage sur le contexte des cybermenaces en évolution et obtenir la définition de termes et de concepts importants mentionnés dans la présente ECMN à consulter les ressources suivantes :

- [Introduction à l'environnement de cybermenaces](#)⁹
- [Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023](#)¹⁰
- [La menace posée par les générateurs de texte basés sur des modèles de langage de grande taille](#)¹¹



CYBERMENACE PROVENANT D'ÉTATS ADVERSAIRES

Le Canada affronte un cyberécosystème étatique plus complexe et en pleine expansion

Adversaires stratégiques

Les programmes de cyberactivité de la RPC, de la Russie et de l'Iran demeurent les plus grandes cybermenaces stratégiques visant le Canada. Tous ces pays souhaitent contester la domination des États-Unis dans de multiples domaines, dont le cyberspace, et promouvoir une vision autoritaire de la gouvernance d'Internet et de la surveillance nationale¹². Le programme de cyberactivité de la RPC surpasse les autres États hostiles au chapitre de la portée et des ressources consacrées aux activités de cybermenace contre le Canada.

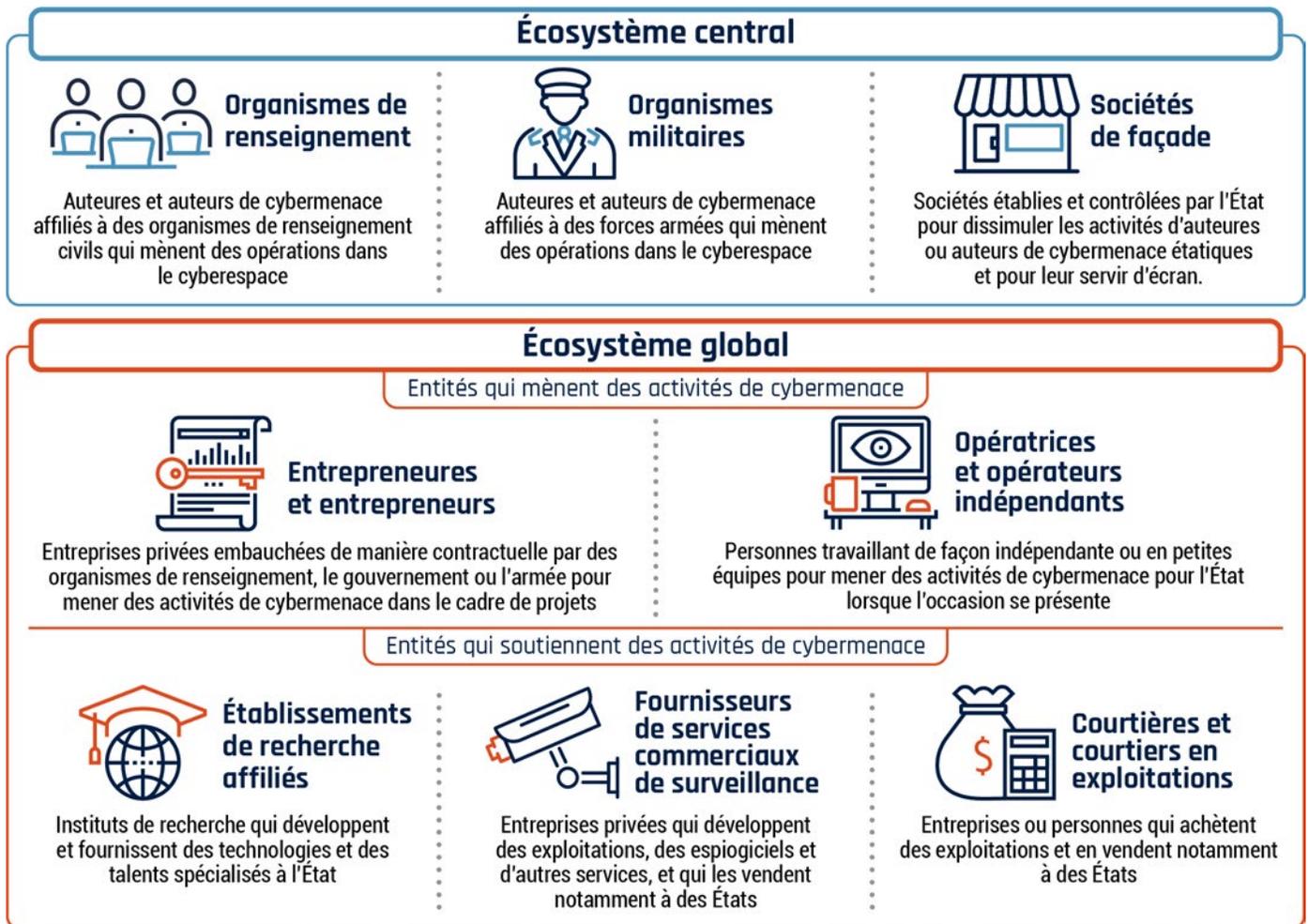
Nouveaux programmes de cyberactivité

Parallèlement, des pays qui aspirent à devenir de nouveaux centres de pouvoir au sein du système mondial, comme l'Inde, élaborent des programmes de cyberactivité qui présentent divers niveaux de menace pour le Canada¹³. Les nouveaux États concentrent leurs activités dans le cyberspace sur les menaces nationales et les rivaux régionaux, tout en se servant de leurs cybercapacités pour suivre et surveiller les activistes et les dissidentes et dissidents vivant à l'étranger.

Cyberécosystème global

Les États avancés et émergents tirent parti d'un écosystème complexe de fournisseurs de services commerciaux de surveillance, d'entrepreneurs et entrepreneurs et d'établissements de recherche affiliés pour soutenir ou exécuter des activités de cybermenace (voir la figure 1)¹⁴. Les États font appel à ces entités pour dissimuler leurs cyberopérations ou pour acquérir des exploitations, une infrastructure numérique et des données. Les États émergents utilisent très probablement l'écosystème global pour tenter de gravir les échelons de la sophistication et d'acquérir des capacités qui pourraient dépasser leur capacité de développement interne.

Figure 1 : Écosystème des programmes de cyberactivité étatiques¹⁵



République populaire de Chine

La RPC représente pour le Canada la cybermenace la plus active et la plus sophistiquée

Le vaste et vigoureux programme de cyberactivité de la RPC comporte des capacités mondiales de cybersurveillance, d'espionnage et d'attaque, et constitue la menace de cybersécurité la plus complète à laquelle fait face le Canada à l'heure actuelle. Le Canada, tout comme ses partenaires de la collectivité des cinq, est une cible permanente du programme de cyberactivité de la RPC. La RPC mène des cyberopérations contre les intérêts canadiens pour servir de grands objectifs politiques et industriels, dont l'espionnage, le vol de propriété intellectuelle (PI), l'influence malveillante et la répression transnationale. Parmi nos adversaires, la portée, la capacité et la visée du programme de cyberactivité de la RPC dans le cyberspace sont inégalées.

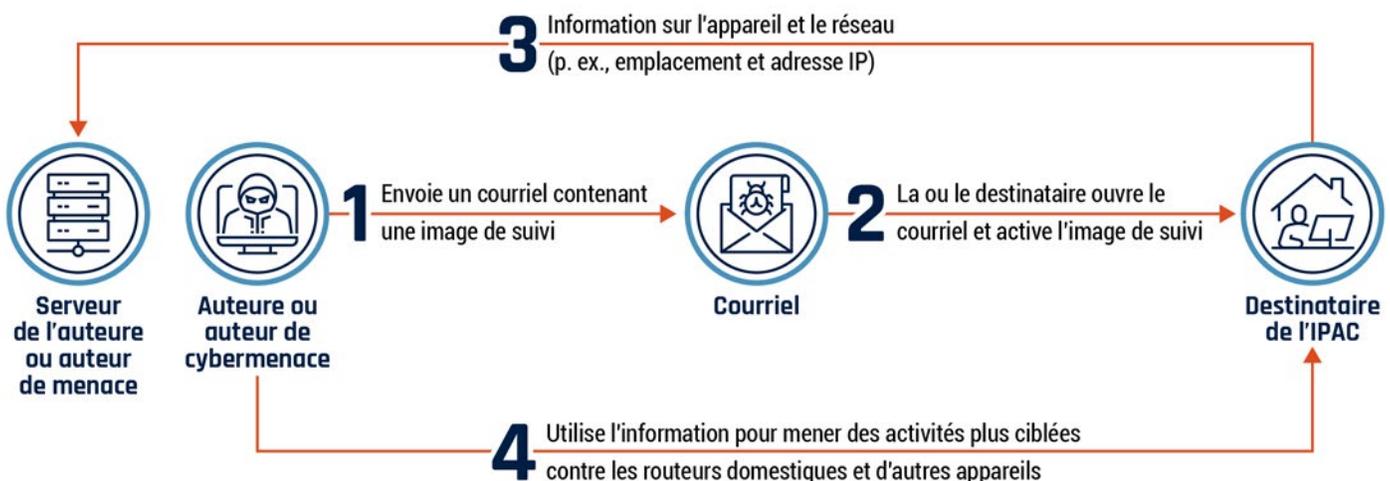
Tous les ordres de gouvernement et les fonctionnaires ciblés par la RPC pour obtenir du renseignement utile

Les auteurs et auteurs de cybermenace parrainés par la RPC exécutent des opérations de cyberspionnage contre les réseaux des gouvernements fédéral, provinciaux, territoriaux et autochtones, et ceux des administrations municipales au Canada. Les auteurs et auteurs de cybermenace de la RPC ont compromis et maintenu l'accès à de multiples réseaux gouvernementaux au cours des cinq dernières années, recueillant des communications et d'autres renseignements utiles¹⁶. Bien que toutes les compromissions connues du gouvernement fédéral aient été réglées, il est fort probable que les auteurs et auteurs responsables de ces intrusions aient consacré beaucoup de temps et de ressources à se renseigner sur les réseaux cibles.

Les auteurs et auteurs de cybermenace parrainés par la RPC ciblent également les représentantes et représentants du gouvernement canadien, en particulier les personnes que la RPC considère comme critiques envers le Parti communiste chinois. Selon une mise en accusation du United States Department of Justice, en 2021, des auteurs et auteurs de cybermenace parrainés par la RPC ont ciblé des membres de l'Alliance interparlementaire sur la Chine (IPAC), un groupe de législatrices et législateurs de partout au monde dont la fin convenue est de contrer les menaces que représente le Parti communiste chinois pour l'ordre international et les principes démocratiques. Les auteurs et auteurs de menace ont envoyé des courriels contenant des images de suivi à des destinataires afin de mener des activités de reconnaissance réseau (voir la figure 2)¹⁷. Un certain nombre de politiciennes et politiciens canadiens membres de l'IPAC ont confirmé avoir été ciblés dans cette opération¹⁸.

Au cours des quatre dernières années, au moins 20 réseaux associés à des ministères et organismes du gouvernement du Canada ont été compromis par des auteurs et auteurs de cybermenace de la RPC.

Figure 2 : Opération de la Chine menée par courriel contre des membres de l'Alliance interparlementaire sur la Chine





La RPC cible les fonctionnaires et les réseaux du gouvernement canadien pour obtenir de l'information qui servira ses intérêts stratégiques, économiques et diplomatiques et qui donnera au gouvernement de la RPC l'avantage quant aux questions opérationnelles et dans les relations bilatérales entre la Chine et le Canada. Par exemple, les gouvernements provinciaux et territoriaux sont susceptibles d'être une cible intéressante étant donné qu'ils ont un pouvoir décisionnel sur le commerce régional, notamment l'extraction de ressources (par exemple, l'énergie et les minéraux critiques)¹⁹. En plus de réaliser les priorités de la RPC en matière de collecte de renseignement, les informations recueillies servent sans doute à appuyer l'influence malveillante et les activités d'ingérence de la RPC contre les processus et les institutions démocratiques du Canada.

Les activités de cybermenace de la RPC contre le Canada semblent s'intensifier à la suite d'événements qui accroissent les tensions bilatérales entre le Canada et la RPC. Dans ce contexte, les activités de cybermenace de la RPC sont probablement conçues pour la recherche opportune de renseignement sur les réactions des fonctionnaires et pour suivre l'évolution de la situation.

Des personnes au Canada ciblées par des activités de cyberrépression transnationale de la RPC

Les auteures et auteurs de cybermenace de la RPC appuient fort probablement les mesures prises par la Chine à l'étranger pour réduire au silence les activistes, les journalistes, les collectivités de la diaspora et d'autres groupes que la RPC considère comme des menaces à la sécurité. Ces groupes, appelés collectivement « les cinq poisons » par les représentantes et représentants de la RPC, comprennent les suivants :

- les pratiquantes et praticiens du Falun Gong;
- les Ouïghoures et Ouïghours;
- les Tibétaines et Tibétains;
- les partisans et partisans de l'indépendance taïwanaise;
- les militantes et militants prodémocratie.

Les auteures et auteurs de la RPC facilitent très probablement la répression transnationale en surveillant et en harcelant ces groupes en ligne et en les suivant au moyen de la cybersurveillance²⁰. Par exemple, la RPC a été liée publiquement à des opérations de cyberespionnage contre le groupe minoritaire ouïghour, y compris des membres vivant au Canada, au moyen de courriels de harponnage et de logiciels espions²¹.

Le gouvernement de la RPC tire fort probablement parti des plateformes technologiques chinoises, dont certaines collaborent sûrement avec les services de renseignement et de sécurité de la RPC, pour faciliter la répression transnationale²².

La RPC cible le secteur privé et l'écosystème de l'innovation du Canada pour obtenir un avantage concurrentiel

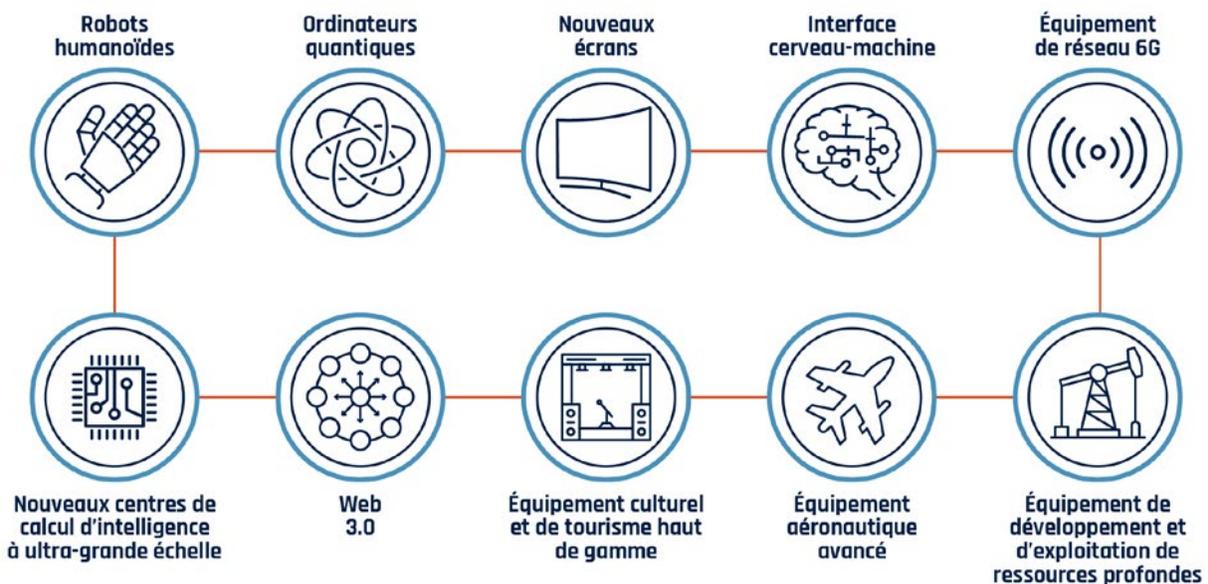
L'écosystème de l'innovation du Canada est une priorité de longue date de la collecte de renseignement de la RPC. Le programme de cyberactivité de la RPC continue presque certainement d'appuyer les activités d'espionnage de la RPC contre le secteur privé, le milieu universitaire, les chaînes d'approvisionnement et les établissements de recherche et développement (R et D) gouvernementaux du Canada. Les auteures et auteurs de cybermenace de la RPC ont fort probablement volé des données commercialement sensibles à des entreprises et institutions canadiennes.

La RPC fait appel à des cyberentrepreneurs et cyberentrepreneurs et à des opératrices et opérateurs indépendants pour appuyer l'espionnage

La RPC a recours à un marché concurrentiel d'auteurs et auteurs de cybermenace contractuels et indépendants pour répondre aux besoins de la RPC en matière de collecte de renseignement. Par exemple, I-Soon est un entrepreneur privé de la RPC qui fournit des services de « pirates professionnels ». Selon des documents ayant fait l'objet d'une fuite, l'entreprise a travaillé sur des projets sur une base contractuelle pour diverses entités gouvernementales et militaires de la RPC et des sociétés d'État. I-Soon aurait vendu à sa clientèle des données exfiltrées provenant de cibles²³.

Les auteurs et auteurs de cybermenace de la RPC ciblant le Canada accordent probablement la priorité à la collecte de renseignements confidentiels et exclusifs qui servent les intérêts économiques et militaires de la RPC et qui peuvent aider à accélérer le développement de technologies avancées et stratégiques par la RPC (voir la figure 3). La RPC intensifiera probablement ses activités d'espionnage contre le secteur canadien de l'innovation à mesure que les tensions économiques entre la RPC et le Canada (et ses alliés) s'accroissent²⁴.

Figure 3 : « Produits iconiques » d'industries de l'avenir estimés comme prioritaires pour la stratégie industrielle de la Chine (2024)²⁵



Le prépositionnement de la RPC dans les infrastructures essentielles des États-Unis augmente le risque pour le Canada

Dans le cadre d'un changement stratégique, la RPC intègre très probablement les cyberopérations offensives à sa planification militaire afin de tirer un avantage lors d'un conflit potentiel avec les États-Unis. Les auteurs et auteurs de cybermenace parrainés par la RPC, connus sous le nom de Volt Typhoon, cherchent presque certainement à se prépositionner au sein des réseaux d'infrastructures essentielles des États-Unis en vue de lancer des cyberattaques perturbatrices ou destructrices advenant une crise ou un conflit majeur avec les États-Unis. Selon les représentantes et représentants américains, l'opération de la RPC vise à ralentir l'intervention des forces armées américaines et à semer la panique dans la société²⁶. Le groupe Volt Typhoon est particulièrement digne de mention, car la RPC n'a jamais mené de cyberopérations perturbatrices ou destructrices contre des infrastructures essentielles²⁷.

Nous estimons que la menace directe que les auteurs et auteurs de cybermenace parrainés par la RPC représentent pour les infrastructures essentielles canadiennes est probablement inférieure à celle qui pèse sur les infrastructures américaines. Bien que les futures opérations de cyberguerre de la RPC visent probablement les États-Unis, les activités de cybermenace perturbatrices ou destructrices contre les infrastructures essentielles intégrées de l'Amérique du Nord, comme les pipelines, les réseaux électriques et les voies ferrées, auraient probablement une incidence sur le Canada en raison de l'interopérabilité et l'interdépendance frontalières²⁸.

Fédération de Russie

La Russie tire parti de son programme de cyberactivité pour affronter l'Occident

Le programme de cyberactivité imprévisible de la Russie remet régulièrement en question les normes en vigueur dans le cyberspace et renforce l'ambition de Moscou de vouloir confronter et déstabiliser le Canada et ses alliés.

La Russie considère presque certainement son programme de cyberactivité comme faisant partie intégrante d'une stratégie à plusieurs niveaux visant à influencer et à façonner l'environnement de l'information. La Russie conjugue les activités de cyberespionnage conventionnelles et les attaques de réseaux informatiques aux activités de désinformation et d'influence pour²⁹ :

- promouvoir le statut mondial de la Russie et renforcer les discours pro-Russie;
- miner la confiance dans les institutions démocratiques;
- inciter la population à appuyer les efforts de guerre de la Russie, tant au pays qu'à l'étranger;
- affaiblir ou gêner psychologiquement ses adversaires.

Les activités de cybermenace de la Russie sont soutenues par un réseau d'auteurs et auteurs étatiques et non étatiques, notamment un groupe en constante évolution de cybercriminelles et cybercriminels, de hacktivistes et de « pirates professionnels » associés à la Russie, lesquels sont probablement motivés par un mélange de patriotisme, de profit ou d'opportunisme. Cette stratégie hybride, qui procure à la Russie la possibilité de nier, semble avoir inspiré d'autres États, créant ainsi un environnement de cybermenaces plus complexe pour le Canada et ses alliés³⁰.

Une auteure ou un auteur de cybermenace russe lance une cyberattaque destructive contre l'Ukraine pour causer des effets psychologiques

En décembre 2023, une auteure ou un auteur de cybermenace russe a lancé une cyberattaque par virus effaceur destructive contre la société de télécommunications ukrainienne Kyivstar, privant des millions d'Ukrainiennes et Ukrainiens d'Internet et de services mobiles pendant plusieurs jours. La personne en cause se serait introduite dans les systèmes de Kyivstar au plus tôt en mai 2023 et aurait été en mesure de voler des renseignements sur les abonnées et abonnés et d'intercepter des messages texte. Cette personne a revendiqué l'attaque dans un message sur la plateforme Telegram adressé au président ukrainien Volodymyr Zelenskyy. Selon les responsables ukrainiens, l'objectif de l'attaque destructrice était de porter un coup psychologique à l'Ukraine³¹.

Le Canada ciblé par la Russie à des fins d'espionnage

Le Canada est fort probablement une cible intéressante pour l'espionnage pour les auteures et auteurs de cybermenace parrainés par la Russie, compte tenu de son statut de pays membre de l'Organisation du Traité de l'Atlantique Nord, de son soutien de l'Ukraine et de sa présence dans l'Arctique. Des auteures et auteurs de cybermenace russes ciblent fort probablement les réseaux du gouvernement, des forces armées, du secteur privé et des infrastructures essentielles du pays dans le cadre d'activités de collecte de renseignement militaire et étranger³².

Les organisations des secteurs public et privé au Canada sont également vulnérables aux compromissions de la chaîne d'approvisionnement mondiale par les auteures et auteurs de cybermenace russes. Par exemple, en 2020, des auteures et auteurs de cybermenace parrainés par la Russie ont compromis la chaîne d'approvisionnement en implantant des maliciels dans une mise à jour du logiciel SolarWinds³³. Les auteures et auteurs de cybermenace parrainés par la Russie ciblent presque certainement les services infonuagiques comptant un grand nombre de clientes et clients au Canada³⁴.

Une auteure ou un auteur de cybermenace russe compromet le système de courriel d'entreprise de Microsoft à des fins d'espionnage

En janvier 2024, Microsoft a découvert qu'une auteure ou un auteur de cybermenace parrainé par la Russie connu sous le nom de Midnight Blizzard s'était introduit dans son service de courriel d'entreprise en nuage. Midnight Blizzard a accédé aux comptes de courriel d'entreprise de Microsoft, exfiltrant des correspondances entre Microsoft et des représentantes et représentants du gouvernement au Canada, aux États-Unis et au Royaume-Uni³⁵. Selon Microsoft, la personne en cause cherchait initialement à obtenir des renseignements à son sujet³⁶. Cette personne a ensuite utilisé des données personnelles et des justificatifs d'identité dans les courriels pour tenter d'accéder aux systèmes clients de Microsoft.

Figure 4 : Exemples notables d'activités de cybermenace non étatiques pro-Russie contre le Canada (2023)⁴¹

Février 2023

Des groupes d'auteurs et auteurs de cybermenace non étatiques pro-Russie participent à une campagne visant à saboter les infrastructures essentielles de pays qui prêtent assistance à l'Ukraine, y compris le Canada.

Avril 2023

Un groupe d'auteurs et auteurs de cybermenace non étatique pro-Russie revendique une campagne par DDoS contre des sites Web canadiens, notamment le site Web public du Cabinet du Premier ministre.

Septembre 2023

Un groupe d'auteurs et auteurs de cybermenace non étatique pro-Russie revendique une campagne par DDoS contre des sites Web canadiens, notamment des sites Web du gouvernement provincial du Québec.

Le Canada ciblé par des auteures et auteurs de cybermenace non étatiques pro-Russie pour influencer sa politique étrangère

À la suite de l'invasion de l'Ukraine par la Russie en 2022, des auteures et auteurs de cybermenace non étatiques pro-Russie, dont certains, nous estimons, ont probablement des liens avec le gouvernement et les services de renseignement russes, ont presque certainement mené des activités perturbatrices de cybermenace contre le Canada et ont utilisé les médias sociaux pour attirer l'attention sur ces attaques (voir la figure 4)³⁷. Nous croyons que ces campagnes visent fort probablement à influencer et à miner le soutien du Canada à l'endroit de l'Ukraine. Par exemple, une campagne d'attaque par déni de service distribué (DDoS) menée en avril 2023 par des auteures et auteurs de cybermenace non étatiques pro-Russie contre les sites Web du gouvernement du Canada et du secteur privé canadien a coïncidé avec la visite du premier ministre ukrainien au Canada³⁸.

Bien que les activités de cybermenace menées par des auteures et auteurs non étatiques pro-Russie contre le Canada aient principalement consisté en des attaques par DDoS et la défiguration de sites Web, quelques auteures et auteurs ont tenté de compromettre les systèmes de technologies opérationnelles (TO) au sein des infrastructures essentielles en Amérique du Nord et en Europe dans le but de perturber ces systèmes. Cette activité cible de façon opportuniste les appareils accessibles par Internet et exploite les vulnérabilités de base, comme les logiciels d'accès à distance non sécurisés ou l'utilisation de mots de passe par défaut³⁹. Par exemple, en janvier 2024, un groupe d'auteurs et auteurs de cybermenace non étatiques pro-Russie a revendiqué le débordement des réservoirs de stockage d'eau dans des installations de traitement de l'eau au Texas. Le groupe aurait publié une vidéo sur la compromission et la manipulation des systèmes de contrôle à chaque installation sur un forum public⁴⁰.

Nous estimons que des parties prenantes non étatiques pro-Russie tenteront probablement de perturber les systèmes de TO vulnérables branchés à Internet au sein des infrastructures essentielles canadiennes lorsque l'occasion se présentera. Les activités de cybermenace contre les TO menées par des auteures et auteurs de cybermenace non étatiques pro-Russie pourraient entraîner une défaillance des systèmes, ce qui pourrait endommager ou détruire ces systèmes et nuire à la sécurité publique.

République islamique d'Iran

L'Iran intensifie ses activités de cybermenace perturbatrices contre l'Occident

L'Iran dispose d'un programme de cyberactivité agressive, et le régime s'en sert pour contraindre, harceler et réprimer ses opposants et gérer les risques d'escalade. La volonté grandissante de l'Iran de lancer des cyberattaques destructrices au-delà du Moyen-Orient et ses efforts soutenus en vue de suivre et de surveiller les opposants du régime dans le cyberspace représentent une difficulté grandissante pour le Canada et ses alliés en matière de cybersécurité.

L'Iran a profité de son duel disputé dans le cyberspace avec Israël pour renforcer ses capacités de cyberespionnage et de cyberopérations offensives et pour perfectionner ses campagnes de collecte d'information, et il met presque assurément ses nouvelles connaissances à profit contre des cibles en Occident⁴². Pour l'heure, le Canada n'est probablement pas une cible prioritaire du programme de cyberactivité de l'Iran, mais les auteures et auteurs de cybermenace de ce pays ont vraisemblablement accès à des réseaux informatiques au Canada, dont ceux d'infrastructures essentielles.

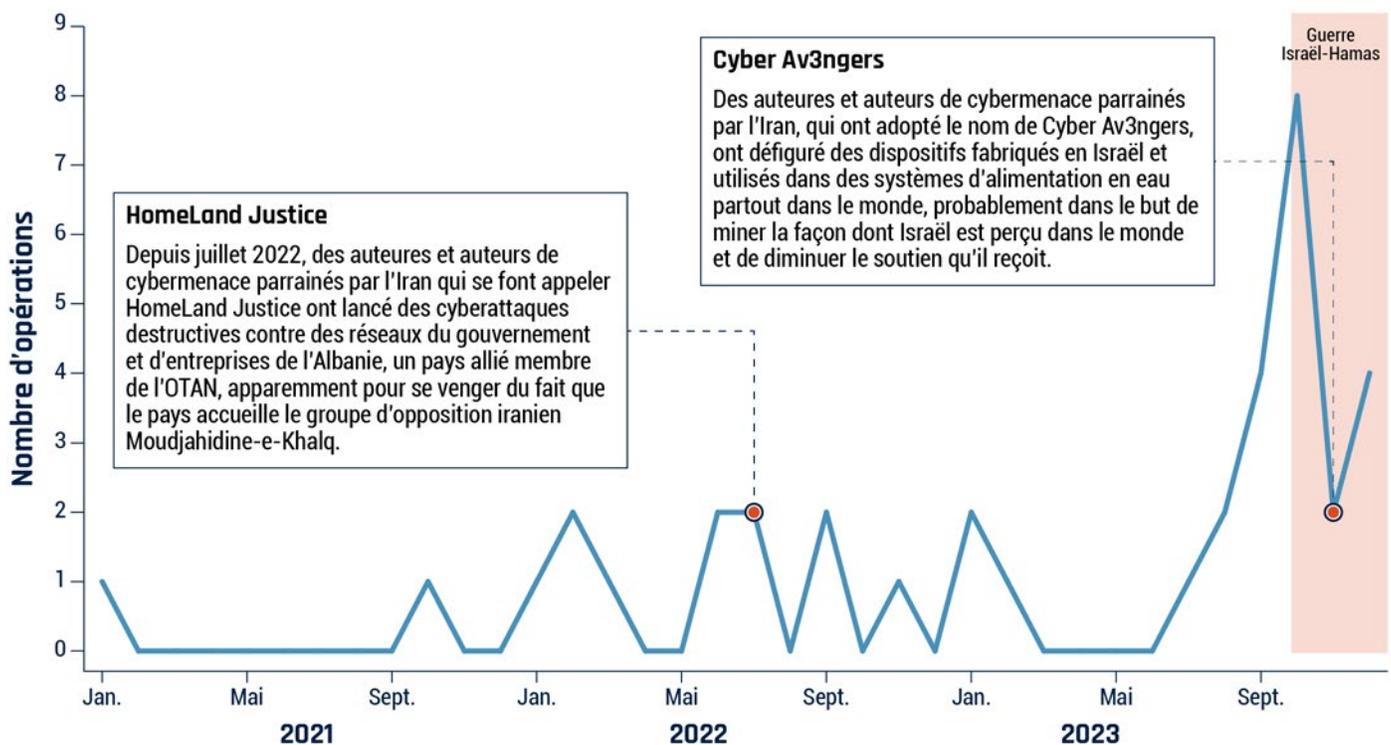
Les cyberopérations adverses menées par l'Iran dans le monde représentent un risque pour le Canada

Les auteures et auteurs de cybermenace parrainés par l'Iran ont mis sur pied et lancé des cyberopérations perturbatrices en plusieurs étapes partout dans le monde pour intimider les opposants du régime, signaler le mécontentement de celui-ci et persuader un pays de changer son attitude (voir la figure 5)⁴³.

Les auteures et auteurs de cybermenace iraniens ont mené des attaques par déni de service, tenté de manipuler des systèmes de contrôle industriels et accédé à des réseaux gouvernementaux et privés pour chiffrer, effacer et divulguer des données. L'Iran a tissé un réseau de hacktivisme composé de personas et de canaux de médias sociaux qui exploitent les événements perturbateurs pour propager les messages du régime et influencer le public cible tout en faisant en sorte que la participation de Téhéran à ces activités reste vague et niable⁴⁴.

Selon nos observations, la montée des tensions dans les relations bilatérales canado-iraniennes augmenterait fort probablement le risque que le Canada devienne une cible des cyberopérations perturbatrices de l'Iran.

Figure 5 : Cyberopérations perturbatrices liées publiquement à l'Iran (2021-2023)⁴⁵



L'Iran recourt au piratage psychologique à des fins de répression transnationale et d'espionnage

Il est probable que des auteures et auteurs de cybermenace parrainés par l'Iran surveillent des personnes au Canada qui sont une menace aux yeux du régime iranien, comme des activistes politiques, des journalistes, des chercheuses ou chercheurs dans le domaine des droits de la personne et des membres de la diaspora iranienne. Les groupes de cybermenace iraniens sont particulièrement habiles pour combiner le piratage psychologique et le harponnage dans le but de soutenir les activités de répression transnationale et de surveillance de Téhéran (voir la figure 6)⁴⁶. À titre d'exemple, l'Iran s'est fort probablement servi de l'écrasement du vol 752 à Téhéran comme leurre dans ses opérations de piratage psychologique et de harponnage. Ces efforts sont particulièrement inquiétants à la lumière de récentes informations rendues publiques qui lient l'Iran à des complots d'enlèvement et d'assassinat contre des opposants du régime qui habitent en Occident⁴⁷.

Figure 6 : Éléments d'une campagne de piratage psychologique menée par l'Iran



L'Iran se sert aussi du piratage psychologique pour cibler des fonctionnaires et accéder à des réseaux gouvernementaux et privés de partout dans le monde, notamment dans les secteurs de l'aérospatiale, de l'énergie, de la défense, des voyages et des télécommunications, pour répondre à ses besoins en matière de collecte de renseignement⁴⁸.



République populaire démocratique de Corée

Le programme de cyberactivité de la République populaire démocratique de Corée (RPDC) comporte deux volets : prioriser la production de revenus et répondre aux besoins du régime en matière de stratégie et de renseignement. Les auteurs et auteurs de cybermenace parrainés par la RPDC se livrent régulièrement à des activités de cybercriminalité, dont l'exploitation de rançongiciel et le vol de cryptomonnaies, pour financer les ambitions politiques et militaires du régime ainsi que les opérations du programme de cyberactivité⁴⁹. Le régime nord coréen oriente et protège fort probablement ces attaques motivées par des gains financiers et tolère vraisemblablement les activités de cybercriminalité nuisibles et perturbatrices⁵⁰.

Nous estimons que le programme de cyberactivité de la RPDC ne représente pas pour le Canada une cybermenace sur le plan stratégique comparable à celles que font planer d'autres pays, comme la RPC et la Russie. Toutefois, la volonté de Pyongyang de se tourner vers la cybercriminalité pour gouverner le pays fait presque assurément peser une menace persistante et sophistiquée sur des personnes et des organismes du Canada issus d'une grande variété d'industries et de secteurs de l'économie. La RPDC continuera presque assurément de s'adapter à l'évolution de la technologie numérique et de se livrer à de nouvelles opérations de cybercriminalité⁵¹.

République de l'Inde

Il est presque certain que les têtes dirigeantes de l'Inde aspirent à un programme de cyberactivité moderne doté de capacités internes⁵². L'Inde se sert fort probablement de son programme de cyberactivité pour faire avancer ses objectifs liés à la sécurité nationale, notamment en matière d'espionnage et d'antiterrorisme, et pour soutenir ses efforts visant à rehausser son statut mondial et à contrer les messages défavorables à l'endroit du pays et de son gouvernement. Nous estimons que le programme de cyberactivité indien recourt probablement à des fournisseurs commerciaux de cyberactivité pour renforcer ses opérations⁵³.

Selon nos observations, des auteurs et auteurs de cybermenace parrainés par l'Inde s'adonnent probablement à des activités de cybermenace contre les réseaux du gouvernement du Canada à des fins d'espionnage. Nous sommes d'avis que les relations bilatérales officielles canado-indiennes dicteront fort probablement les activités de cybermenace parrainées par l'Inde au détriment du Canada.



MENACES ÉMANANT DE LA CYBERCRIMINALITÉ

Un écosystème de cybercriminalité virtuel et interconnecté facilite la cybercriminalité comme service

La cybercriminalité opportuniste et motivée par des gains financiers est toujours l'activité de cybermenace la plus susceptible de toucher la population et les entreprises canadiennes. Nous estimons que si la cybercriminalité perdure au Canada et dans le monde, c'est presque assurément, en partie, à cause de la popularité du modèle opérationnel de cybercriminalité comme service (CaaS). Des auteurs et auteurs de menace spécialisés recourent à la CaaS pour vendre en ligne à d'autres cybercriminelles et cybercriminels des données volées ou fuitées et des outils malveillants prêts à l'emploi⁵⁴.

Services de la CaaS que les cybercriminelles et cybercriminels peuvent se procurer en ligne

- **Maliciel comme service** : Un service de soutien au développement et au déploiement de maliciels servant à voler ou à chiffrer les données de victimes ou à acquérir le contrôle à distance des systèmes des victimes.
- **Rançongiciel comme service** : Un noyau de développeuses et développeurs vend ou loue sa variante de rançongiciel à d'autres auteurs et auteurs de menace, appelés associées et associés; les développeurs aident les associées et associés dans le déploiement de leur rançongiciel en échange d'un paiement forfaitaire unique, de frais d'abonnement, d'une part des profits ou des trois.
- **Accès comme service** : Des auteurs et auteurs de menace spécialisés accèdent aux systèmes de victimes et vendent cet accès à des clientes et clients.
- **Hameçonnage comme service** : Instructions détaillées, modèles de courriels et outils prêts à l'emploi servant à exécuter des attaques d'hameçonnage.
- **Attaque par déni de service distribué (DDoS) comme service** : Location de réseaux de zombies et d'interfaces conviviales permettant aux clientes et clients de lancer des attaques par DDoS.
- **Exploitation comme service** : Des auteurs et auteurs de menace spécialisés louent des troussees d'exploitation à des clientes et clients et aident ceux-ci à utiliser les exploitations pour profiter de vulnérabilités logicielles.

Nous estimons que la CaaS a presque certainement fait augmenter le nombre de personnes se livrant à la cybercriminalité étant donné qu'elle réduit les obstacles à l'entrée et permet à des auteurs et auteurs de menace moins habiles sur le plan technique de lancer des attaques de cybercriminalité. Même les grands groupes de la cybercriminalité profitent des offres de la CaaS, comme les maliciels, les infrastructures de cyberattaque (par exemple, infrastructure d'hébergement) et les services de blanchiment d'argent, pour augmenter leurs capacités à mener des activités de la cybercriminalité⁵⁵.

Les plateformes en ligne jouent un rôle important dans la facilitation de la cybercriminalité

L'écosystème de la cybercriminalité est grandement interconnecté. Les plateformes en ligne, comme les marchés, les forums et les plateformes de clavardage liés à la cybercriminalité, facilitent la vente et la revente de données volées ainsi que les interactions entre les fournisseurs de CaaS et les cybercriminelles et cybercriminels qui cherchent à se procurer ces services. De plus, ces plateformes en ligne permettent à des cybercriminelles et cybercriminels de toutes les sphères d'activité d'établir des liens professionnels entre eux et d'échanger des ressources⁵⁶.

Figure 7 : Utilisation des plateformes en ligne par les cybercriminelles et cybercriminels



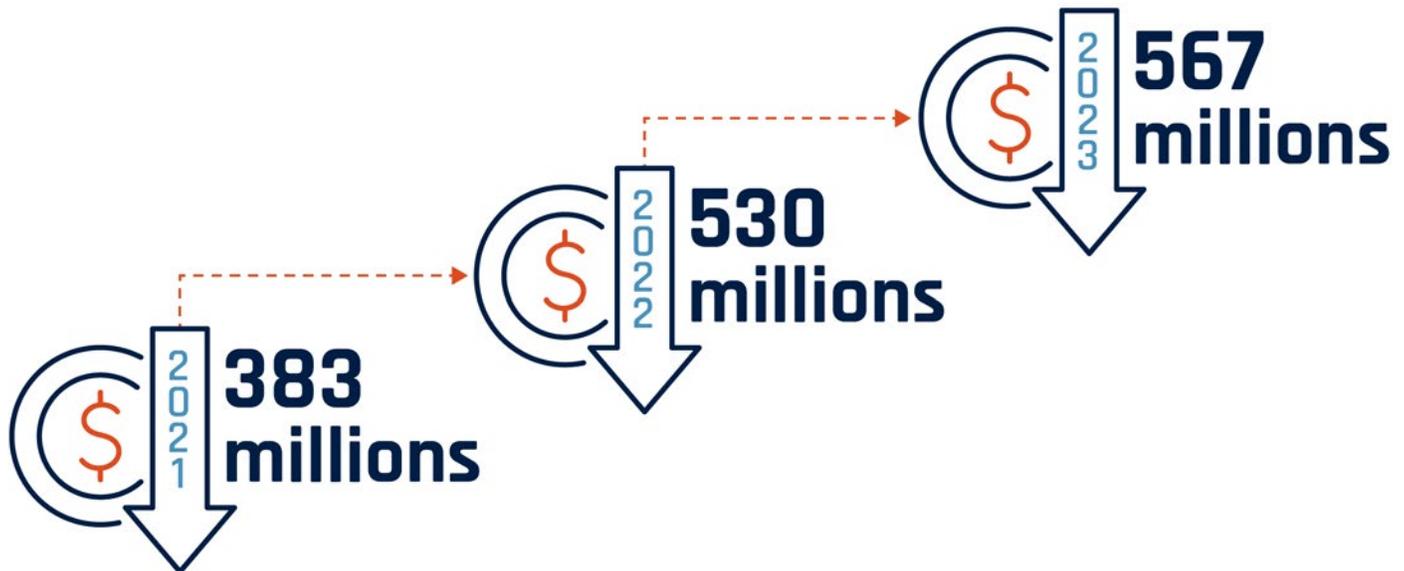
Genesis Market

Genesis Market était un marché de la cybercriminalité qui servait à la vente de justificatifs d'identité volés de millions d'ordinateurs compromis dans le monde. Les cybercriminelles et cybercriminels achetaient sur Genesis des justificatifs d'accès et des empreintes digitales numériques qui leur permettaient d'accéder à des comptes en ligne sans déclencher les alertes de sécurité. Genesis Market est lié à des millions d'incidents de cybersécurité motivés par des gains financiers, notamment des cas de fraude et des attaques par rançongiciel⁶⁰, perpétrés dès la création du marché en mars 2018 jusqu'à son démantèlement par les forces policières en avril 2023⁶¹.

La fraude et les escroqueries sont toujours une menace pour les Canadiennes et Canadiens

Comme nous l'avons mentionné dans l'ECMN de 2023-2024, nous sommes d'avis que la fraude et les escroqueries sont presque certainement les formes les plus communes de cybercrimes qui touchent les Canadiennes et Canadiens. Les cybercriminelles et cybercriminels tentent de voler de l'information personnelle, financière et d'entreprise en se servant de techniques de piratage psychologique comme l'hameçonnage⁶². L'hameçonnage est parmi les types de fraude les plus signalés au Canada et le harponnage est au nombre de ceux qui ont les plus importantes répercussions financières signalées pour les victimes⁶³. Par exemple, le harponnage peut mener à des compromissions qui entraînent le vol de données sensibles et qui peuvent engendrer des pertes financières considérables pour les entreprises⁶⁴.

Figure 8 : Pertes attribuables à des fraudes au Canada (en dollars canadiens)⁶⁵



De nouveaux outils et services rendent l'hameçonnage plus accessible et perfectionné

Nous estimons que la menace de fraude et d'escroquerie continuera de s'intensifier au cours des deux prochaines années en raison de la prolifération des outils à la disposition des cybercriminelles et cybercriminels, comme les troussees d'hameçonnage comme service vendues en ligne ainsi que les agents conversationnels alimentés par l'intelligence artificielle qui conçoivent des courriels d'hameçonnage convaincants. En raison de ces outils, les attaques par hameçonnage sont davantage à la portée des cybercriminelles et cybercriminels moins doués sur le plan technique⁶⁶.



La menace de rançongiciel au Canada continue de croître et d'évoluer

Les rançongiciels sont parmi les formes de cybercrime les plus perturbatrices qui planent sur le Canada et ses alliés. Depuis 2020, la portée, la fréquence et la complexité des attaques par rançongiciel ne font qu'augmenter⁶⁷. Nous estimons que les rançongiciels continueront presque assurément à représenter la cybermenace la plus percutante qui pèsera sur les organisations canadiennes ces deux prochaines années étant donné que les opératrices et opérateurs de rançongiciel peaufinent constamment leurs tactiques pour maximiser les profits⁶⁸.

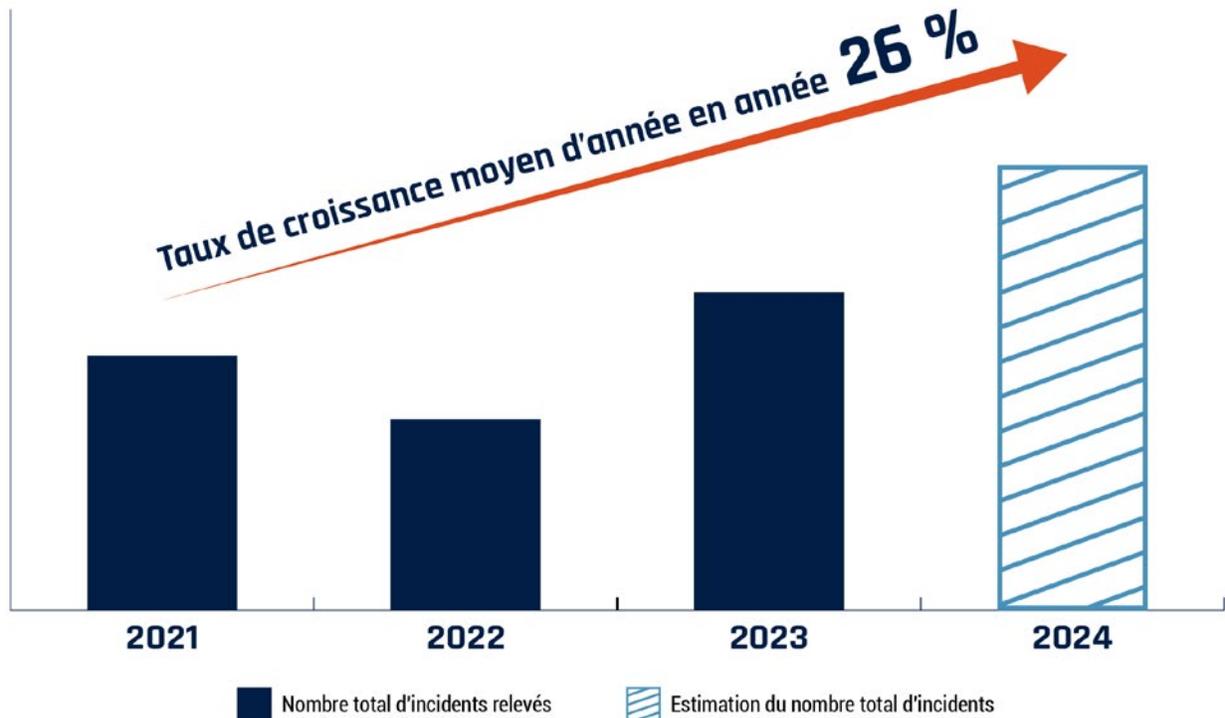
Augmentation du nombre d'incidents liés à des rançongiciels et de rançons

2023 a été une année record en ce qui a trait aux rançongiciels. Certaines estimations indiquent que le nombre d'incidents liés à des rançongiciels dans le monde a augmenté de 74 pour cent en 2023 par rapport à 2022⁶⁹, et que les rançons versées à l'échelle planétaire se sont élevées à la somme record d'un milliard de dollars américains⁷⁰. Selon une estimation, la rançon moyenne versée au Canada en 2023 était de 1,130 million de dollars canadiens, ce qui représente une hausse de presque 150 pour cent sur deux ans⁷¹. Des sources ouvertes rapportent que cette tendance s'est poursuivie au cours de la première moitié de 2024 et que le montant des rançons et le nombre d'incidents devraient dépasser ceux observés en 2023⁷². Les augmentations observées d'incidents liés à des rançongiciels sont presque assurément plus élevées étant donné que de nombreux incidents ne sont pas signalés⁷³. Nous estimons que la menace de rançongiciel continuera presque certainement de croître au cours des deux prochaines années à moins que l'écosystème de rançongiciel soit profondément fragilisé.

Principales menaces de rançongiciel dans le monde en 2023

1. **LOCKBIT** : Lockbit est un groupe cybercriminel de RaaS qui exploite une variante de rançongiciel du même nom qui a servi à nuire à une grande variété d'entités des infrastructures essentielles, notamment dans les secteurs gouvernemental, des soins de santé et de l'énergie⁷⁴.
2. **ALPHV** : ALPHV est un groupe cybercriminel de RaaS qui exploite la variante de rançongiciel BlackCat qui a servi à nuire à diverses industries des secteurs financier, manufacturier, juridique et judiciaire et de services professionnels, entre autres⁷⁵.
3. **CLOP** : CLOP est un RaaS exploité par le groupe cybercriminel russophone TA505 qui a servi à nuire à diverses industries en exploitant des vulnérabilités logicielles non corrigées⁷⁶.
4. **PLAY** : Play est un groupe cybercriminel de RaaS qui exploite une variante de rançongiciel du même nom qui a servi à nuire à des organismes des secteurs des soins de santé et de la manufacture⁷⁷.
5. **BLACK BASTA** : Black Basta est un groupe cybercriminel de RaaS qui exploite une variante de rançongiciel du même nom qui a servi à nuire à des entités des infrastructures essentielles, dont des organismes des secteurs gouvernemental et des soins de santé⁷⁸.

Figure 9 : Croissance relative depuis 2021 des incidents liés à des rançongiciels au Canada connus du Centre pour la cybersécurité⁷⁹



En 2022, nous avons estimé que la diminution observée s'explique en partie par la pression accrue exercée par les forces policières qui a probablement poussé certains opérateurs et opératrices de rançongiciel à suspendre temporairement leurs activités. L'invasion de l'Ukraine par la Russie a probablement aussi perturbé l'écosystème des rançongiciels. Par exemple, certains opérateurs et opératrices de rançongiciel ont vraisemblablement délaissé la cybercriminalité motivée par des intérêts financiers pour lancer des attaques à caractère politique⁸⁰. Toutefois, en 2023, les opératrices et opérateurs de rançongiciel se sont fort probablement remis sur pied après ces perturbations et ont élevé leur jeu d'un cran pour compenser les pertes financières subies en 2022⁸¹.

Répercussions de CLOP - Compromissions des chaînes d'approvisionnement numériques

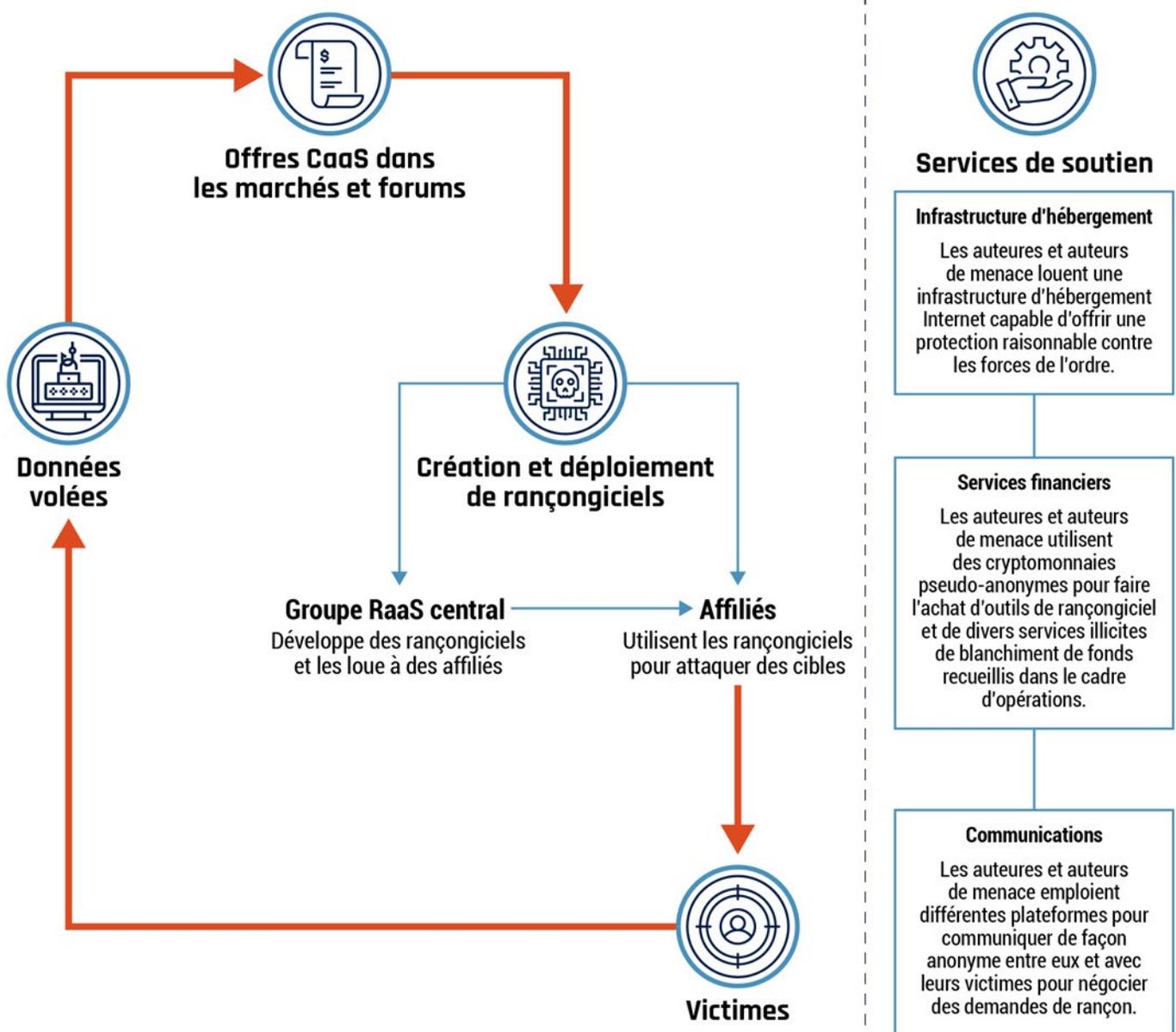
Pour se procurer divers services et applications, de nombreuses organisations comptent sur les chaînes d'approvisionnement numériques composées de multiples fournisseurs. Les cybercriminelles et cybercriminels peuvent profiter d'une intrusion contre un seul fournisseur pour déclencher une cascade d'incidents touchant de nombreuses organisations⁸². Par exemple, la flambée d'incidents liés à des rançongiciels à l'échelle planétaire en 2023 peut fort probablement être en partie attribuée à CLOP, une souche de rançongiciel exploitée par des cybercriminelles et cybercriminels russophones⁸³. CLOP a servi à exploiter des vulnérabilités non corrigées dans les populaires logiciels d'application de transfert de fichiers GoAnywhere et MOVEit. Selon les estimations, seulement avec MOVEit, CLOP a touché 2 750 entreprises et 94 millions de personnes⁸⁴ et engrangé environ 100 millions de dollars américains en rançons⁸⁵. Parce qu'elles sont très profitables, les attaques par rançongiciel contre les chaînes d'approvisionnement numériques vont presque certainement se poursuivre au cours des deux prochaines années.

Les principaux groupes de rançongiciel utilisent le modèle de rançongiciel comme service

Comme l'indiquait l'ECMN de 2023-2024, la plupart des principaux groupes de rançongiciel qui sévissent au Canada recourent au modèle de RaaS selon lequel un noyau d'opératrices et opérateurs vend ou loue sa variante de rançongiciel à des associées ou associés qui lancent les attaques. L'écosystème de RaaS fait partie de l'écosystème plus vaste de CaaS. Il est alimenté par une chaîne d'approvisionnement complexe composée de divers intervenants qui offrent différents services de CaaS pouvant servir à mener des attaques par rançongiciel. Cela comprend les services de soutien qui sont à la base du fonctionnement de l'écosystème (voir la figure 10)⁸⁶.

Nous estimons que la popularité soutenue du RaaS contribue presque certainement à l'augmentation du nombre d'incidents liés à des rançongiciels étant donné qu'il réduit les obstacles techniques à l'entrée et permet à un plus grand nombre d'auteurs et auteurs de lancer des attaques sans avoir à développer leur propre rançongiciel⁸⁷. Il est difficile de localiser précisément les opératrices et opérateurs de rançongiciel. Toutefois, nous estimons que le noyau de membres des principaux groupes de rançongiciel qui sévissent au Canada se trouve fort probablement dans des pays de l'ancienne Union soviétique, mais que leurs associées ou associés mènent leurs activités à partir de n'importe où dans le monde.

Figure 10 : Écosystème du rançongiciel comme service



Les rançongiciels affectent les infrastructures essentielles du Canada

Nous estimons que les opératrices et opérateurs de rançongiciel profitent presque certainement des occasions qui se présentent à eux et ne visent aucune industrie en particulier. Ces dernières années, une grande variété d'entreprises canadiennes ont été touchées par des incidents liés à des rançongiciels, y compris de grands détaillants et des établissements d'enseignement. Ces incidents démontrent qu'aucune entité n'est à l'abri de la menace de rançongiciel. Toutefois, les rançongiciels sont presque assurément la principale menace de la cybercriminalité qui plane sur les infrastructures essentielles du Canada, car ils peuvent paralyser des opérations d'affaires essentielles, détruire ou endommager des données commerciales importantes et révéler de l'information sensible⁸⁸. En plus d'engendrer des pertes financières causées par la réparation des systèmes et la perturbation des opérations, les attaques par rançongiciel peuvent ébranler des services essentiels et ainsi mettre en péril la sécurité physique et le bien-être émotionnel des victimes⁸⁹.

Les infrastructures essentielles sont une cible attrayante pour les opératrices et opérateurs de rançongiciel, car elles sont perçues comme étant disposées à payer de fortes rançons pour protéger leurs opérations essentielles. En 2021, des rançons de plusieurs millions de dollars ont été versées aux auteurs et auteurs de menace responsables des incidents liés à des rançongiciels menés contre Colonial Pipeline aux États-Unis et les opérations de JBS Foods en Amérique du Nord et en Australie⁹⁰.

Selon des rapports sur la cybersécurité, les victimes en 2023 étaient moins enclines à payer les rançons demandées⁹¹. Nous estimons que la perspective d'enregistrer d'importants profits, jumelée à la volonté décroissante des victimes de verser des rançons, ont presque certainement encouragés les groupes de rançongiciel plus avancés sur le plan technique à rehausser leurs techniques d'extorsion et à embaucher des associées ou associés compétents capables de cibler des entités des infrastructures essentielles pour empocher des rançons plus importantes⁹². Cette technique s'appelle la chasse au « gros gibier » et elle est, selon nos estimations, la principale stratégie utilisée par nombre des groupes de rançongiciel les plus efficaces qui sévissent au Canada⁹³.



Figure 11 : Incidents de cybersécurité affectant les infrastructures essentielles du Canada

Les secteurs d'activités des infrastructures essentielles du Canada ont été la cible de divers incidents de cybersécurité, dont des incidents liés à des rançongiciels et des intrusions de réseau, qui ont eu pour effet de perturber leurs fonctions opérationnelles essentielles.

Secteur de l'énergie



Juin 2023 : Suncor Energy a été la cible d'un incident de cybersécurité qui a affecté sa filiale Petro-Canada. L'incident a nui temporairement au traitement des transactions par cartes de crédit et de débit dans les stations-service à l'échelle du Canada⁹⁴.

Secteur des soins de santé



Décembre 2022 : L'hôpital SickKids de Toronto a été la cible d'un incident par rançongiciel perpétré par un affilié du groupe de rançongiciel LockBit. Les répercussions de l'incident ont été mineures et LockBit a émis des excuses publiques et offert de fournir le décrypteur à l'hôpital⁹⁵.

Octobre 2023 : Daixin, un groupe de rançongiciel, est responsable d'un incident lié à des rançongiciels qui a touché 5 hôpitaux dans le sud de l'Ontario. L'incident visait le fournisseur de technologies de l'information des hôpitaux et a forcé ceux-ci à arrêter temporairement leurs systèmes internes. Il a mené au vol de dossiers sensibles et entraîné des retards dans les soins prodigués aux patientes et patients⁹⁶.

Février 2024 : LockBit aurait revendiqué un incident lié à des rançongiciels contre la chaîne de pharmacies canadienne London Drugs qui a forcé l'entreprise à fermer temporairement certains de ses magasins dans l'ouest du Canada⁹⁷.

Secteur gouvernemental



Juin 2023 : Le gouvernement de la Nouvelle-Écosse a été affecté par l'exploitation mondiale des vulnérabilités du système de transfert de fichiers MOVEit effectuée par le groupe CL0P. Selon les estimations, l'incident a mené à la fuite des renseignements personnels de 100 000 fonctionnaires qui sont ou qui ont été employés et employés par la province⁹⁸.

Septembre 2023 : Des cybercriminelles et cybercriminels se sont introduits dans les systèmes de Services globaux de relogement Brookfield (BGRS), entreprise qui aide le personnel militaire et du Service extérieur du Canada avec les réinstallations, et ont accédé sans autorisation aux renseignements de membres du personnel du gouvernement du Canada⁹⁹.

Mars 2024 : Un incident lié à des rançongiciels a ciblé les systèmes de technologies de l'information de la ville de Hamilton qui gèrent diverses fonctions municipales, comme les lignes téléphoniques de la ville. Ses effets se sont fait ressentir pendant des semaines¹⁰⁰.

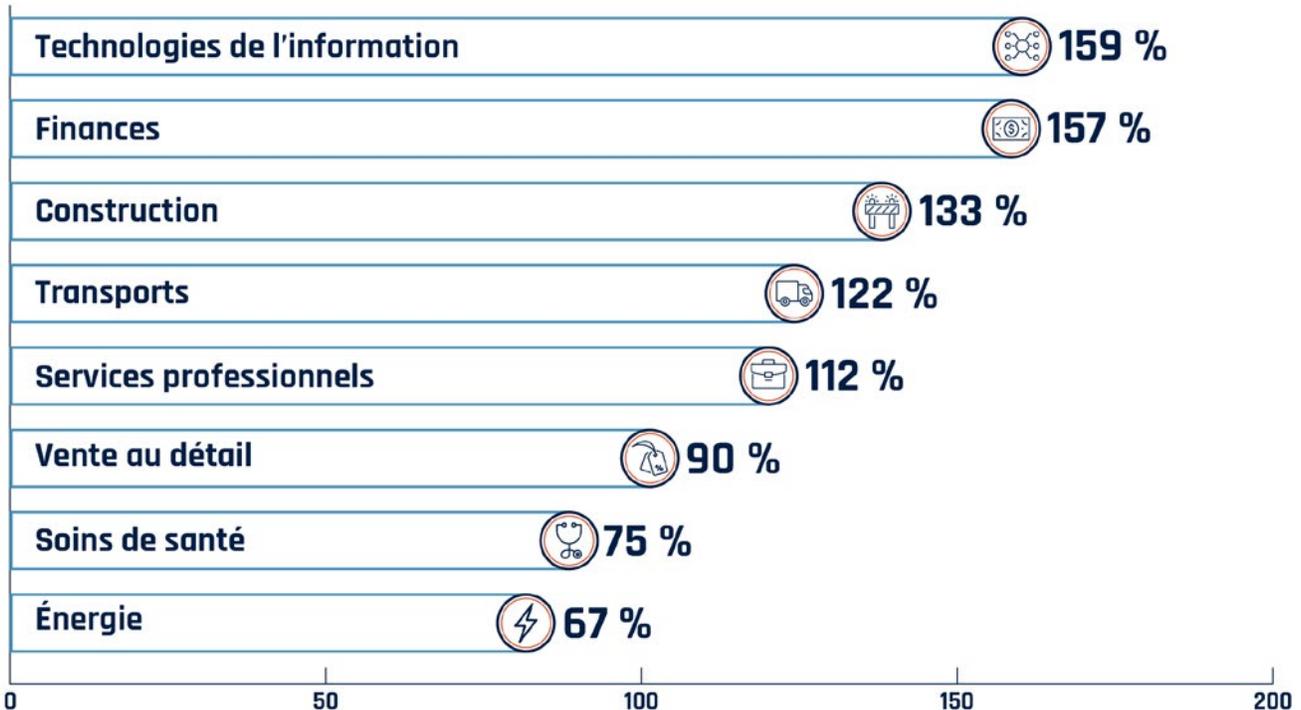


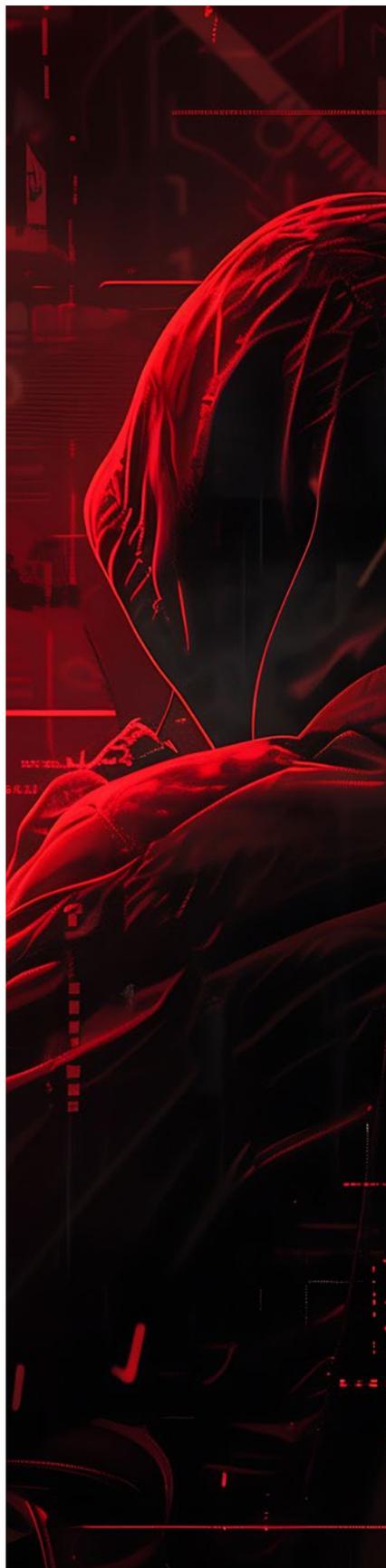
Augmentation du nombre d'incidents liés à des rançongiciels touchant le secteur des soins de santé

Le nombre d'incidents de rançongiciel ciblant le secteur des soins de santé augmente de façon régulière dans le monde¹⁰¹. Ces dernières années, le Canada et ses alliés ont tous vécu des attaques par rançongiciel très médiatisées contre le secteur des soins de santé. En mars 2024, Change Healthcare a versé une rançon de plusieurs millions de dollars pour que des données médicales sensibles soient restaurées à la suite d'une attaque par rançongiciel qui a perturbé le processus de facturation pour les ordonnances dans des pharmacies partout aux États-Unis¹⁰². Peu de temps après, soit en juin 2024, un incident lié à des rançongiciels ciblant la société de pathologie Synnovis a entraîné des retards importants dans plusieurs hôpitaux de Londres, au Royaume-Uni, et a mené au vol de données sensibles que les opératrices et opérateurs de rançongiciel ont publiées en ligne¹⁰³.

Selon une estimation, le nombre d'incidents liés à des rançongiciels touchant le secteur des soins de santé a presque doublé depuis 2022¹⁰⁴. Cette situation est inquiétante, car de tels incidents nuisent directement à la capacité des entités du secteur des soins de santé à offrir des services essentiels aux patientes et patients¹⁰⁵. Toutefois, nous estimons qu'au cours des deux prochaines années, les opératrices et opérateurs de rançongiciel continueront presque assurément à choisir leurs victimes en fonction des occasions qui se présentent à eux plutôt qu'à jeter leur dévolu sur des cibles précises. Toute augmentation observée d'incidents liés à des rançongiciels touchant le secteur des soins de santé reflétera presque certainement une hausse du nombre d'incidents liés à des rançongiciels en général ainsi qu'un recours continu à la chasse au « gros gibier » par les principaux groupes de rançongiciel.

Figure 12 : Augmentation, par secteur, du nombre d'incidents liés à des rançongiciels au Canada observés par le Centre pour la cybersécurité, de 2022 à 2023





Les opératrices et opérateurs de rançongiciel peaufinent leurs tactiques pour maximiser les profits et éviter la détection

Les opératrices et opérateurs de rançongiciel améliorent sans cesse leurs stratégies et adaptent leurs techniques afin de maximiser leurs profits et d'éviter la détection par les forces policières¹⁰⁶. Nous sommes d'avis que les motivations financières et la souplesse du modèle de RaaS ont presque assurément renforcé la résistance des opératrices et opérateurs de rançongiciel face aux mesures de perturbation prises par les organismes d'application de la loi.

L'écosystème de rançongiciel se fractionne sous l'effet de la pression des organismes d'application de la loi

Des opérations majeures menées récemment par les forces d'application de la loi partout dans le monde dans le but de fragiliser l'écosystème de rançongiciel ont presque certainement amoindri les capacités des groupes visés et semé le chaos dans les mouvements cybercriminels clandestins¹⁰⁷. Cependant, nous sommes d'avis que ces perturbations n'auront presque certainement pas un effet à long terme sur l'environnement de rançongiciel parce que les opératrices et opérateurs trouvent habituellement des façons de s'ajuster, de se doter d'une nouvelle image et de reprendre leurs opérations, sauf si les membres des principaux groupes de RaaS sont arrêtés¹⁰⁸.

Dans le même ordre d'idée, il est presque certain que le modèle de CaaS a rendu l'écosystème de rançongiciel plus résistant aux mesures prises par les organismes d'application de la loi. Il est difficile d'enquêter sur la cybercriminalité étant donné la complexité du réseau dont font partie les services facilitateurs et les cybercriminelles et cybercriminels qui interagissent dans des espaces en ligne sans frontières¹⁰⁹. Si une opération policière ébranle les opérations d'un fournisseur de CaaS populaire, la ou le responsable va souvent renouveler son image et relancer ses services ou bien un autre service va rapidement prendre sa place. En raison de la souplesse du modèle de CaaS, il est facile pour les cybercriminelles et cybercriminels de faire appel simultanément à plusieurs fournisseurs de services de sorte à pouvoir se tourner vers d'autres fournisseurs si l'un d'eux se fait prendre¹¹⁰.

Opérations internationales de perturbation menées par les organismes d'application de la loi contre l'écosystème de rançongiciel

Les groupes suivants étaient des éléments importants de l'écosystème de rançongiciel. Avant les opérations de perturbation, ils étaient liés à plus de 1 000 compromissions partout dans le monde et avaient amassé des millions de dollars en rançon¹¹¹.

- **Janvier 2023** : Des organismes d'application de la loi ont infiltré les réseaux de Hive, fourni les décrypteurs aux victimes pour qu'elles puissent récupérer leurs données et saisi l'infrastructure de Hive¹¹².
- **Décembre 2023** : Des organismes d'application de la loi ont saisi l'infrastructure d'ALPHV (aussi connu sous le nom de BlackCat) et fourni un décrypteur aux victimes¹¹³.
- **Février 2024** : Des organismes d'application de la loi ont saisi l'infrastructure de LockBit et ont gelé des comptes de cryptomonnaie liés à LockBit. Ils ont aussi arrêté certains des membres principaux du groupe¹¹⁴.

Nous estimons avec quasi-certitude que le fractionnement de l'écosystème de rançongiciel s'intensifiera au cours des deux prochaines années¹¹⁵. Les associées ou associés commenceront presque certainement à agir de façon autonome et à créer leurs propres variantes de rançongiciel pour réduire le risque d'être touchés par les opérations de perturbation des organismes d'application de la loi¹¹⁶. Nous estimons que les plus petits groupes de rançongiciel commenceront probablement à collaborer pour accroître leurs capacités ou tenteront d'attirer dans leurs rangs des associées ou associés de groupes touchés par les opérations de perturbation afin de prendre la place de leurs anciens compétiteurs et s'emparer d'une plus grande part du marché des attaques par rançongiciel, ce qui vient embrouiller davantage le contexte de la menace¹¹⁷.

Intensification des méthodes d'extorsion

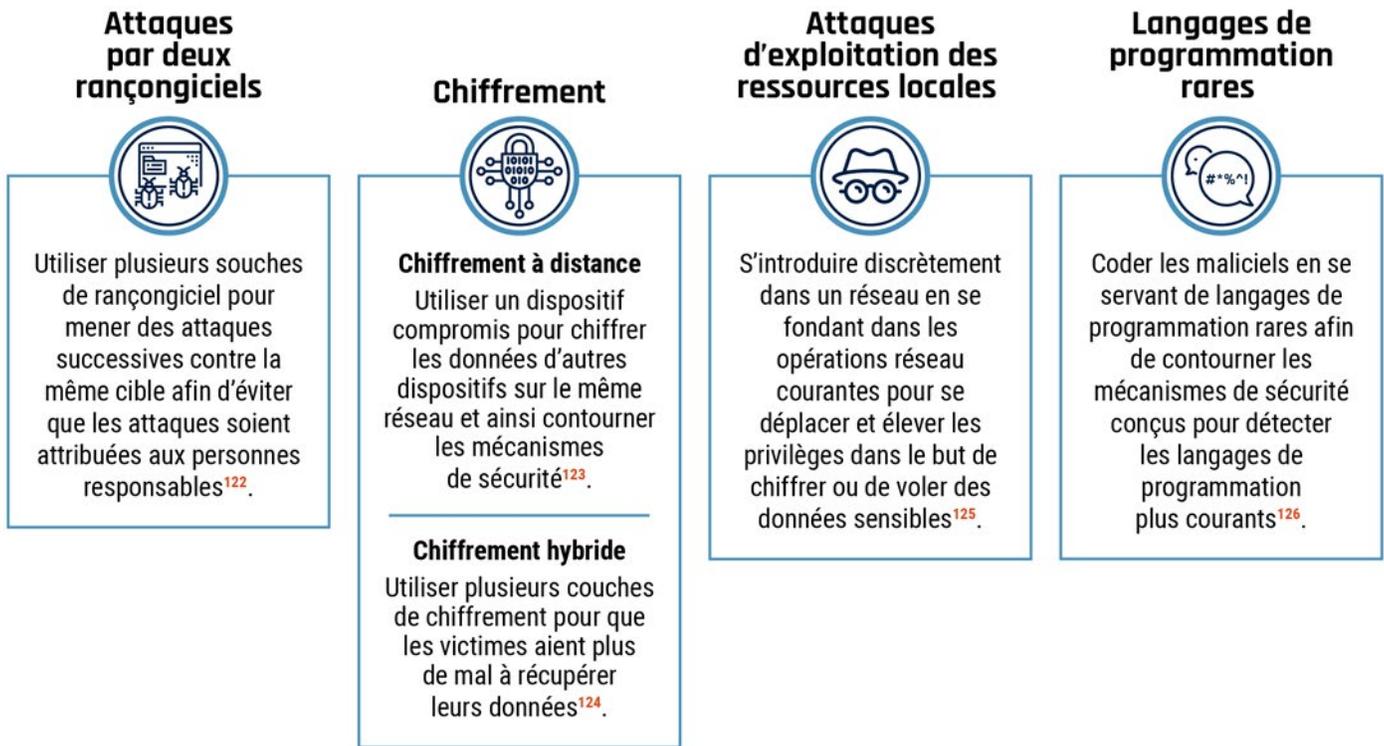
Les opératrices et opérateurs de rançongiciel intensifient leurs méthodes d'extorsion et exercent une plus grande pression sur les victimes pour qu'elles paient les rançons. Certains groupes de rançongiciel ont commencé à afficher sur leur site Web un compte à rebours jusqu'à la fuite prévue des données volées ou ils vont même jusqu'à appeler directement les victimes ou leurs clients et à les menacer de divulguer leur information personnelle s'ils ne paient pas la rançon demandée¹¹⁸. De plus, des opératrices et opérateurs de rançongiciel ont critiqué publiquement les organisations victimes de leur rançongiciel dans le but de nuire à leur réputation et ont encouragé des clients des victimes à poursuivre ces dernières en justice¹¹⁹. Des opératrices et opérateurs de rançongiciel ont même commencé à faire pression sur leurs victimes en évoquant de nouvelles lois qui obligent les victimes à signaler les incidents liés à des rançongiciels. Par exemple, des opératrices et opérateurs liés à ALPHV ont prétendu avoir déposé une plainte auprès de la Commission des valeurs mobilières des États-Unis (U.S. Securities and Exchange Commission) contre la victime parce que celle-ci a omis de signaler un incident lié à des rançongiciels dont ALPHV est lui-même responsable¹²⁰. Nous estimons que les opératrices et opérateurs de rançongiciel continueront de modifier leurs méthodes d'extorsion au cours des deux prochaines années dans le but de maximiser la chance de recevoir des paiements des victimes.

Les opératrices et opérateurs de rançongiciel emploient de nouvelles tactiques pour cacher leurs activités

Des organismes d'application de la loi se sont intéressés de près à certains opérateurs et opératrices de rançongiciel, alors nombre d'entre eux ont commencé à appliquer simultanément plusieurs techniques d'obscurcissement pour se camoufler, éviter la détection et minimiser leur empreinte numérique¹²¹.



Figure 13 : Techniques d'obscurissement utilisées dans le cadre d'incidents liés à des rançongiciels



La collaboration est de mise pour contrer la menace changeante de rançongiciel

Nous sommes d'avis que les opératrices et opérateurs de rançongiciel continueront à diversifier leurs tactiques en réaction à l'attention grandissante que leur portent les organismes d'application de la loi. Pour contrer la menace à l'avenir, il sera primordial de comprendre la menace et le modèle d'activité de CaaS et de tenir compte de la nature changeante de l'écosystème. La collaboration entre l'industrie, les organismes d'application de la loi et tous les échelons de gouvernement ainsi que la sensibilisation de la population canadienne à la cybercriminalité seront de mise pour renforcer la résilience face à cette menace changeante¹²⁷.



**TENDANCES QUI INFLUENCENT
LE CONTEXTE DES
CYBERMENACES DU CANADA**

Contexte

Le CST utilise son expertise pour aider à surveiller et à détecter les menaces sur les réseaux et systèmes d'information du Canada, ainsi que pour mener des enquêtes connexes. Selon nos observations depuis l'ECMN 2023-2024, nous avons relevé cinq tendances qui influenceront le contexte des cybermenaces du Canada jusqu'en 2026 :

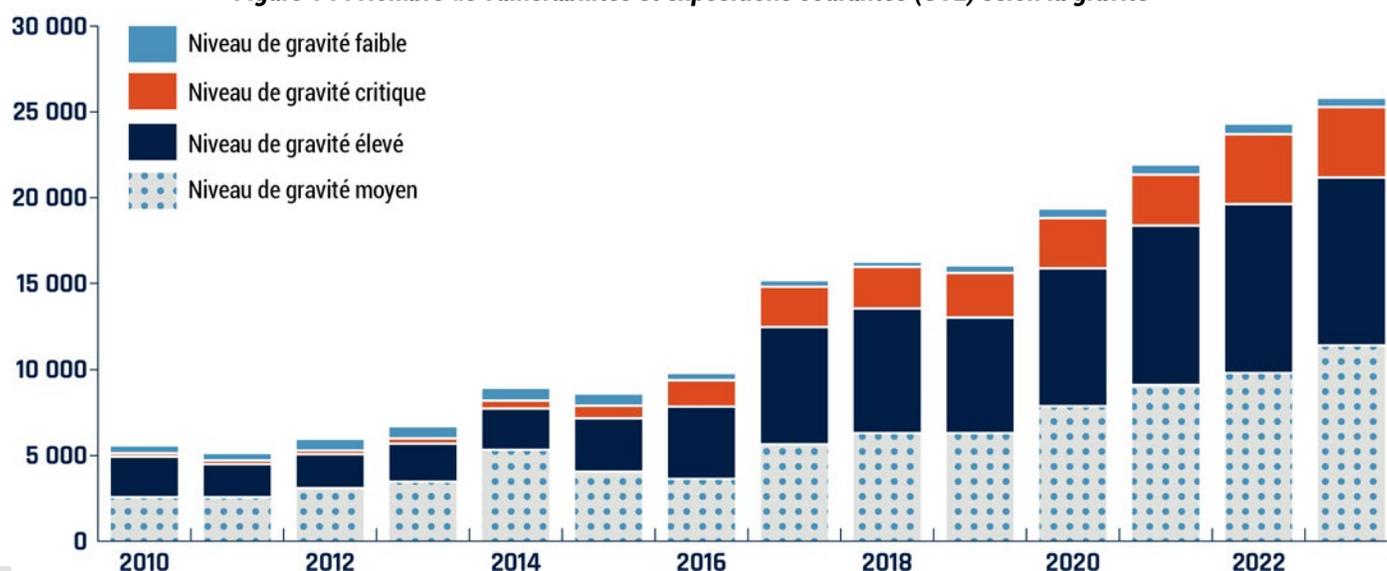
- **Tendance no 1** : Les technologies d'intelligence artificielle (IA) amplifient les menaces dans le cyberspace
- **Tendance no 2** : Le savoir-faire des auteures et auteurs de cybermenace évolue pour échapper à la détection
- **Tendance no 3** : Les auteures et auteurs de cybermenace non étatiques inspirés par des intérêts géopolitiques sont source d'imprévisibilité
- **Tendance no 4** : La concentration des fournisseurs augmente la vulnérabilité en matière de cybersécurité
- **Tendance no 5** : Les services commerciaux à double usage se retrouvent sur le champ de bataille numérique

Les tendances notées dans les ECMN antérieures sont toujours pertinentes

Avant d'examiner les cinq tendances susmentionnées, il est important de noter que les tendances ayant une incidence sur le contexte des cybermenaces du Canada énumérées dans les ECMN précédentes demeurent d'actualité. Ces tendances continuent à évoluer au fil du temps en fonction des développements géopolitiques, technologiques et des auteures et auteurs de menace. Par exemple :

- **L'exposition aux cybermenaces continue d'augmenter** : Outre l'adoption et le déploiement continu de l'Internet des objets (par exemple, les véhicules connectés), il est prévu que l'essor des services et des plateformes infonuagiques d'IA stimule la demande pour les infrastructures de soutien, comme la production d'énergie et les centres de données capables d'appuyer l'IA, et mène au transfert de volumes encore plus élevés de données aux environnements en nuage. Il est aussi très probable que les organisations spécialisées dans l'IA (dont les laboratoires axés sur la recherche sur l'IA et le développement de modèles d'IA) soient maintenant des cibles plus importantes pour les auteures et auteurs de cybermenace¹²⁸.
- **Les attaques contre la chaîne d'approvisionnement se poursuivent** : Les auteures et auteurs de cybermenace continuent de lancer des attaques contre la chaîne d'approvisionnement numérique en compromettant ou en exploitant un fournisseur de services infonuagiques, de technologies de l'information (TI) ou de logiciels pour permettre l'exploitation des clientes et clients qui utilisent le service. Ces attaques comprennent les doubles attaques contre la chaîne d'approvisionnement, où une attaque contre la chaîne d'approvisionnement en amène une autre¹²⁹.
- **Les vulnérabilités publiques continuent d'être exploitées** : Les auteures et auteurs de cybermenace mènent constamment des analyses afin de trouver des vulnérabilités de sécurité publiques dans les logiciels et exploitent les vulnérabilités non corrigées afin d'accéder sans autorisation à des réseaux privés et publics. Le nombre de vulnérabilités et expositions courantes (CVE pour *Common Vulnerabilities and Exposures*) continue d'augmenter (voir la figure 14). Les auteures et auteurs de menace exploitent ces vulnérabilités plus rapidement que jamais. Des attaques sont lancées à peine quelques jours après le dévoilement d'une vulnérabilité¹³⁰.

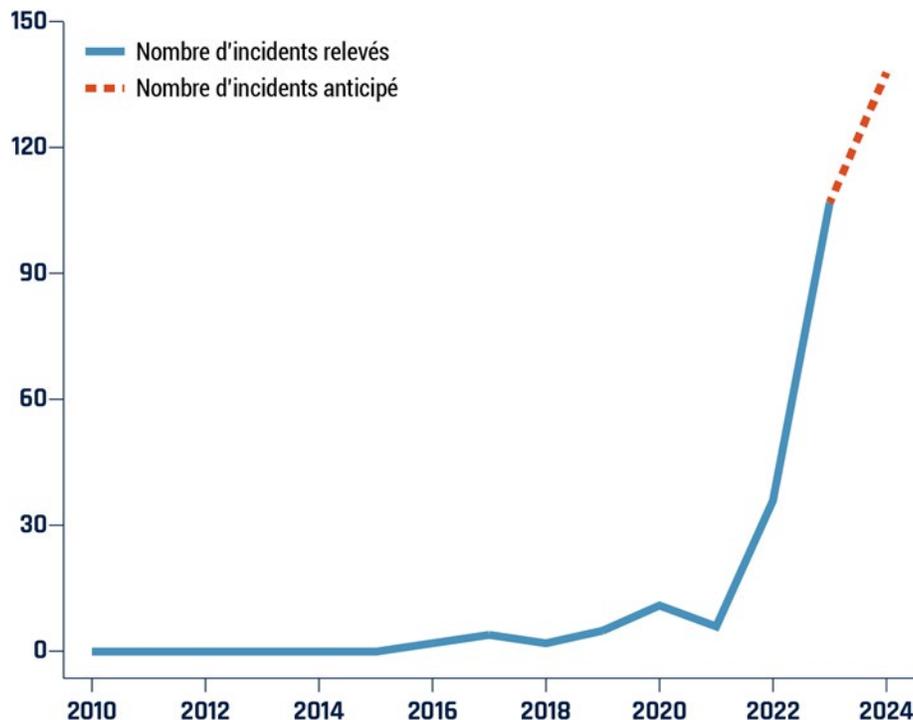
Figure 14 : Nombre de vulnérabilités et expositions courantes (CVE) selon la gravité¹³¹



Tendance no 1 : Les technologies d'intelligence artificielle amplifient les menaces dans le cyberspace

Les technologies d'IA réduisent presque certainement les obstacles à l'entrée et augmentent la qualité, l'ampleur et la précision des activités de cybermenace malveillantes¹³². Les cybercriminelles et cybercriminels ainsi que les auteures et auteurs de cybermenace parrainés par un État utilisent des outils d'IA générative et prédictive (notamment les grands modèles de langage [GML]) pour appuyer leurs processus de travail, de la génération de contenu à l'analyse de mégadonnées. Nous estimons que les auteures et auteurs de cybermenace compétents sur le plan technique tenteront presque certainement de trouver de nouvelles façons malveillantes d'employer les outils d'IA au cours des deux prochaines années à mesure que les technologies évoluent. Ils pourraient, par exemple, automatiser certaines parties de la chaîne de cyberattaque dans le but d'accroître la productivité¹³³.

Figure 15 : Incidents liés à l'IA générative à l'échelle mondiale ayant été signalés publiquement et ayant causé un préjudice ou un quasi-préjudice¹³⁴



L'IA améliore la personnalisation et le pouvoir de persuasion des attaques par piratage psychologique

Les cybercriminelles et cybercriminels ainsi que les auteures et auteurs de cybermenace parrainés par un État ont presque certainement recours à des GML pour améliorer les attaques par piratage psychologique qui visent à manipuler les cibles afin de les amener à faire quelque chose qui porte atteinte à leurs intérêts, comme divulguer de l'information sensible, autoriser des transactions frauduleuses ou télécharger un maliciel¹³⁵. Les outils d'IA générative permettent aux auteures et auteurs de cybermenace de créer du contenu visuel et audio réaliste en usurpant l'identité de personnes de confiance (c'est-à-dire l'hypertrucage), ce qui renforce l'apparence de légitimité aux yeux des cibles et aide à les persuader¹³⁶. Les auteures et auteurs de cybermenace ont également recours à l'IA pour concevoir des courriels d'hameçonnage personnalisés à grande échelle qui sont à la fois convaincants et rédigés sans erreurs grammaticales et dans un style naturel. Les destinataires ont alors encore plus de mal à repérer et à filtrer les tentatives d'hameçonnage¹³⁷.

Les technologies d'IA augmentent la qualité et l'ampleur des campagnes étrangères d'influence en ligne

Dans l'ECMN 2023-2024, nous avons discuté de la façon dont les auteures et auteurs de cybermenace peuvent créer et répandre la désinformation générée par IA. Depuis, un nombre croissant de pays, y compris la Chine, la Russie, l'Iran et Israël, auraient incorporé des articles, des images et des vidéos générés par IA trompeurs ou faux (hypertrucage) à leurs opérations d'influence en ligne (mésinformation, désinformation et malinformation) afin d'augmenter la qualité et l'ampleur de leurs campagnes¹³⁸. Ils utilisent également très probablement des outils d'IA pour générer des personas fictifs en ligne et des comptes robots sur les médias sociaux dans le but d'amplifier l'engagement¹³⁹. Ces campagnes visent à affaiblir les adversaires en polluant l'espace d'information en ligne, en minant la confiance envers les institutions et en semant le doute et la division au sein de la société ciblée¹⁴⁰.

Nous estimons que la désinformation accentuée par l'IA risque davantage de gagner du terrain lorsqu'elle présente au moins l'une des caractéristiques suivantes¹⁴¹ :

- intensifie des messages polarisants qui existent déjà dans la société ciblée;
- comble un vide dans l'espace d'information;
- est répandue par une ou des sources fiables ou officielles;
- cible des situations temporaires où le temps pour réfuter le faux contenu est limité.

L'essor des sites Web générés par IA

Les États étrangers créent des sites Web de fausses nouvelles qui ont l'air de vrais organes de presse dans le cadre de leurs campagnes de désinformation. Bon nombre de ces sites sont conçus pour ressembler à des médias locaux qui ont cessé leurs activités et reposent sur du contenu généré par IA¹⁴².

L'IA prédictive améliore les capacités d'analyse des mégadonnées

Les États bien nantis tirent très probablement avantage des outils d'IA pour les aider à traiter et à analyser les larges volumes de données qu'ils recueillent. Nous évaluons que les services de renseignement étranger utilisent très probablement l'analyse de données augmentée par IA pour trouver des schémas et des modèles dans les données en masse, obtenir des renseignements sur les personnes et les actifs d'intérêt, et informer les cyberopérations consécutives¹⁴³.



Tendance no 2 : Le savoir-faire des auteures et auteurs de cybermenace évolue pour échapper à la détection

Puisque les mesures de défense des réseaux réussissent mieux à détecter les menaces pour la sécurité et à y intervenir, les auteures et auteurs de cybermenace ont développé leur savoir-faire dans le but de réduire au minimum la détection et de dissimuler plus longtemps leurs activités sur les systèmes des victimes.

Les auteures et auteurs de cybermenace ciblent et exploitent les appareils périphériques connectés pour accéder à des réseaux

Les auteures et auteurs de cybermenace exploitent les vulnérabilités touchant les dispositifs de sécurité et de réseau situés en périphérie des réseaux – que l'on appelle les appareils « périphériques » connectés (comme les routeurs, les pare-feux et les solutions de réseau privé virtuel [RPV]). En compromettant un appareil périphérique connecté, une auteure ou un auteur de cybermenace peut s'introduire dans un réseau, surveiller, modifier et exfiltrer le trafic réseau circulant sur l'appareil ou possiblement pénétrer encore plus loin dans le réseau de la victime.

Les auteures et auteurs de cybermenace ciblent très probablement les appareils périphériques connectés parce que les mesures de défense réseau peuvent offrir des capacités limitées de surveillance et de détection des activités liées à des maliciels sur les réseaux, surtout comparativement à d'autres vecteurs d'accès tels que les courriels d'hameçonnage¹⁴⁴. À titre d'exemple, au début de 2024, le Canada et ses alliés ont détecté qu'une auteure ou un auteur de cybermenace parrainé par un État doté de fonds importants et de moyens sophistiqués avait recueilli et exfiltré des données après avoir exploité deux vulnérabilités nouvellement découvertes dans des appareils RPV utilisés par les réseaux du gouvernement et d'infrastructures essentielles nationales¹⁴⁵.

Les auteures et auteurs de menace exploitent des ressources locales dans les environnements compromis pour échapper à la détection

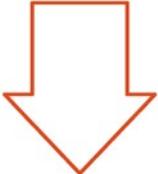
Les auteures et auteurs de cybermenace ayant recours à des techniques d'exploitation des ressources locales (LOTL pour *Living-of-the-Land*) utilisent, à d'autres fins, les processus et les outils natifs des systèmes qui sont déjà présents dans l'environnement afin de se déplacer discrètement dans le réseau¹⁴⁶. Les mesures de défense réseau parviennent difficilement à détecter les intrusions puisqu'il n'y a pas de déploiement de maliciel ou d'outil personnalisé sur le réseau compromis¹⁴⁷. Des auteures et auteurs de cybermenace parrainés par la Chine, la Russie et l'Iran ont recours à des techniques LOTL¹⁴⁸. Par exemple, une auteure ou un auteur de cybermenace russe aurait compromis le réseau d'un service public d'électricité ukrainien en octobre 2022 et utilisé des techniques LOTL pour se déplacer dans l'environnement de technologies opérationnelles du service public avant de provoquer une panne d'électricité¹⁴⁹.

Les auteures et auteurs de cybermenace abusent d'infrastructures à domicile pour cacher leurs activités malveillantes

Des auteures et auteurs de cybermenace parrainés par un État ainsi que des cybercriminelles et cybercriminels mènent presque assurément des activités malveillantes contre le Canada en se servant des ressources virtuelles et des infrastructures de mise en réseau (comme les routeurs) situées en Amérique du Nord pour limiter la surveillance et la visibilité de leurs opérations¹⁵¹. À titre d'exemple, afin de se fondre dans les activités réseau normales, des auteures ou auteurs de cybermenace parrainés par la Russie et la Chine ont été observés en train d'acheminer leurs cyberopérations malveillantes au moyen d'équipement réseau compromis de petites entreprises et de bureaux à domicile (SOHO pour *Small Office and Home Office*) situé au Canada et aux États-Unis, notamment des routeurs appartenant à des ménages et à des entreprises qui ne se doutaient de rien¹⁵².

Le temps d'occupation des attaquantes et attaquants diminue

Le temps d'occupation global moyen – nombre de jours pendant lesquels une attaquante ou un attaquant est présent sur un système compromis avant la détection – a continué de diminuer en 2023 comparativement à 2022.

Mandiant¹⁵⁰
16 jours
 en 2022

10 jours
 en 2023

Tendance no 3 : Les auteures et auteurs de cybermenace non étatiques inspirés par des intérêts géopolitiques sont source d'imprévisibilité

Les conflits et les tensions géopolitiques inspirent des activités de cybermenace perturbatrices chez les groupes non étatiques que l'on appelle communément les hacktivistes. Les hacktivistes motivés par des intérêts géopolitiques mènent généralement des attaques dans le but d'attirer l'attention, dont des attaques par DDoS, la défiguration de sites Web et des fuites de données. Certains groupes ont augmenté l'impact de leurs activités en ciblant, de façon opportuniste, et en perturbant les infrastructures essentielles vulnérables, comme les réseaux d'adduction et de distribution d'eau, ce qui risque d'entraîner de graves préjudices pour le public¹⁵³.

L'hacktivisme géopolitique est en forte hausse en période de conflits militaires. Les groupes hacktivistes ont orchestré des campagnes en lien avec l'invasion de l'Ukraine par la Russie en 2022 et la guerre entre Israël et le Hamas en 2023¹⁵⁴. Les tensions diplomatiques motivent également les activités d'hacktivisme. Après que le Canada a accusé l'Inde d'être impliquée dans l'assassinat d'un citoyen canadien, un groupe hacktiviste pro-Inde a déclaré avoir défiguré des sites Web au Canada et avoir lancé de brèves attaques par DDoS contre de tels sites Web, y compris le site Web public des Forces armées canadiennes¹⁵⁵.

Cet écosystème non étatique est dynamique et imprévisible. Certaines et certains hacktivistes sont réellement motivés par un mélange de patriotisme, d'idéologie ou par une cause politique, mais d'autres sont opportunistes et profitent des conflits à des fins personnelles ou de notoriété. De nouveaux groupes font leur entrée de jeu régulièrement, alors que d'autres groupes bien établis se dissolvent et réapparaissent sous un nouveau nom. Les cibles et les motivations des joueuses et joueurs changent couramment. Des groupes s'unissent pour collaborer et coordonner leurs efforts, même si les intérêts géopolitiques pour lesquels ils militent sont différents¹⁵⁶. Bien que les activités d'hacktivisme puissent parfois être alignées sur les intérêts d'un État adverse, la relation entre un hacktiviste et l'État, le cas échéant, peut être difficile à discerner.



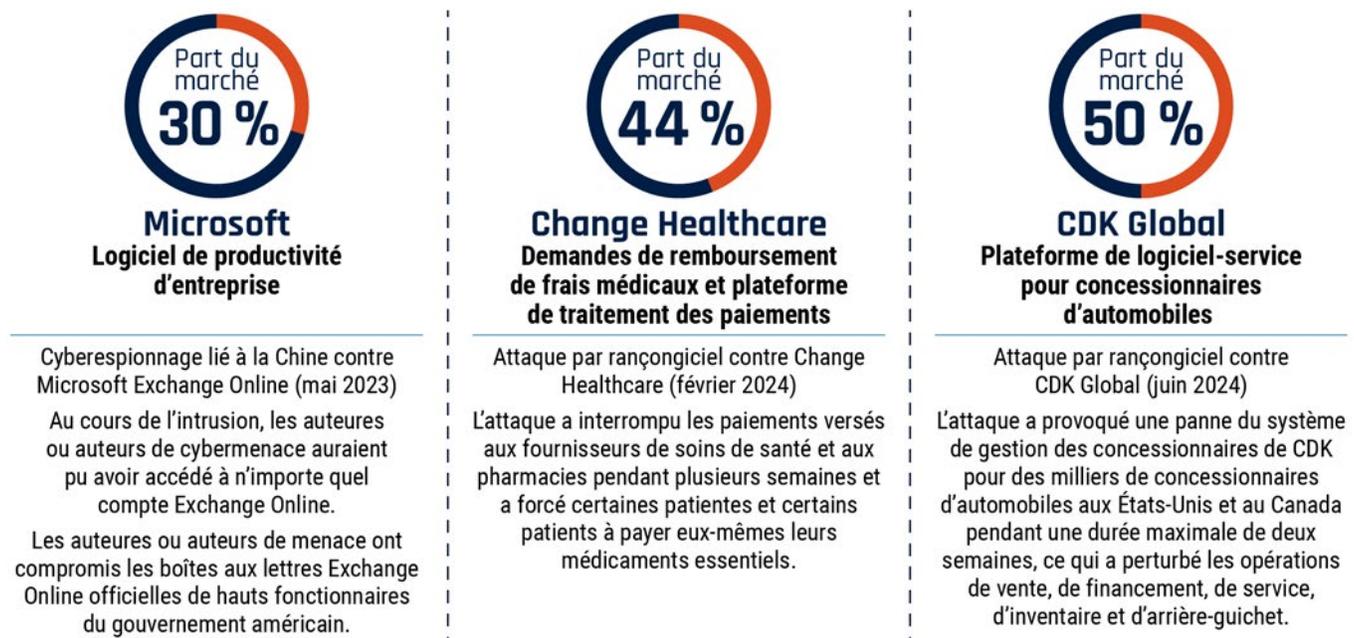
Tendance no 4 : La concentration des fournisseurs augmente la vulnérabilité en matière de cybersécurité

La prestation de nombreux services technologiques est concentrée, puisqu'un service numérique donné est offert par quelques grands fournisseurs seulement qui comptent chacun une vaste base d'utilisatrices et utilisateurs¹⁵⁷. Des organisations des secteurs public et privé, dont des banques, des compagnies aériennes et des prestataires de soins de santé, dépendent de ces fournisseurs de service dominants, comme un fournisseur de services infonuagiques ou une plateforme logiciel-service spécialisée, pour soutenir des fonctions et des opérations critiques¹⁵⁸. Un cyberincident touchant un seul fournisseur de services dominant peut avoir un impact sur l'ensemble d'un secteur.

Les fournisseurs de services dominants sont des cibles de prédilection pour les auteurs et auteures de cybermenace qui cherchent à voler les données de la clientèle ou à obtenir des rançons¹⁵⁹. À titre d'exemple, Amazon, Microsoft et Google, les trois fournisseurs de services infonuagiques commerciaux les plus importants qui représentent environ 65 % du marché infonuagique mondial, font face sans relâche aux assauts des auteurs et auteures de cybermenace étatiques qui développent des capacités pour les compromettre¹⁶⁰. Ces auteurs et auteures se renseignent sur les réseaux internes des plateformes infonuagiques et améliorent leurs techniques pour contourner les mécanismes de sécurité et exfiltrer des données sans se faire découvrir.

La compromission des fournisseurs de services dominants amplifie l'impact des incidents de cybersécurité. Les activités de cybermenace contre des services qui représentent de véritables goulots d'étranglement numériques – points de défaillance uniques dans les chaînes d'approvisionnement – peuvent avoir un effet de domino déstabilisant et généralisé sur l'économie et la société, voire mettre en péril notre sécurité nationale (voir la figure 16)¹⁶¹.

Figure 16 : Cyberattaques récentes contre les fournisseurs dominants et leur part du marché¹⁶²



Même si les fournisseurs de services dominants savent qu'ils sont des cibles très prisées, l'envergure et la complexité de leurs opérations peuvent limiter leur capacité de découvrir et de corriger les vulnérabilités en matière de cybersécurité¹⁶³. Par exemple, en mai 2023, une auteure ou un auteur de menace que l'on considère affilié à la Chine a compromis le service de messagerie Exchange de Microsoft qui est basé sur le nuage et, selon le comité d'examen de la cybersécurité (*Cyber Safety Review Board*) des États-Unis qui enquêtait sur l'incident, cette intrusion aurait pu être évitée¹⁶⁴. Moins d'un an plus tard, en novembre 2023, une auteure ou un auteur de cybermenace parrainé par la Russie a compromis à son tour le service Exchange du géant de l'informatique et a exfiltré des données de comptes de courriel d'entreprise de Microsoft, y compris des données de clientes et clients. Puis, en juillet 2024, le service d'informatique en nuage Azure de Microsoft n'a pas résisté à une attaque par DDoS qui a causé une interruption de certains services Microsoft partout dans le monde pendant des heures¹⁶⁵. D'après Microsoft, une erreur dans ses mécanismes de défense a contribué à la panne¹⁶⁶.

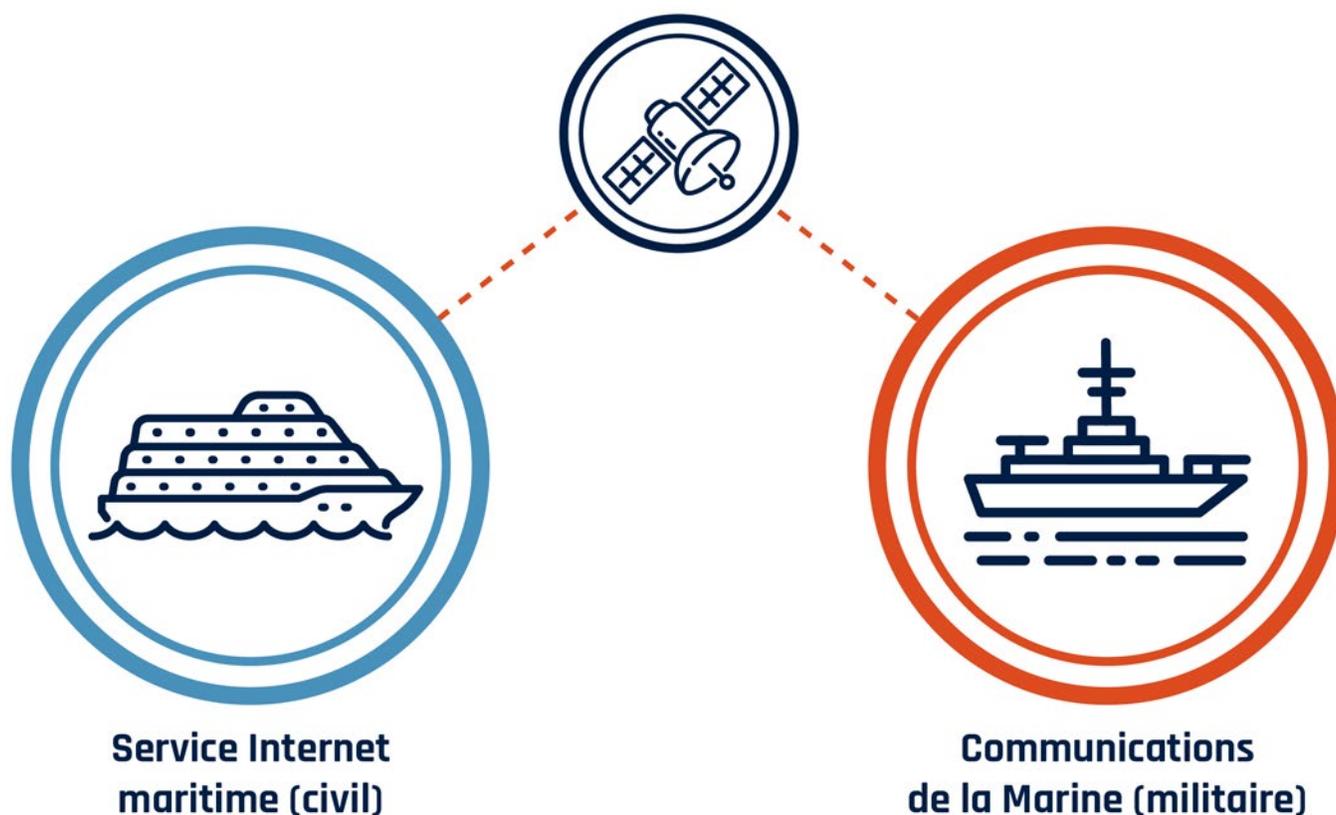
Tendance no 5 : Les services commerciaux à double usage se retrouvent sur le champ de bataille numérique

Des gouvernements partout dans le monde se tournent vers des services commerciaux pour s'assurer un avantage concurrentiel sur leurs adversaires et assurer leur résilience durant un conflit. Les solutions commerciales, telles que les capacités informatiques avancées et les systèmes commerciaux de télécommunications par satellite, permettent aux forces armées et aux organismes de renseignement d'avoir accès à des technologies novatrices à grande échelle pouvant être déployées rapidement¹⁶⁷.

Nous estimons que les services commerciaux fournis à des clientèles civiles et militaires (appelés services à double usage) sont presque certainement ciblés par des auteurs et auteurs de cybermenace parrainés par un État¹⁶⁸. Nos adversaires se sont montrés désireux et capables de faire appel à des cyberattaques pour interrompre, réduire ou refuser l'accès de leurs concurrents à des services commerciaux lors d'un conflit armé¹⁶⁹. Ces attaques peuvent avoir un effet domino perturbateur sur les clientes et clients civils ainsi que les clientes et clients d'infrastructures essentielles qui utilisent ces mêmes services.

Par exemple, des auteurs et auteurs de cybermenace parrainés par un État visent très probablement les systèmes satellites commerciaux à double usage qui appuient les communications militaires ou gouvernementales, les outils de télédétection et les capacités de navigation. Depuis le début de l'invasion de l'Ukraine par la Russie en février 2022, des auteurs et auteurs de cybermenace parrainés par la Russie mènent des opérations de guerre informatique et électronique (comme le brouillage et l'usurpation) contre les services de télécommunications par satellite commerciaux utilisés par les forces armées ukrainiennes¹⁷⁰. Au moins l'une de ces attaques a causé une interruption des services Internet par satellite pour des clientes et clients civils à l'extérieur de la zone de conflit.

Figure 17 : Exemple de service de télécommunications par satellite à double usage



Conclusion

Les auteures et auteurs de cybermenace représentent une menace persistante pour la prospérité économique et la sécurité nationale du Canada. En tant que pays prospère, le Canada demeure une cible intéressante pour les cybercriminelles et cybercriminels motivés par l'appât du gain qui sont appuyés par un écosystème de cybercriminalité hautement adaptable et résilient. Parallèlement, la menace que font peser les activités de cybermenace parrainées par des États sur le Canada sera influencée par les événements géopolitiques au-delà de nos frontières, l'état des relations étrangères du Canada et un contexte international défini par la rivalité sur le plan économique et technologique¹⁷¹. Les menaces dans le cyberspace seront de plus en plus influencées par un système mondial où un large éventail d'auteurs et auteurs de cybermenace forment des réseaux de force et de convenance variées à la poursuite de leurs intérêts individuels¹⁷².

En dépit des vulnérabilités en matière de cybersécurité du Canada et de l'environnement de cybermenace qui évolue sans cesse, il est possible d'atténuer l'intensité des cybermenaces et leur incidence sur le Canada grâce à la sensibilisation et à l'adoption de pratiques exemplaires en matière de cybersécurité par la population et les organisations.

Le CST met à profit tous les aspects de son mandat, ainsi que ses partenariats, pour défendre les réseaux fédéraux et les systèmes d'importance pour le gouvernement du Canada. Il continuera à communiquer de l'information importante sur le contexte des cybermenaces à la population canadienne, au secteur privé et aux infrastructures essentielles. Les Canadiennes et Canadiens peuvent avoir l'assurance que le Centre pour la cybersécurité est déterminé à surveiller les cybermenaces pesant sur le Canada, à faire avancer la cybersécurité et à protéger les systèmes sur lesquels ils comptent au quotidien, en soutenant les réseaux des infrastructures essentielles ainsi que d'autres systèmes qui sont importants pour le Canada. Nous continuerons de travailler avec le secteur privé pour favoriser la sécurité et la résilience, et pour nouer des partenariats internationaux en vue d'atteindre nos objectifs communs en matière de cybersécurité.

Nous invitons les lectrices et lecteurs à consulter nos [conseils sur la cybersécurité](#)¹⁷³ pour obtenir de plus amples renseignements sur les cybermenaces exposées dans la présente évaluation et sur les façons de se protéger contre ces cybermenaces. Les organisations peuvent également consulter notre [Boîte à outils des objectifs intersectoriels relatifs à l'état de préparation en matière de cybersécurité](#)¹⁷⁴ pour en apprendre davantage sur les approches permettant d'améliorer leur posture de cybersécurité.

Notes de fin de texte

- 1 <https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2018>
- 2 <https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020>
- 3 <https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024>
- 4 <https://www.cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces>
- 5 <https://www.pensezcybersecurite.gc.ca/>
- 6 Statistique Canada. *Enquête canadienne sur l'utilisation d'Internet, 2022*, 20 juillet 2023. <https://www150.statcan.gc.ca/n1/daily-quotidien/230720/dq230720b-fra.htm>; DIXON, Chris. *Read Write Own: Building the Next Era of the Internet*, New York: Random House, 2024.
- 7 Federal Trade Commission. *FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens*, 19 septembre 2024. <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance> (en anglais seulement); GOUJON, Reva. *Shut Out: Data Security and Cybersecurity Converge in Next Wave of US Tech Controls*, Rhodium Group, 5 mars 2024. <https://rhg.com/research/shut-out-data-security-and-cybersecurity-converge-in-next-wave-of-us-tech-controls/> (en anglais seulement).
- 8 KLAAS, Brian. *The CrowdStrike Failure Was a Warning*, The Atlantic, 21 juillet 2024. <https://www.theatlantic.com/ideas/archive/2024/07/crowdstrike-failure-warning-solutions/679174/> (en anglais seulement).
- 9 <https://www.cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces>
- 10 <https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023>
- 11 <https://www.cyber.gc.ca/fr/orientation/menace-posee-generateurs-texte-bases-modeles-langage-grande-taille>
- 12 RAUCH, Jonathan. *The World is Realigning*, The Atlantic, 1er juillet 2024. <https://www.theatlantic.com/ideas/archive/2024/07/russia-china-nato-axis-resistance/678831/> (en anglais seulement); WONG, Chun Han. *China's Xi Jinping Takes Rare Direct Aim at U.S. in Speech*, The Wall Street Journal, 6 mars 2023. <https://www.wsj.com/articles/chinas-xi-jinping-takes-rare-direct-aim-at-u-s-in-speech-5d8fde1a> (en anglais seulement).
- 13 SMEETS, Max. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, Oxford: Oxford University Press, 2022 (en anglais seulement); PANDIT, Rajat. *Armed forces formulate new doctrine for cyberspace operations*, The Times of India, 18 juin 2024. <https://timesofindia.indiatimes.com/india/armed-forces-formulate-new-doctrine-for-cyberspace-operations/articleshow/111089679.cms> (en anglais seulement).
- 14 Google Threat Analysis Group. *Buying Spying: Insights into Commercial Surveillance Vendors*, Google, février 2024. <https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/> (en anglais seulement); ROBERTS, Jen, et coll. *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and its Threats to National Security and Human Rights*, DFRLab, 4 septembre 2024. <https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/> (en anglais seulement).

- 15 Mise en accusation caviardée. *United States v. Gaobin*, 1:24-cr-00043, (E.D.N.Y.), déposée le 25 mars 2024. <https://www.justice.gov/usao-edny/media/1345131/dl> (en anglais seulement); United States Department of the Treasury. *Treasury Designates Iranian Cyber Actors Targeting U.S. Companies and Government Agencies*, 23 avril 2024. <https://home.treasury.gov/news/press-releases/jy2292> (en anglais seulement); SEPHARD, Christian, et coll. *Leaked files from Chinese firm show vast international hacking effort*, The Washington Post, 22 février 2024. <https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoan/> (en anglais seulement); United States Department of Justice. *Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of The Islamic Revolutionary Guards Corps*, 23 mars 2018. <https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary> (en anglais seulement); Google Threat Analysis Group. *Buying Spying: Insights into Commercial Surveillance Vendors*, Google, février 2024. <https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/> (en anglais seulement); WAHLSTROM, Alden, et coll. *Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan*, Mandiant, 30 mars 2023. <https://cloud.google.com/blog/topics/threat-intelligence/cyber-operations-russian-vulkan> (en anglais seulement); United States Department of Commerce. *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*, 3 novembre 2021. <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list> (en anglais seulement) SMEETS, Max. *Hack Global, Buy Local: The Inefficiencies of the Zero-Day Exploit Market*, Lawfare, 6 juin 2022. <https://www.lawfaremedia.org/article/hack-global-buy-local-inefficiencies-zero-day-exploit-market> (en anglais seulement).
- 16 Centre canadien pour la cybersécurité. *Cyberbulletin : Le Centre pour la cybersécurité invite les Canadiennes et Canadiens à s'informer et à se protéger contre les activités de cybermenace de la RPC*, 3 juin 2024. <https://www.cyber.gc.ca/fr/orientation/cyberbulletin-centre-cybersecurite-invite-canadiennes-canadiens-sinformer-se-protger-contre-activites-cybermenace-rpc>.
- 17 Mise en accusation caviardée. *United States v. Gaobin*, 1:24-cr-00043, (E.D.N.Y.), déposée le 25 mars 2024. <https://www.justice.gov/usao-edny/media/1345131/dl> (en anglais seulement).
- 18 FIFE, Robert, et Steve CHASE. *Canadian spy agency says it shared details of Chinese hacking with Parliamentary officials*, The Globe and Mail, 30 avril 2024. <https://www.theglobeandmail.com/politics/article-canadian-spy-agency-says-it-shared-details-of-chinese-hacking-with> (en anglais seulement).
- 19 Centre canadien pour la cybersécurité. *Cyberbulletin : Le Centre pour la cybersécurité invite les Canadiennes et Canadiens à s'informer et à se protéger contre les activités de cybermenace de la RPC*, 3 juin 2024. <https://www.cyber.gc.ca/fr/orientation/cyberbulletin-centre-cybersecurite-invite-canadiennes-canadiens-sinformer-se-protger-contre-activites-cybermenace-rpc>.
- 20 United States Department of State. *Global Engagement Center Special Report: How the People's Republic of China Seeks to Reshape the Global Information Environment*, 28 septembre 2023. <https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/> (en anglais seulement); Plainte et affidavit caviardés à l'appui de l'application de mandats d'arrestation. *United States v. Bai*, 1:23-mj-00334, (E.D.N.Y.), déposés le 6 avril 2023. https://www.justice.gov/d9/2023-04/squad_912_-_23-mj-0334_redacted_complaint_signed.pdf (en anglais seulement). United States House Select Committee on the CCP. *HEARING: CCP Transnational Repression: The Party's Effort to Silence and Coerce Critics Overseas*, 13 décembre 2023. <https://selectcommitteeonthecp.house.gov/media/witness-testimony/hearing-ccp-transnational-repression-partys-effort-silence-and-coerce> (en anglais seulement).
- 21 DVILYANSKI, Mike. *Taking Action Against Hackers in China*, Meta, 24 mars 2021. <https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/> (en anglais seulement); Mise en accusation caviardée. *United States v. Gaobin*, 1:24-cr-00043, (E.D.N.Y.), déposée le 25 mars 2024. <https://www.justice.gov/usao-edny/media/1345131/dl> (en anglais seulement); BALAAM, Kristina, et coll. *BadBazaar: iOS and Android Surveillanceware by China's APT15 Used to Target Tibetans and Uyghurs*, Lookout, 22 janvier 2024. <https://www.lookout.com/threat-intelligence/article/badbazaar-surveillanceware-apt15> (en anglais seulement).
- 22 Congressional-Executive Commission on China. *The Human Rights Situation in Tibet and the International Response*, 116e Congrès, deuxième session, 30 septembre 2020. <https://www.congress.gov/event/116th-congress/joint-event/LC68497/text> (en anglais seulement); HOGUE, Marie-Josée, commissaire. *Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux : rapport initial*, Bureau du Conseil privé, 3 mai 2024. <https://publications.gc.ca/site/fra/9.935032/publication.html>; Amnesty Internationale. *Chine. Les étudiant-e-s chinois à l'étranger sont en butte au harcèlement et à la surveillance dans le cadre de la campagne de répression transnationale*, 13 mai 2024. <https://www.amnesty.org/fr/latest/news/2024/05/china-overseas-students-face-harassment-and-surveillance-in-campaign-of-transnational-repression/>.

- 23 CARY, Dakota, et Aleksandar MILENKOSKI. *Unmasking I-Soon I The Leak That Revealed China's Cyber Operations*, SentinelLabs, 21 février 2024. <https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/> (en anglais seulement); SEPPERD, Christian, et coll. *Leaked files from Chinese firm show vast international hacking effort*, The Washington Post, 22 février 2024. https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-ison (en anglais seulement).
- 24 Mise en accusation caviardée. *United States v. Gaobin*, 1:24-cr-00043, (E.D.N.Y.), déposée le 25 mars 2024. <https://www.justice.gov/usao-edny/media/1345131/dl> (en anglais seulement).
- 25 Center for Security and Emerging Technology. *Translation: Implementation Opinions of Seven Ministries Including the Ministry of Industry and Information Technology on Promoting the Innovative Development of Future Industries*, 12 février 2024. <https://cset.georgetown.edu/publication/future-industry-implementation-opinions/> (en anglais seulement).
- 26 Cybersecurity and Infrastructure Security Agency. *Opening Statement by CISA Director Jen Easterly*, 31 janvier 2024. <https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly> (en anglais seulement); Centre canadien pour la cybersécurité, *Cyberbulletin : Le Centre pour la cybersécurité invite les Canadiennes et Canadiens à s'informer et à se protéger contre les activités de cybermenace de la RPC*, 3 juin 2024. <https://www.cyber.gc.ca/fr/orientation/cyberbulletin-centre-cybersecurite-invite-canadiennes-canadiens-sinformer-se-protoger-contre-activites-cybermenace-rpc>.
- 27 Cybersecurity and Infrastructure Security Agency. *Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Alerte AA24-038A, 7 février 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a> (en anglais seulement); The Economist. *The new front in China's cyber campaign against America*, The Economist, 13 juin 2024. <https://www.economist.com/international/2024/06/13/the-new-front-in-chinas-cyber-campaign-against-america> (en anglais seulement).
- 28 Centre canadien pour la cybersécurité. *Cyberbulletin : Le Centre pour la cybersécurité invite les Canadiennes et Canadiens à s'informer et à se protéger contre les activités de cybermenace de la RPC*, 3 juin 2024. <https://www.cyber.gc.ca/fr/orientation/cyberbulletin-centre-cybersecurite-invite-canadiennes-canadiens-sinformer-se-protoger-contre-activites-cybermenace-rpc>.
- 29 United States Department of Justice. *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election*, 13 juillet 2018. <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election> (en anglais seulement); Microsoft Threat Intelligence Report. *Iran steps into US election 2024 with cyber-enabled influence operations*, 9 août 2024. <https://blogs.microsoft.com/on-the-issues/2024/08/iran-targeting-2024-us-election/> (en anglais seulement); United States Department of Justice. *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*, 4 septembre 2024. <https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence> (en anglais seulement); Centre canadien pour la cybersécurité. *Des auteures et auteurs de cybermenace de l'armée russe ciblent les infrastructures essentielles américaines et internationales*, 5 septembre 2024. <https://www.cyber.gc.ca/fr/nouvelles-evenements/auteurs-auteurs-cybermenace-armee-russe-ciblent-infrastructures-essentielles-americaaines-internationales>.
- 30 Centre canadien pour la cybersécurité. *Le CST exhorte la collectivité canadienne de la cybersécurité à être vigilante à l'occasion du deuxième anniversaire de l'invasion massive de l'Ukraine par la Russie*, 19 février 2024. <https://www.cyber.gc.ca/fr/nouvelles-evenements/cst-exhorte-collectivite-canadienne-cybersecurite-etre-vigilante-loccasion-deuxieme-anniversaire-linvasion-massive-lukraine-russie>.
- 31 BALMFORTH, Tom. *Exclusive: Russia hackers were inside Ukraine telecom giant for months*, Reuters, 5 janvier 2024. <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/> (en anglais seulement).
- 32 Centre canadien pour la cybersécurité. *Bulletin sur les cybermenaces : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie*, 14 juillet 2022. <https://www.cyber.gc.ca/fr/orientation/bulletin-cybermenaces-activites-cybermenace-liees-invasion-Ukraine-Russie>.
- 33 Centre canadien pour la cybersécurité. *Évaluation des cybermenaces nationales 2023-2024*, 28 octobre 2022. <https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024>.
- 34 Cybersecurity and Infrastructure Security Agency. *Cybersecurity Advisory: SVR Cyber Actors Adapt Tactics for Initial Cloud Access*, 26 février 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a> (en anglais seulement).

- 35 Cybersecurity and Infrastructure Security Agency. *Emergency Directives ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*, 2 avril 2024. <https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system> (en anglais seulement); MARTIN, Alexander. *Exclusive: Russian spies hacked UK government data and emails earlier this year*, The Record, 8 août 2024. <https://therecord.media/russia-hack-uk-government-home-office-microsoft> (en anglais seulement).
- 36 Microsoft. *Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*, 19 janvier 2024. <https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard> (en anglais seulement).
- 37 KEAST-BUTLER, Anne, directrice, GCHQ. *CYBERUK 2024: Anne Keast-Butler keynote speech*, 14 mai 2024. <https://www.ncsc.gov.uk/speech/cyberuk-2024-gchq-director-keynote-speech> (en anglais seulement).
- 38 TUNNEY, Catharine. *Trudeau shrugs off reports pro-Russia hackers brought down PMO website*, CBC News, 11 avril 2023. <https://www.cbc.ca/news/politics/cse-cyber-attack-ukrainian-visit-1.6806709> (en anglais seulement).
- 39 Centre canadien pour la cybersécurité. *Alerte – Risques de cyberactivités malveillantes contre les nations alliées de l'Ukraine*, 24 février 2023. <https://www.cyber.gc.ca/fr/alertes-avis/risques-cyberactivites-malveillantes-contre-nations-alliees-ukraine>; NAKASHIMA, Ellen. *Tex. Hack may be first disruption of U.S. water system by Russia*, The Washington Post, 17 avril 2024. <https://www.washingtonpost.com/politics/2024/04/17/tex-hack-may-be-first-disruption-us-water-system-by-russia/> (en anglais seulement); Cybersecurity and Infrastructure Security Agency. *Defending OT Operations Against Ongoing Pro-Russia Hactivist Activity*, 1er mai 2024. <https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hactivist-activity> (en anglais seulement).
- 40 United States Department of Treasury. *Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn*, 19 juillet 2024. <https://home.treasury.gov/news/press-releases/jy2473> (en anglais seulement).
- 41 Personnel de La Presse canadienne. *Quebec government says data not compromised after websites hit by cyberattack*, CTV News, 13 septembre 2023. <https://montreal.ctvnews.ca/quebec-government-sites-under-cyber-attack-1.6560005?cache=hhhufcdil> (en anglais seulement); ALLAN, Michelle. *Websites for PMO's office, NCC among those crashed by hackers*, CBC News, 15 avril 2023. <https://www.cbc.ca/news/canada/ottawa/websites-for-pmo-s-office-ncc-among-those-crashed-by-hackers-1.6810684> (en anglais seulement).
- 42 BARAM, Gil. *How the cyberwar between Iran and Israel has intensified*, The Washington Post, 25 juillet 2022. <https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war> (en anglais seulement); WROBEL, Sharon. *Cyberattacks by Iran, Hezbollah have tripled during the war, says Israel cyber czar*, The Times of Israel, 4 juillet 2024. <https://www.timesofisrael.com/cyberattacks-by-iran-hezbollah-have-tripled-during-the-war-says-israel-cyber-czar/> (en anglais seulement).
- 43 United States Department of the Treasury. *Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities*, 9 septembre 2022. <https://home.treasury.gov/news/press-releases/jy0941> (en anglais seulement); United States Department of the Treasury. *Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure*, 2 février 2024. <https://home.treasury.gov/news/press-releases/jy2072> (en anglais seulement).
- 44 Cybersecurity and Infrastructure Security Agency. *Exploitation of Unitronics PLCs used in Water and Wastewater Systems*, 28 novembre 2023. <https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems> (en anglais seulement); WALTER, Jim. *Iran-Backed Cyber Avengers Escalates Campaigns Against U.S. Critical Infrastructure*, Sentinel One, 30 novembre 2023. <https://www.sentinelone.com/blog/iran-backed-cyber-avengers-escalates-campaigns-against-u-s-critical-infrastructure/> (en anglais seulement).

- 45 Les données de la figure 5 sont tirées des sources suivantes : Microsoft Threat Intelligence. *Iran surges cyber-enabled influence operations in support of Hamas*, 26 février 2024. <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas> (en anglais seulement); Cybersecurity and Infrastructure Security Agency. *Exploitation of Unitronics PLCs used in Water and Wastewater Systems*, 28 novembre 2023. <https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems> (en anglais seulement); WALTER, Jim. *Iran-Backed Cyber Av3ngers Escalates Campaigns Against U.S. Critical Infrastructure*, Sentinel One, 30 novembre 2023. <https://www.sentinelone.com/blog/iran-backed-cyber-av3ngers-escalates-campaigns-against-u-s-critical-infrastructure/> (en anglais seulement); Cybersecurity and Infrastructure Security Agency. *Iranian State Actors Conduct Cyber Operations Against the Government of Albania*, 23 septembre 2022. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a> (en anglais seulement); The Federal Bureau of Investigations and the Cybersecurity and Infrastructure Security Agency. *Iranian State Actors Conduct Cyber Operations Against the Government of Albania*, 21 septembre 2022. <https://www.cisa.gov/sites/default/files/publications/aa22-264a-iranian-cyber-actors-conduct-cyber-operations-against-the-government-of-albania.pdf> (en anglais seulement); Affaires mondiales Canada. *Déclaration sur la cyberactivité malveillante de l'Iran portant atteinte à l'Albanie*, 22 septembre 2022. <https://www.canada.ca/fr/affaires-mondiales/nouvelles/2022/09/declaration-sur-la-cyberactivite-malveillante-de-liran-portant-atteinte-a-lalbanie.html>; Clearsky Cyber Security. *No Justice Wiper. Wiper attack on Albania by Iranian APT*, 4 janvier 2024. <https://www.clearskysec.com/wp-content/uploads/2024/01/No-Justice-Wiper.pdf> (en anglais seulement); ANTONIUK, Daryna. *Wiper malware found in analysis of Iran-linked attacks on Albanian institutions*, The Record, 8 janvier 2024. <https://therecord.media/albania-parliament-telecoms-airline-cyberattacks-wiper-malware> (en anglais seulement); Personnel de l'Associated Press. *Albanian authorities accuse Iranian-backed hackers of cyberattack on Institute of Statistics*, Associated Press News, 14 février 2024. <https://apnews.com/article/albania-iran-hackers-cyberattack-statistics-e80780e2d927394589c3d8903e36d066> (en anglais seulement); Microsoft Threat Intelligence. *Iran turning to cyber-enabled influence operations for greater effect*, 5 février 2023. <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-turning-to-cyber-enabled-influence-operations-for-greater-effect> (en anglais seulement); Personnel de l'Associated Press. *Hackers target Bahrain airport, news sites to mark uprising*, CTV News, 14 février 2023. <https://www.ctvnews.ca/hackers-target-bahrain-airport-news-sites-to-mark-uprising-1.6273145> (en anglais seulement).
- 46 Google Threat Analysis Group. *Iranian backed group steps up phishing campaigns against Israel, U.S.*, 14 août 2024. <https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/> (en anglais seulement); ROZMANN, Ofir, et coll. *Uncharmed: Untangling Iran's APT42 Operations*, Mandiant, 1er mai 2024. <https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations> (en anglais seulement); INSIKT Group. *Social Engineering Remains Key Tradecraft for Iranian APTs*, Recorded Future, 30 mars 2022. <https://www.recordedfuture.com/research/social-engineering-remains-key-tradecraft-for-iranian-apt> (en anglais seulement).
- 47 DARAGAH, Borzou. *Iran is using its cyber capabilities to kidnap its foes in the real world*, The Atlantic Council, 24 mai 2023. <https://www.atlanticcouncil.org/blogs/iransource/iran-cyber-warfare-kidnappings/> (en anglais seulement); United States Department of Justice. *One Iranian and Two Canadian Nationals Indicted in Murder-for-Hire Scheme*, 29 janvier 2024. <https://justice.gov/opa/pr/one-iranian-and-two-canadian-nationals-indicted-murder-hire-scheme> (en anglais seulement); United States Department of Justice. *Members of Iran's Islamic Revolutionary Guards Corps (IRGC) Charged with Plot to Murder the Former National Security Advisor*, 10 août 2022; AZIZI, Arash. *Iran's Deadly Message to Journalists Abroad*, The Atlantic, 12 avril 2024. <https://www.theatlantic.com/international/archive/2024/04/iran-journalism-west-violence/678038> (en anglais seulement); MILLER, Greg, Souad MEKHENNET et Cate BROWN. *Iran turns to Hells Angels and other criminal gangs to target critics*, The Washington Post, 12 septembre 2024. <https://www.washingtonpost.com/world/2024/09/12/iran-criminal-gangs-target-dissidents/> (en anglais seulement).
- 48 United States Department of the Treasury. *Treasury Designates Iranian Cyber Actors Targeting U.S. Companies and Government Agencies*, 23 avril 2024. <https://home.treasury.gov/news/press-releases/jy2292> (en anglais seulement).
- 49 United States Department of Justice. *North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Healthcare Providers*, 25 juillet 2024. <https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals> (en anglais seulement).
- 50 Cybersecurity and Infrastructure Security Agency. *Guidance on the North Korean Cyber Threat*, 23 juin 2020. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a> (en anglais seulement); LYGASS, Sean. *North Korean hackers extorted health care organizations to fund further cyberattacks, US and South Korea say*, CNN, 9 février 2023. <https://www.cnn.com/2023/02/09/politics/north-korea-cyber-health-care-ransom/index.html> (en anglais seulement).

- 51 O'NEILL, Alex. *Countering North Korean Cybercrime and Its Enablers*, Lawfare, 2 mai 2024. <https://www.lawfaremedia.org/article/countering-north-korean-cybercrime-and-its-enablers> (en anglais seulement).
- 52 PANDIT, Rajat. *Armed forces formulate new doctrine for cyberspace operations*, The Times of India, 18 juin 2024. <https://timesofindia.indiatimes.com/india/armed-forces-formulate-new-doctrine-for-cyberspace-operations/articleshow/111089679.cms> (en anglais seulement).
- 53 SRIVASTAVA, Mehul et Kaye WIGGINS. *India hunts for spyware that rivals controversial Pegasus system*, Financial Times, 31 mars 2023. <https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9> (en anglais seulement); ROBERTS, Jen, et coll. *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and its Threats to National Security and Human Rights*, DFRLab, 4 septembre 2024. <https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/> (en anglais seulement).
- 54 Bleeping Computer. *Ransomware as a Service and the Strange Economics of the Dark Web*, 27 mars 2024. <https://www.bleepingcomputer.com/news/security/ransomware-as-a-service-and-the-strange-economics-of-the-dark-web/> (en anglais seulement); Field Effect. *The rise of cybercrime-as-a-service*, 19 avril 2023. <https://fieldeffect.com/blog/cybercrime-as-a-service> (en anglais seulement); National Cyber Security Centre. *Ransomware, extortion and the cyber crime ecosystem*, 11 septembre 2023. https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_6 (en anglais seulement).
- 55 MARTIN, Alexander. *Ransomware ecosystem fragmenting under law enforcement pressure and distrust*, The Record, 23 juillet 2024. <https://therecord.media/ransomware-ecosystem-changing-under-law-enforcement-pressure-distrust> (en anglais seulement); Bleeping Computer. *Ransomware as a Service and the Strange Economics of the Dark Web*, 27 mars 2024. <https://www.bleepingcomputer.com/news/security/ransomware-as-a-service-and-the-strange-economics-of-the-dark-web/> (en anglais seulement); SHEA, Courtney. *Why Canada has so many cyberattacks—and why we're all at risk*, Macleans, 18 mars 2024. <https://macleans.ca/society/technology/cyberattacks-canada/> (en anglais seulement); National Cyber Security Centre. *Ransomware, extortion and the cyber crime ecosystem*, 11 septembre 2023. https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_6 (en anglais seulement).
- 56 Sophos. *Sophos 2023 Threat Report: Maturing Criminal Marketplaces Present New Challenges to Defenders*, 17 novembre 2023. <https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf> (en anglais seulement).
- 57 Intel471. *How Threat Actors Use Underground Marketplaces*, 22 septembre 2022. <https://intel471.com/blog/how-threat-actors-use-underground-marketplaces> (en anglais seulement).
- 58 Flare. *Top Cybercrime Forums to Monitor in 2023*, 16 mai 2023. <https://flare.io/learn/resources/blog/top-cybercrime-forums/> (en anglais seulement).
- 59 Kela. *Telegram: How a Messenger Turned into a Cybercrime Ecosystem by 2023*. https://www.kelacyber.com/wp-content/uploads/2024/01/KELA_Telegram_CEBIN_24.pdf (en anglais seulement).
- 60 MARTIN, Alexander. *Genesis Market, one of world's largest platforms for cyber fraud, seized by police*, The Record, 4 avril 2023. <https://therecord.media/genesis-market-takedown-cybercrime> (en anglais seulement).
- 61 United States Department of Justice. *Criminal Marketplace Disrupted in International Cyber Operation*, 5 avril 2023. <https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation> (en anglais seulement).
- 62 Centre canadien pour la cybersécurité. *Évaluation des menaces de base : Cybercriminalité*, 28 août 2023. <https://www.cyber.gc.ca/fr/orientation/evaluation-menaces-base-cybercriminalite>.
- 63 Gendarmerie royale du Canada. *Mois de la prévention de la fraude 2024 : Lutter contre la fraude à l'ère numérique*, 29 février 2024. <https://www.rcmp-grc.gc.ca/fr/nouvelles/2024/mois-prevention-fraude-2024-lutter-fraude-a-lere-numerique>.
- 64 IBM. *Qu'est-ce que la compromission d'e-mails professionnels (BEC)?*, <https://www.ibm.com/fr-fr/topics/business-email-compromise> (en anglais seulement).
- 65 Centre antifraude du Canada. *Rapport annuel 2022*. https://publications.gc.ca/collections/collection_2024/grc-rcmp/PS61-46-2022-fra.pdf; Gendarmerie royale du Canada. *Mois de la prévention de la fraude 2024 : Lutter contre la fraude à l'ère numérique*, 29 février 2024. <https://www.rcmp-grc.gc.ca/fr/nouvelles/2024/mois-prevention-fraude-2024-lutter-fraude-a-lere-numerique>.

- 66 Europol. *Internet Organized Crime Threat Assessment (IOCTA) 2024*, 26 juillet 2024. <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024> (en anglais seulement); Recorded Future. *2023 Annual Report*, 21 mars 2024. <https://go.recordedfuture.com/hubfs/reports/ta-2024-0321.pdf> (en anglais seulement).
- 67 Chainalysis. *Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline*, 7 février 2024. <https://www.chainalysis.com/blog/ransomware-2024/> (en anglais seulement); Cyber Threat Intelligence Integration Center. *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, 28 février 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf (en anglais seulement).
- 68 MARTIN, Alexander. *Ransomware ecosystem fragmenting under law enforcement pressure and distrust*, The Record, 23 juillet 2024. <https://therecord.media/ransomware-ecosystem-changing-under-law-enforcement-pressure-distrust> (en anglais seulement).
- 69 Cyber Threat Intelligence Integration Center. *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, 28 février 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf (en anglais seulement).
- 70 Chainalysis. *Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline*, 7 février 2024. <https://www.chainalysis.com/blog/ransomware-2024/> (en anglais seulement).
- 71 DOVE, Nathaniel. *Canadian firms paying 'significantly' more in ransomware attacks: data*, Global News, 7 décembre 2023. <http://www.globalnews.ca/news/10155151/companies-1-million-ransomware-attacks/> (en anglais seulement).
- 72 Chainalysis. *2024 Crypto Crime Mid-year Update Part 1: Cybercrime Climbs as Exchange Thieves and Ransomware Attackers Grow Bolder*, 15 août 2024. <https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/> (en anglais seulement); GRIEG, Jonathan. *Ransomware gangs rake in more than \$450 million in first half of 2024*, The Record, 15 août 2024. <https://therecord.media/ransomware-gangs-set-record-for-money-extorted> (en anglais seulement); PEARSON, Jordan. *Ransomware Is 'More Brutal' Than Ever in 2024*, Wired, 10 juin 2024. <https://www.wired.com/story/state-of-ransomware-2024/> (en anglais seulement).
- 73 ZAPATA, Karina. *It's time for companies to double down on cybersecurity measures as ransomware attacks rise, say experts*, CBC, 11 août 2023. <https://www.cbc.ca/news/canada/calgary/cybersecurity-measures-ransomware-attacks-1.6934486> (en anglais seulement).
- 74 Centre canadien pour la cybersécurité. *Le Centre de la sécurité des télécommunications et des partenaires internationaux publie un bulletin de cybersécurité sur le rançongiciel LockBit*. <https://www.cyber.gc.ca/fr/nouvelles-evenements/centre-securite-telecommunications-partenaires-internationaux-publie-bulletin-cybersecurite-rancongiel-lockbit>.
- 75 Centre canadien pour la cybersécurité. *Alerte - Rançongiciel ALPHV/BlackCat ciblant les industries canadiennes*, 25 juillet 2023. <https://www.cyber.gc.ca/fr/alertes-avis/rancongiel-alphvblackcat-ciblent-industries-canadiennes>.
- 76 Centre canadien pour la cybersécurité. *Profil : Rançongiciel CLOP / TA505*, 11 juillet 2023, <https://www.cyber.gc.ca/fr/orientation/profil-rancongiel-cl0p-ta505>; Sentinelle One. *What is Clop ransomware?* <https://www.sentinelone.com/anthology/clop/> (en anglais seulement).
- 77 Internet Crime Complaint Centre. *Joint Cybersecurity Advisory: #StopRansomware: Play Ransomware*, 18 décembre 2023. <https://www.ic3.gov/Media/News/2023/231218.pdf> (en anglais seulement).
- 78 Cybersecurity Infrastructure & Security Agency. *CISA and Partners Release Advisory on Black Basta Ransomware*, 10 mai 2024. <https://www.cisa.gov/news-events/alerts/2024/05/10/cisa-and-partners-release-advisory-black-basta-ransomware> (en anglais seulement).
- 79 La barre pour 2024 représente une estimation du nombre total d'incidents qui seront signalés au Centre pour la cybersécurité en fonction des signalements reçus au cours des six premiers mois de 2024. Étant donné que de nombreux incidents liés à des rançongiciels ne sont pas signalés, il est presque certain que le nombre réel de ces incidents au Canada est plus élevé que ce qui est représenté dans le graphique.
- 80 Chainalysis. *Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline*, 7 février 2024. <https://www.chainalysis.com/blog/ransomware-2024/> (en anglais seulement); MCLAUGHLIN, Jenna. *The rise in ransomware attacks this year may be related to Russia's war in Ukraine*, NPR, 13 juillet 2023. <https://www.npr.org/2023/07/13/1187573935/the-rise-in-ransomware-attacks-this-year-may-be-related-to-russias-war-in-ukrain> (en anglais seulement).

- 81 SADAYAPPAN Bavi, Zach RIDDLE, Jordan NUCE, Joshua SHILKO et Jeremy KENNELLY. *Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools*, Google Cloud, 3 juin 2024. <https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools> (en anglais seulement).
- 82 HISERODT, Laura. *Third-Party Breaches: Risk in the Supply Chain*, Resilience, 18 octobre 2023. <https://www.cyberresilience.com/threatonomics/third-party-breaches-risk-in-the-supply-chain/> (en anglais seulement).
- 83 Centre canadien pour la cybersécurité. *Profil : Rançongiciel CLOP / TA505*, 11 juillet 2023. <https://www.cyber.gc.ca/fr/orientation/profil-rancongiel-cl0p-ta505>.
- 84 Recorded Future. *2023 Annual Report*, 21 mars 2024. <https://go.recordedfuture.com/hubfs/reports/ta-2024-0321.pdf> (en anglais seulement).
- 85 Chainalysis. *Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline*, 7 février 2024. <https://www.chainalysis.com/blog/ransomware-2024/> (en anglais seulement); Recorded Future. *2023 Annual Report*, 21 mars 2024. <https://go.recordedfuture.com/hubfs/reports/ta-2024-0321.pdf> (en anglais seulement).
- 86 National Cyber Security Centre. *Ransomware, extortion and the cyber crime ecosystem*, 11 septembre 2023. https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_6 (en anglais seulement).
- 87 Arctic Wolf. *Ransomware-as-a-Service Will Continue to Grow in 2024*, 19 janvier 2024. <https://arcticwolf.com/resources/blog/ransomware-as-a-service-will-continue-to-grow-in-2024/> (en anglais seulement); Chainalysis. *Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline*, 7 février 2024. <https://www.chainalysis.com/blog/ransomware-2024/> (en anglais seulement); Mandiant. *Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools*, 3 juin 2024. <https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools>.
- 88 ALAMRI, Abdulrahman H. *Dragos Industrial Ransomware Analysis: Q4 2023*, Dragos, 25 janvier 2024. <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/> (en anglais seulement); Centre canadien pour la cybersécurité. *Évaluation des menaces de base : Cybercriminalité*, 28 août 2023. <https://www.cyber.gc.ca/fr/orientation/evaluation-menaces-base-cybercriminalite>; Centre canadien pour la cybersécurité. *Cybermenaces contre le secteur pétrolier et gazier du Canada*. <https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-secteur-petrolier-gazier-canada>.
- 89 MARTIN, Alexander. *Ransomware attacks leave small business owners feeling suicidal, report says*, The Record, 17 janvier 2024. <https://therecord.media/small-business-ransomware-attacks-mental-health-rusi-study> (en anglais seulement).
- 90 GREENBERG, Andy. *Change Healthcare Finally Admits it Paid Ransomware Hackers \$22 Million – and Still Faces a Patient Data Leak*, Wired, 22 avril 2024. <https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/> (en anglais seulement); DURBIN, Dee-ann. *Meat company JBS Foods confirms it paid US\$11M ransom in cyberattack*, Global News, 9 juin 2021. <https://globalnews.ca/news/7936930/jbs-foods-ransomware-attack-paid/> (en anglais seulement); WILKIE, Christina. *Colonial Pipeline paid \$5 million ransomware one day after cyberattack, CEO tells Senate*, CNBC, 9 juin 2021. <https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html> (en anglais seulement).
- 91 Chainalysis. *Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline*, 7 février 2024. <https://www.chainalysis.com/blog/ransomware-2024/> (en anglais seulement).
- 92 Centre canadien pour la cybersécurité. *Bulletin sur les cybermenaces : Les cybermenaces visant les technologies opérationnelles*, 16 décembre 2021. <http://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-operational-technology>.
- 93 Centre canadien pour la cybersécurité. *Évaluation des menaces de base : Cybercriminalité*, 28 août 2023. <https://www.cyber.gc.ca/fr/orientation/evaluation-menaces-base-cybercriminalite>.
- 94 DUHATSCHEK, Paula. *Suncor swaps out laptops after cybersecurity incident as energy sector takes stock of risks*, CBC, 6 juillet 2023. <https://www.cbc.ca/news/canada/calgary/suncor-cybersecurity-incident-energy-sector-1.6898118> (en anglais seulement); Suncor. *Update on Suncor Energy response to cybersecurity incident*, 6 juillet 2023. https://www.suncor.com/-/media/project/suncor/files/news-releases/2023/2023-07-06-nr-su-update-cybersecurity-incident-en.pdf?modified=20230706200434&_ga=2.177511533.959371021.1688674862-1934455315.1687893565 (en anglais seulement).
- 95 Centre canadien pour la cybersécurité. *Évaluation des menaces de base : Cybercriminalité*, 28 août 2023. <https://www.cyber.gc.ca/fr/orientation/evaluation-menaces-base-cybercriminalite>; SickKids. *SickKids lifts Code Grey with 80 per cent of priority systems restored*, 5 janvier 2023. <https://www.sickkids.ca/en/news/archive/2023/sickkids-lifts-code-grey-with-80-per-cent-of-priority-systems-restored/> (en anglais seulement).

- 96 Chatham-Kent Health Alliance. *Update on Cyber Attacks at Regional Hospitals*, 31 octobre 2023. <https://www.ckha.on.ca/update-on-cyber-attacks-at-regional-hospitals-2/> (en anglais seulement); MUSYJ, David. *CYBER ATTACK STATEMENT*, 3 avril 2024. https://windsor.bluelemonmedia.com/uploads/Common/News/Cyberattack_Statement_Apr_3_2024.pdf (en anglais seulement); GARTON, Rich. *Notorious ransomware group claims responsibility for local hospitals cyberattack*, CTV News, 3 novembre 2023. <https://windsor.ctvnews.ca/notorious-ransomware-group-claims-responsibility-for-local-hospitals-cyberattack-1.6630237> (en anglais seulement).
- 97 KULKARNI, Akshay. *London Drugs confirms it was victim of ransomware attack*, CBC News, 21 mai 2024. <https://www.cbc.ca/news/canada/british-columbia/london-drugs-ransomware-attack-1.7210754> (en anglais seulement); GATLAN, Sergiu. *LockBit says they stole data in London Drugs ransomware attack*, Bleeping Computer, 21 mai 2024. <https://www.bleepingcomputer.com/news/security/lockbit-says-they-stole-data-in-london-drugs-ransomware-attack/> (en anglais seulement).
- 98 Government of Nova Scotia. *Update on MOVEit Global Security Breach*, 6 juin 2023. <https://news.novascotia.ca/en/2023/06/06/update-moveit-global-security-breach> (en anglais seulement).
- 99 Ministère de la Défense nationale. *Mise à jour : Incident touchant les systèmes de Services globaux de relogement Brookfield (BGRS)*, 20 octobre 2023. <https://www.canada.ca/fr/ministere-defense-nationale/feuille-derable/defense/2023/10/mise-a-jour-incident-touchant-systems-services-globaux-de-relogement-brookfield.html>; HILT, Kailee. *As We Enter 2024, Cyberthreats to Canada Are Growing*, Centre for International Governance Innovation, 28 décembre 2023. <https://www.cigionline.org/articles/as-we-enter-2024-cyberthreats-to-canada-are-growing/> (en anglais seulement).
- 100 City of Hamilton. *City Confirms Cyber Incident is a Ransomware Attack*, 5 mars 2024. <https://www.hamilton.ca/city-council/news-notice/news-releases/city-confirms-cyber-incident-ransomware-attack> (en anglais seulement).
- 101 Cyber Threat Intelligence Integration Center. *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, 28 février 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf (en anglais seulement).
- 102 WHITTAKER, Zack. *How the ransomware attack at Change Healthcare went down: A timeline*, Tech Crunch, 17 août 2024. <https://techcrunch.com/2024/08/17/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/> (en anglais seulement).
- 103 BBC. *Hospitals cyber attack impacts 800 operations*, 14 juin 2024. <https://www.bbc.com/news/articles/cd11v377eywo> (en anglais seulement); TIDY, Joe. *Stolen test data and NHS numbers published by hospital hackers*, BBC, 21 juin 2024. <https://www.bbc.com/news/articles/c9ww90j9dj8o> (en anglais seulement).
- 104 Cyber Threat Intelligence Integration Center. *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, 28 février 2024. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf (en anglais seulement).
- 105 ALAMRI, Abdulrahman H. *Dragos Industrial Ransomware Analysis: Q4 2023*, Dragos, 25 janvier 2024. <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/> (en anglais seulement).
- 106 Chainalysis. *Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline*, 7 février 2024. <https://www.chainalysis.com/blog/ransomware-2024/> (en anglais seulement).
- 107 Chainalysis. *Examining the Impact of Ransomware Disruptions: Qakbot, LockBit, and BlackCat*, 6 mai 2024. <https://www.chainalysis.com/blog/ransomware-disruptions-impact/> (en anglais seulement).
- 108 Europol. *Internet Organized Crime Threat Assessment (IOCTA) 2024*, 26 juillet 2024. <https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> (en anglais seulement).
- 109 Bleeping Computer. *Ransomware as a Service and the Strange Economics of the Dark Web*, 27 mars 2024. <https://www.bleepingcomputer.com/news/security/ransomware-as-a-service-and-the-strange-economics-of-the-dark-web/> (en anglais seulement); National Cyber Security Centre. *Ransomware, extortion and the cyber crime ecosystem*, 11 septembre 2023. https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_6 (en anglais seulement).
- 110 Europol. *Internet Organized Crime Threat Assessment (IOCTA) 2024*, 26 juillet 2024. <https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> (en anglais seulement).

- 111 BURGESS, Matt et Lily HAY NEWMAN. *The Unrelenting Menace of the LockBit Ransomware Gang*, Wired, 24 janvier 2023. <https://www.wired.com/story/lockbit-ransomware-attacks/> (en anglais seulement); GATLAN, Sergiu. *FBI: ALPHV ransomware raked in \$300 million from over 1,000 victims*, Bleeping Computer, 19 décembre 2023. <https://www.bleepingcomputer.com/news/security/fbi-alphv-ransomware-raked-in-300-million-from-over-1-000-victims/> (en anglais seulement); United States Department of Justice. *U.S. Department of Justice Disrupts Hive Ransomware Variant*, 26 janvier 2023. <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant> (en anglais seulement).
- 112 United States Department of Justice. *U.S. Department of Justice Disrupts Hive Ransomware Variant*, 26 janvier 2023. <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant> (en anglais seulement).
- 113 United States Department of Justice. *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, 19 décembre 2023. <https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant> (en anglais seulement).
- 114 Europol. *Law enforcement disrupt world's biggest ransomware operation*, 20 février 2024. <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation> (en anglais seulement).
- 115 Europol. *Internet Organized Crime Threat Assessment (IOCTA) 2024*, 26 juillet 2024. <https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> (en anglais seulement).
- 116 Europol. *Internet Organized Crime Threat Assessment (IOCTA) 2024*, 26 juillet 2024. <https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> (en anglais seulement).; SCHWARTZ, Mathew J. *Ever More Toxic Ransomware Brands Breed Lone Wolf Operators*, BankInfoSecurity, 1er août 2024. <https://www.bankinfosecurity.com/blogs/ever-more-toxic-ransomware-brands-breed-lone-wolf-operators-p-3682> (en anglais seulement).
- 117 ALAMRI, Abdulrahman H. *Dragos Industrial Ransomware Analysis: Q4 2023*, Dragos, 25 janvier 2024. <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/> (en anglais seulement); CONSTANTIN, Lucian. *Emerging ransomware groups on the rise: Who they are, how they operate*, CSO, 24 mai 2024. <https://www.csoonline.com/article/2121702/emerging-ransomware-groups-on-the-rise-who-they-are-how-they-operate.html> (en anglais seulement);
- 118 PEARSON, Jordan. *Ransomware Is 'More Brutal' Than Ever in 2024*, Wired, 10 juin 2024. <https://www.wired.com/story/state-of-ransomware-2024/> (en anglais seulement); KAPKO, Matt. *Ransomware gangs incite fear in victims to fuel attacks*, Cybersecurity Dive, 21 mars 2023. <https://www.cybersecuritydive.com/news/ransomware-gangs-extortion-unit42/645544/> (en anglais seulement).
- 119 PEARSON, Jordan. *Ransomware Is 'More Brutal' Than Ever in 2024*, Wired, 10 juin 2024. <https://www.wired.com/story/state-of-ransomware-2024/> (en anglais seulement); Sophos. *Turning the screws: The pressure tactics of ransomware gangs*, 6 août 2024. <https://news.sophos.com/en-us/2024/08/06/turning-the-screws-the-pressure-tactics-of-ransomware-gangs/> (en anglais seulement).
- 120 Mandiant. *Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools*, 3 juin 2024. <https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools> (en anglais seulement); Sophos. *Turning the screws: The pressure tactics of ransomware gangs*, 6 août 2024. <https://news.sophos.com/en-us/2024/08/06/turning-the-screws-the-pressure-tactics-of-ransomware-gangs/> (en anglais seulement).
- 121 ALAMRI, Abdulrahman H. *Dragos Industrial Ransomware Analysis: Q4 2023*, Dragos, 25 janvier 2024. <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/> (en anglais seulement).
- 122 Federal Bureau of Investigation. *Private Industry Notification*, 27 septembre 2023. <https://www.ic3.gov/Media/News/2023/230928.pdf> (en anglais seulement).
- 123 SC Media. *Remote ransomware: What is and how to stop it*, 12 janvier 2024. <https://www.scmagazine.com/resource/remote-ransomware-what-is-and-how-to-stop-it> (en anglais seulement).
- 124 CULAFI, Alexander. *CISA: Akira ransomware extorted \$42M from 250+ victims*, TechTarget, 19 avril 2024. <https://www.techtarget.com/searchsecurity/news/366581522/CISA-Akira-ransomware-extorted-42M-from-250-plus-victims> (en anglais seulement); Recorded Future. *Ransomware Examples*. <https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-examples> (en anglais seulement); Trend Micro. *What is Ransomware?*. https://www.trendmicro.com/en_us/what-is/ransomware.html (en anglais seulement).

- 125 ThreatDown. *Threat Brief: Ransomware Gangs & Living Off the Land Attacks*, 1er novembre 2023. https://www.threatdown.com/wp-content/uploads/2024/05/TD_ThreatBrief_Ransomware_LOTL_Ebook_EN_11142023.pdf (en anglais seulement).
- 126 Sophos. *Sophos 2023 Threat Report: Maturing Criminal Marketplaces Present New Challenges to Defenders*, 17 novembre 2023. <https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf> (en anglais seulement).
- 127 SERGILE, Daniel. *The Evolving Threat of Ransomware – A Call to Action for Cybersecurity*, Palo Alto, 17 avril 2024. <http://www.paloaltonetworks.com/blog/2024/04/the-evolving-threat-of-ransomware/> (en anglais seulement).
- 128 WEISE, Karen. *In Race to Build A.I., Tech Plans a Big Plumbing Upgrade*, The New York Times, 27 avril 2024. <https://www.nytimes.com/2024/04/27/technology/ai-big-tech-spending.html> (en anglais seulement); JACOBS, Jordan. *Canadian AI Sovereign Compute Strategy*, Radical Ventures, 7 avril 2024. <https://radical.vc/canadian-ai-sovereign-compute-strategy/> (en anglais seulement); PATEL, Dylan, et coll. *AI Datacenter Energy Dilemma – Race for AI Datacenter Space*, Semianalysis, 13 mars 2024. <https://www.semianalysis.com/p/ai-datacenter-energy-dilemma-race> (en anglais seulement); Brookfield Renewable Partners. *Brookfield and Microsoft Collaborating to Deliver Over 10.5 GW of New Renewable Power Capacity Globally*, 1er mai 2024. <https://bep.brookfield.com/press-releases/bep/brookfield-and-microsoft-collaborating-deliver-over-105-gw-new-renewable-power> (en anglais seulement); METZ, Cade. *A Hacker Stole OpenAI Secrets, Raising Fears that China Could, Too*, The New York Times, 4 juillet 2024. <https://www.nytimes.com/2024/07/04/technology/openai-hack.html?smid=nytcore-ios-share&referringSource=articleShare> (en anglais seulement); MILLER, Chris. *The global chip war could turn into a cloud war*, Financial Times, 30 juillet 2024. <https://www.ft.com/content/202c3240-fa20-4081-a2a7-8470b7f12110> (en anglais seulement); CTIA. *2024 Annual Survey Highlights*, 10 septembre 2024. <https://www.ctia.org/news/2024-annual-survey-highlights> (en anglais seulement).
- 129 KrebsonSecurity. *3CX Breach Was a Double Supply Chain Compromise*, 20 avril 2023. <https://krebsonsecurity.com/2023/04/3cx-breach-was-a-double-supply-chain-compromise/> (en anglais seulement).
- 130 Mandiant. *M-Trends 2024 Special Report*, <https://cloud.google.com/security/resources/m-trends> (en anglais seulement); Mandiant. *Analysis of Time-to-Exploit Trends: 2021-2022*, 28 septembre 2023. <https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2021-2022/> (en anglais seulement).
- 131 National Institute of Standards and Technology. *National Vulnerability Database*. <https://nvd.nist.gov/vuln/data-feeds> (en anglaise seulement).
- 132 SCHMIDT, Eric. *AI, Great Power Competition & National Security*, Daedalus (2022) 151 (2) : 288-298. <https://direct.mit.edu/daed/article/151/2/288/110603/AI-Great-Power-Competition-amp-National-Security> (en anglais seulement).
- 133 METZ, Rachel. *OpenAI Scale Ranks Progress Toward 'Human-Level' Problem Solving*, Bloomberg, 11 juillet 2024. <https://www.bloomberg.com/news/articles/2024-07-11/openai-sets-levels-to-track-progress-toward-superintelligent-ai> (en anglais seulement); HOLMES, Aaron. *To Unlock AI Spending, Microsoft, OpenAI and Google Prep 'Agents'*, The Information, 18 avril 2024. <https://www.theinformation.com/articles/to-unlock-ai-spending-microsoft-openai-and-google-prep-agents> (en anglais seulement); METZ, Cade. *OpenAI Unveils New ChatGPT That Can Reason Through Math and Science*, The New York Times, 12 septembre 2024. <https://www.nytimes.com/2024/09/12/technology/openai-chatgpt-math.html> (en anglais seulement).
- 134 Responsible AI Collaborative. *AI Incident Database*. <https://incidentdatabase.ai/> (en anglais seulement). Les annotations additionnelles d'incidents dans la base de données ont été ajoutées par le personnel du Centre canadien pour la cybersécurité.
- 135 FBI. *FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence*, 8 mai 2024. <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence> (en anglais seulement); Check Point Team. *Generative AI is the Pride of Cybercrime Services*, 1er février 2024. <https://blog.checkpoint.com/research/generative-ai-is-the-pride-of-cybercrime-services/> (en anglais seulement); CIANCAGLINI, Vincenzo, et David SANCHO. *Back to the Hype. An update on How Cybercriminals Are Using GenAI*, Trend Micro, 8 mai 2024. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genai> (en anglais seulement).

- 136** Cybersecurity and Infrastructure Security Agency. *NSA, FBI, and CISA Release Cybersecurity Information Sheet on Deepfake Threats*, 12 septembre 2023. <https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats> (en anglais seulement); CHEN, Heather, et Kathleen MAGRAMO. *Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'*, CNN, 4 février 2024. <https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html> (en anglais seulement); BURGESS, Matt. *The Real-Time Deepfake Romance Scams Have Arrived*, Wired, 18 avril 2024. <https://www.wired.com/story/yahoo-boys-real-time-deepfake-scams/> (en anglais seulement); EDWARDS, Benj. *Deep-Live-Cam goes viral, allowing anyone to become a digital doppelganger*, arsTechnica, 13 août 2024. <https://arstechnica.com/information-technology/2024/08/new-ai-tool-enables-real-time-face-swapping-on-webcams-raising-fraud-concerns/> (en anglais seulement).
- 137** DE ANGELO, Dena. *The Dark Side of AI in Cybersecurity – AI-Generated Malware*, Paloalto Networks, 15 mai 2024. <https://www.paloaltonetworks.com/blog/2024/05/ai-generated-malware/> (en anglais seulement); MATZ, S.C., et coll. *The potential of generative AI for personalized persuasion at scale*, Sci Rep 14, 4692 (2024). <https://www.nature.com/articles/s41598-024-53755-0> (en anglais seulement).
- 138** Meta. *Adversarial Threats*, First Quarter, mai 2024. <https://transparency.meta.com/metasecurity/threat-reporting> (en anglais seulement); OpenAI. *AI and Covert Influence Operations: Latest Trends*, mai 2024. <https://openai.com/index/disrupting-deceptive-uses-of-ai-by-covert-influence-operations/> (en anglais seulement); STONE, Jeff, et Daniel ZUIDIJK. *Russian Bots Use Fake Tom Cruise for Olympic Disinformation*, Bloomberg, 3 juin 2024. <https://www.bloomberg.com/news/articles/2024-06-03/russian-bots-use-fake-tom-cruise-for-olympic-disinformation> (en anglais seulement); DUFOUR, Nicholas, et coll. *AMMEBA: A Large-Scale Survey and Dataset of Media-Based Misinformation In-The-Wild*, 19 mai 2024. <https://arxiv.org/abs/2405.11697> (en anglais seulement); FRENKEL, Sheera. *Israel Secretly Targets U.S. Lawmakers With Influence Campaign on Gaza War*, The New York Times, 5 juin 2024. <https://www.nytimes.com/2024/06/05/technology/israel-campaign-gaza-social-media.html> (en anglais seulement); BENJAKOB, Omer. *Israel Secretly Targeted American Lawmakers with Gaza War Influence Campaign*, Haaretz, 5 juin 2024. <https://www.haaretz.com/israel-news/security-aviation/2024-06-05/ty-article-magazine/.premium/israel-secretly-targeted-american-lawmakers-with-gaza-war-influence-campaign/0000018f-e7c8-d11f-a5cf-e7cb62af0000> (en anglais seulement); LEVITZ, Stephanie, Alex BALLINGALL et Mark RAMZY. *Trudeau government raises concerns with Israel about 'Islamophobic' misinformation campaign that is 'targeting Canadians'*, The Toronto Star, 11 juin 2024. https://www.thestar.com/politics/federal/trudeau-government-raises-concerns-with-israel-about-islamophobic-misinformation-campaign-that-is-targeting-canadians/article_3c854d48-274f-11ef-865d-a3f2559953b0.html (en anglais seulement); DFRLab. *Inauthentic campaign amplifying Islamophobic content targeting Canadians*, 28 mars 2024. <https://dfrlab.org/2024/03/28/inauthentic-campaign-amplifying-islamophobic-content-targeting-canadians/> (en anglais seulement); U.S. Department of Justice. *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*, 4 septembre 2024. <https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence> (en anglais seulement).
- 139** Centre canadien pour la cybersécurité. *Une organisation médiatique parrainée par la Russie tire avantage du logiciel avancé d'IA « Meliorator » à des fins d'influence étrangère malveillante*, 9 juillet 2024. <https://www.cyber.gc.ca/fr/nouvelles-evenements/organisation-mediatique-parrainee-russie-tire-avantage-logiciel-avance-dia-meliorator-fins-dinfluence-etrangere-malveillante>.
- 140** Centre canadien pour la cybersécurité. *La menace posée par les générateurs de texte basés sur des modèles de langage de grande taille*, 17 janvier 2024. <https://www.cyber.gc.ca/fr/orientation/menace-posee-generateurs-texte-bases-modeles-langage-grande-taille>; Centre canadien pour la cybersécurité. *Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023*, 6 décembre 2023. <https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-processus-democratique-canada-mise-jour-2023>; Affaires mondiales Canada. *Le recours de la Russie à la désinformation et à la manipulation de l'information*, 28 février 2024. https://www.international.gc.ca/world-monde/issues_developpement-enjeux_developpement/response_conflict-reponse_conflits/crisis-crisis/ukraine-disinfo-desinfo.aspx?lang=fra; VOLZ, Dustin. *China is Targeting U.S. Voters and Taiwan with AI-Powered Disinformation*, The Wall Street Journal, 5 avril 2024. <https://www.wsj.com/politics/national-security/china-is-targeting-u-s-voters-and-taiwan-with-ai-powered-disinformation-34f59e21> (en anglais seulement).

- 141 VICIC, Jelena, et Richard HARKNETT. *The mechanisms of cyber-enabled information campaigning*, Binding Hook, 21 juin 2024. <https://bindinghook.com/articles-binding-edge/the-mechanisms-of-cyber-enabled-information-campaigning/> (en anglais seulement); ZADROZNY, Brandy. *Disinformation poses an unprecedented threat in 2024 – and the U.S. is less ready than ever*, NBC News, 18 janvier 2024. <https://www.nbcnews.com/tech/misinformation/disinformation-unprecedented-threat-2024-election-rcna134290> (en anglais seulement); BELOGOLOVA, Olga, Lee FOSTER, Thomas RID et Gavin WILDE. *Don't Hype the Disinformation Threat*, Foreign Affairs, 3 mai 2024. <https://www.foreignaffairs.com/russian-federation/dont-hype-disinformation-threat> (en anglais seulement); GOLDSTEIN, Josh A., et Renée DIRESTA. *Propagandists are using AI too – and companies need to be open about it*, MIT Technology Review, 8 juin 2024. <https://www.technologyreview.com/2024/06/08/1093356/propagandists-are-using-ai-too-and-companies-need-to-be-open-about-it/> (en anglais seulement); ZAKRZEWSKI, Cat, et Joseph MENN. *Russia and China Pounce on Trump Really Shooting to Undermine U.S.*, The Washington Post, 17 juillet 2024. <https://www.washingtonpost.com/technology/2024/07/17/trump-shooting-china-russia-disinformation-campaign/> (en anglais seulement); HONEYCOMBE-FOSTER, Matt, et Andrew MCDONALD. *UK probes whether 'state actors' stoked far-right riots*, Politico, 5 août 2024. <https://www.politico.eu/article/uk-probes-whether-state-actors-stoked-far-right-riots/> (en anglais seulement); BEDINGFIELD, Will. *Generative AI is Playing a Surprising Role in Israel-Hamas Disinformation*, Wired, 30 octobre 2023. <https://www.wired.com/story/israel-hamas-war-generative-artificial-intelligence-disinformation/> (en anglais seulement); ROSS SORKIN, Andrew, et coll. *An A.I.-Generated Spoof Rattles the Markets*, The New York Times, 23 mai 2023. <https://www.nytimes.com/2023/05/23/business/ai-picture-stockmarket.html> (en anglais seulement).
- 142 BERGER, Eric. *Deluge of 'pink slime' websites threaten to drown out truth with fake news in US election*, The Guardian, 20 juin 2024. <https://www.theguardian.com/us-news/article/2024/jun/20/fake-news-websites-us-election> (en anglais seulement); PATTERSON, Dan. *Black Hat 2024: Foreign Influence Operations Evolve as Narrative Attacks Become Sophisticated*, Blackbird.AI RAV3N Blog, 7 août 2024. <https://blackbird.ai/blog/foreign-influence-operations-evolve-as-narrative-attacks-grow-more-sophisticated/> (en anglais seulement); MYERS, Steven Lee, Tiffany HSU et Farnaz FASSIHI. *Iran Emerges as a Top Disinformation Threat in U.S. Presidential Race*, The New York Times, 4 septembre 2024. <https://www.nytimes.com/2024/09/04/business/media/iran-disinformation-us-presidential-race.html> (en anglais seulement).
- 143 SCHARRE, Paul. *Four Battlegrounds. Power in the Age of Artificial Intelligence*, (New York: W.W. Norton & Company, Inc., 2023); *UAE's Edge Group and G42 get into natural language processing*, Intelligence Online, 22 mars 2023. <https://www.intelligenceonline.com/surveillance--interception/2023/03/22/uae-s-edge-group-and-g42-get-into-natural-language-processing.109926405-art> (en anglais seulement); Palantir Technologies Inc. *Form 10-K Annual Report for the fiscal year ended December 31, 2023*. <https://www.sec.gov/ix?doc=/Archives/edgar/data/1321655/000132165524000022/pltr-20231231.htm> (en anglais seulement).
- 144 Mandiant. *M-Trends 2024 Special Report*, <https://cloud.google.com/security/resources/m-trends?hl=en> (en anglais seulement); Cisco Talos. *ArcaneDoor – New espionage-focused campaign found targeting perimeter network devices*, 24 avril 2024. <https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/> (en anglais seulement); GREENBERG, Andy. *Russia's New Cyberwarfare in Ukraine is Fast, Dirty, and Relentless*, 10 novembre 2022. <https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/> (en anglais seulement).
- 145 Centre canadien pour la cybersécurité. *Cyberactivité touchant les réseaux privés virtuels Cisco ASA*, 24 avril 2024. <https://www.cyber.gc.ca/fr/nouvelles-evenements/cyberactivite-touchant-reseaux-privés-virtuels-cisco-asa>.
- 146 Centre canadien pour la cybersécurité. *Bulletin conjoint sur des auteurs de menace parrainés par la RPC compromettant les infrastructures essentielles américaines pour établir un accès permanent, et conseils pour identifier et atténuer les attaques hors sol*, 7 février 2024. <https://www.cyber.gc.ca/fr/nouvelles-evenements/bulletin-conjoint-auteurs-menace-parrainees-rpc-compromettant-infrastructures-essentielles-americaaines-etablir-acces-permanent-conseils-identifier-attenuer-attaques-hors-sol>; Australian Cyber Security Centre. *Identifying and Mitigating Living Off the Land Techniques*, 8 février 2024. <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/identifying-and-mitigating-living-off-the-land-techniques> (en anglais seulement).
- 147 Centre canadien pour la cybersécurité. *Cyberbulletin : Le Centre pour la cybersécurité invite les Canadiennes et Canadiens à s'informer et à se protéger contre les activités de cybermenace de la RPC*, 3 juin 2024. <https://www.cyber.gc.ca/fr/orientation/cyberbulletin-centre-cybersecurite-invite-canadiennes-canadiens-sinformer-se-proteger-contre-activites-cybermenace-rpc>.
- 148 Cybersecurity and Infrastructure Agency. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, 7 février 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a> (en anglais seulement); RONCONE, Gabby, et coll. *APT44: Unearthing Sandworm*, Mandiant, 17 avril 2024. <https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm> (en anglais seulement).

- 149 PROSKA, Ken, et coll. *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*, Mandiant, 9 novembre 2023. <https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/> (en anglais seulement); GREENBERG, Andy. *Sandworm Hackers Caused Another Blackout in Ukraine – During a Missile Strike*, Wired, 9 novembre 2023. <https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/> (en anglais seulement).
- 150 Mandiant. *M-Trends 2024 Special Report*, <https://cloud.google.com/security/resources/m-trends?hl=en> (en anglais seulement).
- 151 The President's National Security Telecommunications Advisory Committee. *NSTAC Report to the President. Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*, 26 septembre 2023. <https://www.cisa.gov/resources-tools/groups/presidents-national-security-telecommunications-advisory-committee/presidents-nstac-publications> (en anglais seulement).
- 152 United States Department of Justice. *Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU)*, 15 février 2024. <https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian> (en anglais seulement); Centre canadien pour la cybersécurité. *Cyberbulletin : Le Centre pour la cybersécurité invite les Canadiennes et Canadiens à s'informer et à se protéger contre les activités de cybermenace de la RPC*, 3 juin 2024. <https://www.cyber.gc.ca/fr/orientation/cyberbulletin-centre-cybersecurite-invite-canadiennes-canadiens-sinformer-se-protoger-contre-activites-cybermenace-rpc>.
- 153 GREENBERG, Andy. *Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities*, Wired, 17 avril 2024. <https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/> (en anglais seulement); United States Department of the Treasury. *Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn*, 19 juillet 2024. <https://home.treasury.gov/news/press-releases/jy2473> (en anglais seulement); National Cyber Security Centre. *Heightened threat of state-aligned groups against western critical national infrastructure*, 1er mai 2024. <https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups> (en anglais seulement); Cybersecurity and Infrastructure Security Agency. *Defending OT Operations Against Ongoing Pro-Russia Hactivist Activity*, 1er mai 2024. <https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hactivist-activity> (en anglais seulement); VIGNATI, Mauro. *Civilian hackers blur the lines of modern conflict*, Binding Hook, 13 décembre 2023. <https://bindinghook.com/articles-hooked-on-trends/civilian-hackers-blur-the-lines-of-modern-conflict/> (en anglais seulement).
- 154 KAPPELLMANN ZAFRA, Daniel, et coll. *Global Revival of Hacktivism Requires Increased Vigilance from Defenders*, Mandiant, 27 juin 2024. <https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism> (en anglais seulement); IWASAWA, Akinobu. *Israel-Hamas war draws Russian, Indian 'hacktivists' into shadow conflict*, Nikkei Asia, 7 octobre 2023. <https://asia.nikkei.com/Politics/Middle-East-crisis/Israel-Hamas-war-draws-Russian-Indian-hacktivism-into-shadow-conflict> (en anglais seulement); Centre canadien pour la cybersécurité. *Alerte – Risques de cyberactivités malveillantes contre les nations alliées de l'Ukraine*, 24 février 2023. <https://www.cyber.gc.ca/fr/alertes-avis/risques-cyberactivites-malveillantes-contre-nations-alliees-ukraine>; Centre canadien pour la cybersécurité. *Alerte – Campagne d'attaques par déni de service distribué ciblant de multiples secteurs canadiens*, 15 septembre 2023. <https://www.cyber.gc.ca/fr/alertes-avis/campagne-dattaques-deni-service-distribue-ciblant-multiples-secteurs-canadiens>.
- 155 ROBERTSON, Dylan. *Cyberattacks hit military, Parliament websites as India-based group targets Canada*, CBC News, 28 septembre 2023. <https://www.cbc.ca/news/politics/cyberattacks-parliament-india-1.6981399> (en anglais seulement).
- 156 Radware. *Hacktivism Unveiled, April 2023 Insights Into the Footprints of Hacktivists*, 21 avril 2023. <https://www.radware.com/security/threat-advisories-and-attack-reports/hacktivism-unveiled-april-2023/> (en anglais seulement).
- 157 SCHMIDT, Eric. *AI, Great Power Competition & National Security*, Daedalus (2022) 151 (2) : 288-298. <https://direct.mit.edu/daed/article/151/2/288/110603/AI-Great-Power-Competition-amp-National-Security> (en anglais seulement); BRENNAN, Peter, et Chris HUDGINS. *Market-leading US companies consolidate power in era of 'superstar' firms*, S&P Global, 17 janvier 2023. <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/market-leading-us-companies-consolidate-power-in-era-of-superstar-firms-73773141> (en anglais seulement).

- 158** LIN, Belle. *CDK Global Hack Shows Risk of One Software Vendor Dominating an Industry*, Wall Street Journal, 29 juin 2024. <https://www.wsj.com/articles/cdk-global-hack-shows-risk-of-one-software-vendor-dominating-an-industry-5156420d> (en anglais seulement); BENRATH, Bastian. *AI Risks to Financial Stability Are Already a Central Bank Worry*, Bloomberg, 7 mai 2024; BAGLEY, Drew. *Achieving Ecosystem-level Cybersecurity: A U.S. Policy Perspective*, CrowdStrike Blog, 11 juin 2024. <https://www.crowdstrike.com/blog/next-steps-for-ecosystem-level-cybersecurity/> (en anglais seulement); MANFRA, Jeanette, et Charley SNYDER. *CSRB report highlights the need for new approaches to securing the public sector*, Google, 20 mai 2024. <https://blog.google/technology/safety-security/csrb-report-google-recommendations/> (en anglais seulement); Bureau du surintendant des institutions financières Canada. *Ligne directrice sur la gestion du risque lié aux tiers*, <https://www.osfi-bsif.gc.ca/fr/consignes/repertoire-consignes/ligne-directrice-sur-gestion-du-risque-lie-tiers> (en anglais seulement).
- 159** ZUO, Tianjiu, Justin SHERMAN, Maia HAMIN et Stewart SCOTT. *Critical Infrastructure and the Cloud: Policy for Emerging Risk*, DFRLab, 10 juillet 2023. <https://dfrlab.org/2023/07/10/critical-infrastructure-and-the-cloud-policy-for-emerging-risk/> (en anglais seulement); Microsoft Corporation. *Form 10-Q for the Quarterly period ended December 31, 2023*. https://www.sec.gov/Archives/edgar/data/789019/000095017024008814/msft-20231231.htm#item_1a_risk_factors (en anglais seulement); Cybersecurity and Infrastructure Security Agency. *SVR Cyber Actors Adapt Tactics for Initial Cloud Access*, 26 février 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a> (en anglais seulement).
- 160** Microsoft Threat Intelligence. *Midnight Blizzard: Guidance for responders on nation-state attack*, 25 janvier 2024. <https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/> (en anglais seulement); Microsoft Corporation. *Form 10-K For the Fiscal Year Ended June 30, 2023*. <https://microsoft.gcs-web.com/static-files/e2931fdb-9823-4130-b2a8-f6b8db0b15a9> (en anglais seulement); Alphabet Inc. *Form 10-K for the Fiscal Year Ended December 31, 2023*. <https://www.sec.gov/Archives/edgar/data/1652044/000165204424000022/goog-20231231.htm> (en anglais seulement); RICHTER, Felix. *Amazon Maintains Cloud Lead as Microsoft Edges Closer*, Statista, 2 mai 2024. <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/> (en anglais seulement).
- 161** GELLER, Eric. *The US Government Has a Microsoft Problem*, Wired, 15 avril 2024. <https://www.wired.com/story/the-us-government-has-a-microsoft-problem/> (en anglais seulement); Cybersecurity and Infrastructure Security Agency. *Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*, 2 avril 2024. <https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system> (en anglais seulement).
- 162** Cyber Safety Review Board. *Review of the Summer 2023 Microsoft Exchange Online Intrusion*, 20 mars 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf (en anglais seulement); SUJAY VAILSHERY, Lionel. *Market share of major office productivity software worldwide in 2024*, Statista, 9 février 2024. <https://www.statista.com/statistics/983299/worldwide-market-share-of-office-productivity-software/> (en anglais seulement); UnitedHealth Group Incorporated. *Form 8-K (Amendment No. 1)*, 21 février 2024, <https://www.sec.gov/ix?doc=/Archives/edgar/data/0000731766/000073176624000085/unh-20240221.htm> (en anglais seulement); LIN, Belle. *CDK Global Hack Shows Risk of One Software Vendor Dominating an Industry*, Wall Street Journal, 29 juin 2024. <https://www.wsj.com/articles/cdk-global-hack-shows-risk-of-one-software-vendor-dominating-an-industry-5156420d> (en anglais seulement); GREIG, Jonathan. *Multiple car dealers report disruptions to SEC due to cyberattack on software company*, The Record, 24 juin 2024. <https://therecord.media/car-dealerships-reports-sec-cdk-software-ransomware> (en anglais seulement); Brookfield Business Partners. *Corporate Profile*, février 2024. <https://bbu.brookfield.com/sites/bbu-brookfield-ir/files/2024-02/bbu-q4-2023-corporate-profile-feb-6.pdf> (en anglais seulement); AutoCanada. *AUTOCANADA PROVIDES UPDATE ON CDK CYBER SECURITY INCIDENT*, 4 juillet 2024. <https://investors.autocan.ca/2024/07/autocanada-provides-update-on-cdk-cyber-security-incident/> (en anglais seulement).
- 163** GEER, Dan, Eric JARDINE et Eireann LEVERETT. *On market concentration and cybersecurity risk*, Journal of Cyber Policy, (2020), 5:1, 9-29. <https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1728355> (en anglais seulement).
- 164** Cyber Safety Review Board. *Review of the Summer 2023 Microsoft Exchange Online Intrusion*, 20 mars 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf (en anglais seulement).
- 165** SCHWARTZ, Matthew. *Microsoft Azure Cloud Service Fails to Withstand DDoS Attack*, Gov Info Security, 31 juillet 2024. <https://www.govinfosecurity.com/microsoft-azure-cloud-service-fails-to-withstand-ddos-attack-a-25893> (en anglais seulement).
- 166** Microsoft. *Mitigation Statement – Azure Front Door – Issues accessing a subset of Microsoft services*, ID de suivi : KTY1-HW8, 30 juillet 2024. <https://azure.status.microsoft.fr-fr/status/history/> (en anglais seulement); KOVACS, Eduard. *Microsoft Says Azure Outage Caused by DDoS Attack Response*, SecurityWeek, 31 juillet 2024. <https://www.securityweek.com/microsoft-says-azure-outage-caused-by-ddos-attack-response/> (en anglais seulement).

- 167 United States Department of Defence. *Deputy Secretary of Defence Kathleen Hicks Keynote Address: 'The Urgency to Innovate' (As Delivered)*, 28 août 2023. <https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/> (en anglais seulement); ZEGART, Amy B. *American Spy Agencies are Struggling in the Age of Data*, Wired, 2 février 2022. <https://www.wired.com/story/spies-algorithms-artificial-intelligence-cybersecurity-data/> (en anglais seulement); KURTH CRONIN, Audrey. *How Private Tech Companies are Reshaping Great Power Competition*, The Kissinger Center Papers, août 2023. <https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition> (en anglais seulement); United States Space Force. *U.S. Space Force Commercial Space Strategy: Accelerating the Purposeful Pursuit of Hybrid Space Architectures*, 8 avril 2024. <https://www.spaceforce.mil/News/Article-Display/Article/3736616/ussf-releases-commercial-space-strategy-to-increase-competitive-advantage/> (en anglais seulement); HOROWITZ, Jonathan. *One click from Conflict: Some Legal Considerations Related to Technology Companies Providing Digital Services in Situations of Armed Conflict*, Chicago Journal of International Law, Vol. 24, No. 2, hiver 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4470988 (en anglais seulement).
- 168 National Counterintelligence and Security Center. *Safeguarding the US Space Industry*, 18 août 2023. <https://www.dni.gov/index.php/ncsc-features/2762-safeguarding-our-future> (en anglais seulement); Palantir Technologies Inc. *Form 10-K Annual Report for the fiscal year ended December 31, 2023*. <https://www.sec.gov/ix?doc=/Archives/edgar/data/1321655/000132165524000022/pltr-20231231.htm> (en anglais seulement).
- 169 Reuters. *Russia warns West: We can target your commercial satellites*, 27 octobre 2022. <https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27/> (en anglais seulement); MOZUR, Paul, et Adam SATARIANO. *Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service*, The New York Times, 24 mai 2024. <https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html> (en anglais seulement).
- 170 Affaires mondiales Canada. *Déclaration sur les cyberactivités malveillantes de la Russie qui touchent l'Europe et l'Ukraine*, 10 mai 2022. <https://www.canada.ca/fr/affaires-mondiales/nouvelles/2022/05/declaration-sur-les-cyberactivites-malveillantes-de-la-russie-qui-touchent-leurope-et-lukraine.html>; MOZUR, Paul, et Adam SATARIANO. *Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service*, The New York Times, 24 mai 2024. <https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html> (en anglais seulement).
- 171 FLEMING, Sam, Demetri SEVASTOPULO et Clair JONES. *How national security has transformed economic policy*, Financial Times, 4 septembre 2024. <https://www.ft.com/content/6068310d-4e01-42df-8b10-ef6952804604> (en anglais seulement); DOSHI, Rush. *The Long Game: China's Grand Strategy to Displace American Order*, (New York: Oxford University Press, 2021) (en anglais seulement); HUBER, Elias X. *Technology Controls to Contain China's Quantum Ambitions Are Here*, Lawfare, 22 août 2024. <https://www.lawfaremedia.org/article/technology-controls-to-contain-china-s-quantum-ambitions-are-here> (en anglais seulement).
- 172 KHANNA, Parag. *The Coming Entropy of Our World Order*, NOEMA, 7 mai 2024. <https://www.noemamag.com/the-coming-entropy-of-our-world-order/> (en anglais seulement).
- 173 <https://www.cyber.gc.ca/fr/orientation>
- 174 <https://www.cyber.gc.ca/fr/objectifs-relatifs-letat-preparation-matiere-cybersecurite/boite-outils-objectifs-relatifs-letat-preparation-matiere-cybersecurite-intersectoriels>