ISSN 2816-9204

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Évaluation des **cybermenaces** nationales

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

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

ISSN 2816-9204

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 (CST), le Centre pour la cybersécurité est la source unifiée de conseils, d'avis, de services et de soutien spécialisés en matière de cybersécurité pour les Canadiens et les organisations canadiennes.

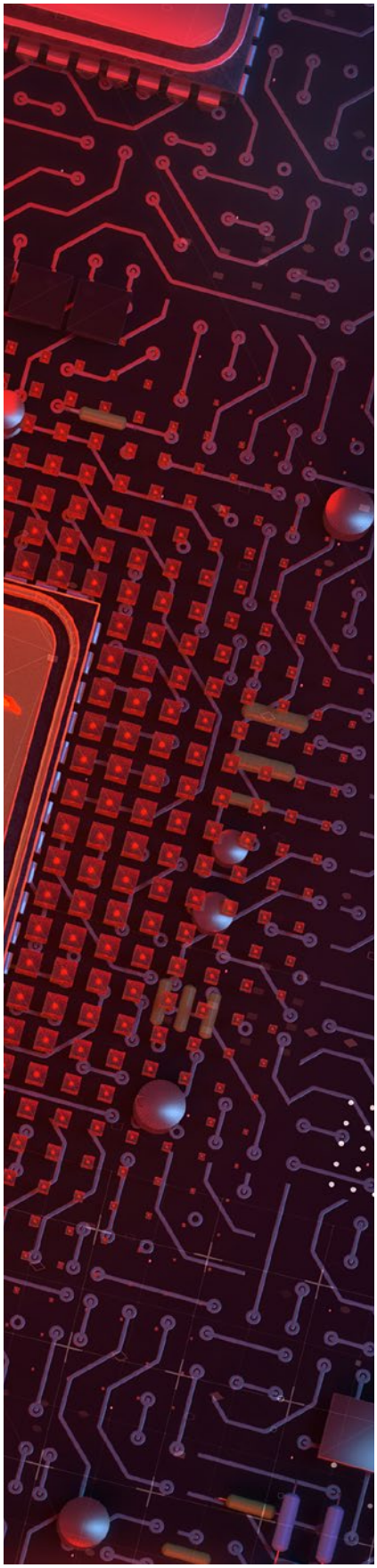
Le Centre pour la cybersécurité travaille étroitement avec les ministères du gouvernement du Canada, les propriétaires et exploitants d'infrastructures essentielles, les entreprises canadiennes et des partenaires internationaux pour intervenir en cas d'incident de cybersécurité ou pour atténuer les conséquences qui en découlent. Le Centre pour la cybersécurité est à l'écoute des entités externes et favorise les partenariats visant un cyberespace canadien fort et résilient. Conformément à la Stratégie nationale de cybersécurité,[1] le Centre pour la cybersécurité représente une approche plus collaborative à la cybersécurité dans notre pays.

Composé d'experts en cybersécurité dignes de confiance, le Centre pour la cybersécurité aide à assurer la sécurité du Canada et des Canadiens comme suit :

- en étant une source claire et fiable de renseignements pertinents sur la cybersécurité pour les 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 et territoriaux, les administrations municipales et des partenaires du secteur privé pour résoudre les défis les plus complexes du Canada en matière de cybersécurité;
- en développant et en diffusant ses 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 lors d'incidents de cybersécurité et en tirant parti de son expertise et de ses 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 Canadiens puissent vivre et travailler en ligne en toute confiance et sécurité.

Pour en savoir plus à ce sujet, consultez le site Web Cyber.gc.ca[2] ou suivez @centrecyber_ca[3] sur Twitter.



Avant-propos de la ministre

Au cours des deux dernières années, la cybersécurité est devenue une des principales préoccupations des Canadiens. Au Canada et à travers le monde, on parle d'incidents liés à des rançongiciels pratiquement tous les jours dans les actualités. Nos services essentiels sont perturbés, qu'il s'agisse d'hôpitaux, d'établissements d'enseignement, d'administrations municipales ou de fournisseurs de services publics. Nos données financières et nos renseignements personnels sont volés, vendus ou fuités en ligne. Nos espaces virtuels sont inondés de fausses informations et de discours incendiaires.

L'*Évaluation des cybermenaces nationales* (ECMN) 2023-2024 aidera les Canadiens à comprendre les tendances actuelles de la cybersécurité et comment on peut s'attendre à ce qu'elles évoluent.

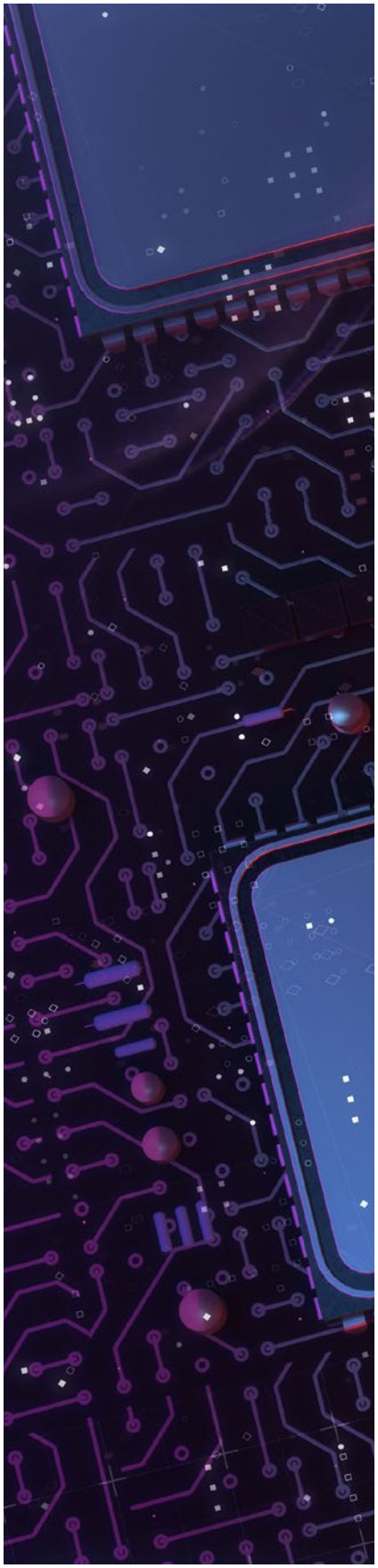
Le Centre pour la cybersécurité offre une vue d'ensemble du contexte des cybermenaces à la fois exhaustif et accessible. L'ECMN se veut particulièrement utile pour les preneurs de décisions canadiens, puisqu'il met l'accent sur les cybermenaces les plus pertinentes pour le Canada. En plus d'être un rapport public, l'ECMN tire également avantage des sources classifiées du CST et du travail accompli par le Centre pour la cybersécurité pour défendre chaque jour le gouvernement du Canada contre les cyberactivités malveillantes. En d'autres mots, cette information est à la fois crédible et complète.

Les menaces évoluent au même rythme que les progrès fulgurants qui ont été réalisés sur le plan de la technologie. Le Centre pour la cybersécurité travaille d'arrache-pied pour soutenir les capacités en cybersécurité dans l'ensemble du Canada, en partenariat avec l'industrie, le milieu universitaire et tous les échelons de gouvernement.

Il faudra miser sur des efforts coordonnés pour faire du Canada un des endroits les plus sûrs où vivre et travailler en ligne. Le travail du Centre pour la cybersécurité protégera les Canadiens et permettra de nous assurer que nous sommes prêts à agir et à intervenir en cas de cybermenaces, et à nous y adapter.

L'honorable Anita Anand
Ministre de la Défense nationale

Message du dirigeant principal du Centre pour la cybersécurité



Merci de faire de la cybersécurité une priorité en lisant le présent rapport.

Si vous avez lu l'une des évaluations des cybermenaces nationales que nous avons publiées en 2018 et en 2020, vous serez familier avec une bonne partie de ce que vous lirez ici.

La cybercriminalité est toujours la principale cybermenace qui touche les Canadiens. Les cyberprogrammes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord continuent d'être les plus grandes cybermenaces stratégiques ciblant le Canada. Les infrastructures essentielles demeurent des cibles de choix pour les cybercriminels et les auteurs parrainés par des États.

Bien qu'il soit rassurant de savoir que notre analyse des grandes tendances est toujours valable, le portrait global du contexte des cybermenaces est tout sauf rassurant. Vous pourriez être tenté d'arrêter votre lecture à mi-chemin, de déconnecter tous vos appareils et de les jeter à la poubelle. Il serait peut-être plus réaliste de hausser les épaules en signe de résignation et de continuer comme avant. J'espère que vous verrez plutôt ce rapport comme un appel à l'action.

Les Canadiens profitent grandement du fait qu'ils vivent dans l'un des pays les plus connectés à Internet au monde, et il faut savoir que les cyberrisques que nous identifions dans ce rapport peuvent être atténués. En fait, il est possible d'éviter la grande majorité des cyberincidents en prenant des mesures de cybersécurité de base.

Pour aider à combler les lacunes entre la connaissance et l'intervention, nous avons préparé des avis et des conseils adaptés à cinq messages transmis dans le présent rapport. Ces publications complémentaires présentent des étapes pratiques permettant d'atténuer les risques associés à chaque thème. D'autres avis et conseils[4] se trouvent sur le site Web du Centre pour la cybersécurité. Et, toujours aussi utile, le site Web Pensez cybersécurité.ca[5] offre aux Canadiens une panoplie de conseils simples et efficaces sur la cybersécurité.

Que vous soyez un débutant en la matière ou un expert chevronné, j'espère que ce rapport ainsi que les conseils qui l'accompagnent sauront vous être utiles pour faire les prochains pas vers une meilleure cybersécurité.

Sami Khoury
Dirigeant principal, Centre canadien pour la cybersécurité

Sommaire

Les Canadiens utilisent Internet pour effectuer des transactions financières, pour communiquer avec leurs proches, pour recevoir des consultations médicales et pour travailler. Compte tenu du fait que les Canadiens passent plus de temps sur Internet et qu'ils accomplissent plus de choses grâce à Internet, les risques occasionnés par les activités de cybermenace ne cessent d'augmenter et peuvent avoir des répercussions sur leur quotidien. Nous avons constaté une augmentation de la quantité de données personnelles, commerciales et financières en ligne, ce qui est attrayant pour les auteurs de cybermenace. Cette tendance de connecter des systèmes importants à Internet fait accroître la menace d'interruption de service causée par des activités de cybermenace. Pendant ce temps, les États-nations et les cybercriminels continuent à développer leurs cybercapacités. Les activités de cybermenace parrainées par des États et motivées par un intérêt financier sont de plus en plus susceptibles de toucher directement les Canadiens. Dans l'ECMN 2023-2024, nous avons choisi de nous concentrer sur cinq discours liés aux cybermenaces que nous croyons être les plus évolutifs et percutants, et qui vont continuer de dominer les activités de cybermenace jusqu'en 2024.

Principaux avis

- **Les rançongiciels représentent une menace omniprésente pour les organisations canadiennes.** La cybercriminalité continue d'être l'activité de cybermenace la plus susceptible de toucher les Canadiens et les organisations canadiennes. En raison de son incidence sur la capacité d'une organisation de fonctionner, les rançongiciels sont presque assurément la forme la plus perturbatrice de cybercriminalité à laquelle sont confrontés les Canadiens. Les cybercriminels qui déploient des rançongiciels ont su évoluer au sein d'un écosystème de cybercriminalité grandissant et sophistiqué; et ils vont continuer à s'adapter de manière à maximiser les profits.

- **Les activités de cybermenace représentent un risque de plus en plus grand pour les infrastructures essentielles.** Les cybercriminels exploitent les infrastructures essentielles, car toute interruption peut être préjudiciable pour les processus industriels et leurs clients. Les auteurs de menace parrainés par des États ciblent les infrastructures essentielles afin d'obtenir de l'information en se livrant à l'espionnage, de se prépositionner en cas d'éventuelles hostilités et de faire acte de force et d'intimidation. Toutefois, selon nos observations, il est très probable que les auteurs de cybermenace parrainés par des États s'abstiennent de perturber ou de détruire intentionnellement les infrastructures essentielles du Canada en l'absence d'hostilités.

- **Les activités de cybermenace parrainées par des États ont des répercussions sur les Canadiens.** Nous estimons que les cyberprogrammes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord sont les plus grandes cybermenaces stratégiques ciblant le Canada. Les activités de cybermenace parrainées par des États visant le Canada représentent une menace constante et continue qui s'inscrivent souvent dans des campagnes mondiales plus vastes qu'entreprennent ces États. Les auteurs de menace étatiques peuvent cibler des activistes et des membres de certaines diasporas au Canada, des organisations canadiennes et leur propriété intellectuelle aux fins d'espionnage, et même des particuliers et des organisations du Canada pour obtenir un gain financier.

- **Les auteurs de cybermenace tentent d'influencer les Canadiens et de briser la confiance accordée aux espaces virtuels.** Nous avons observé que les auteurs de cybermenace ont de plus en plus recours à la mésinformation, à la désinformation et à la malinformation (MDM) depuis les deux dernières années. Les technologies d'apprentissage automatique font en sorte qu'il est plus facile de créer de faux contenus et que ceux-ci sont plus difficiles à détecter. Par ailleurs, les États-nations démontrent de plus en plus de capacité et de volonté envers l'utilisation de MDM pour défendre leurs intérêts géopolitiques. Nous considérons que l'exposition des Canadiens aux campagnes de MDM devrait presque assurément augmenter au cours des deux prochaines années.

- **Les technologies perturbatrices entraînent de nouvelles possibilités et menaces.** Les actifs numériques, comme la cryptomonnaie et les systèmes financiers décentralisés, sont des cibles et des outils qui permettent aux auteurs de cybermenace de mener des activités de cybermenace malveillantes. L'apprentissage automatique est utilisé de manière courante dans les services aux consommateurs et l'analyse de données, mais les auteurs de cybermenace peuvent déjouer et exploiter cette technologie. L'informatique quantique pourrait devenir une menace pour nos systèmes actuels qui inspirent confiance et qui assurent la confidentialité en ligne. En effet, l'information chiffrée qui est volée par des auteurs de menace aujourd'hui pourrait être conservée et déchiffrée après l'arrivée des ordinateurs quantiques.

Table des matières

À propos du présent document vi

Introduction – Évolution des cybermenaces 1
- La COVID-19 et le contexte des cybermenaces 1
- Le travail hybride et le travail depuis n'importe quel endroit impliquent une exposition accrue aux menaces tant pour les particuliers que pour les organisations 2
- Des connexions plus rapides, plus larges et plus de dispositifs connectés à Internet 2
- La cybercriminalité représente une menace sophistiquée pour le Canada 3
- Les auteurs de menace attaquent leurs cibles indirectement en exploitant les vulnérabilités de la chaîne d'approvisionnement et de l'infrastructure d'Internet 3
- La concurrence géopolitique dans le cyberespace expose tout le monde à un risque accru 4
- L'Internet mondial continue de diverger 4

Les rançongiciels représentent une menace omniprésente pour les organisations canadiennes 5
- Les rançongiciels permettent d'autres activités de cybermenace malveillantes 6
- Les rançongiciels perturbent les infrastructures essentielles 6
- L'impact des rançongiciels 6
- Le modèle opérationnel du rançongiciel comme service a rendu les rançongiciels plus accessibles et rentables 7
- Les cybercriminels continueront à adapter leurs méthodes dans le but de maximiser les profits 8

Les activités de cybermenace représentent un risque de plus en plus grand pour les infrastructures essentielles 9
- Les TO connectées augmentent l'exposition aux cybermenaces des infrastructures essentielles 10
- Les infrastructures essentielles dépendent de leur chaîne d'approvisionnement 11
- Les cybercriminels ciblent les infrastructures essentielles 12
- Des auteurs parrainés par des États ciblent les infrastructures essentielles 12

Les activités de cybermenace parrainées par des États ont des répercussions sur les Canadiens 13
- Des États étrangers ciblent les citoyens canadiens 13
- Les auteurs de menace parrainés par des États tentent de compromettre les Canadiens dans le cadre de vastes campagnes à l'échelle mondiale 15
- Des États ciblent la valeur économique du Canada 15
- Des États cherchent à obtenir un gain financier par des moyens virtuels 16
- Des États utilisent des activités et des outils de la cybercriminalité pour éviter l'attribution 16

Les auteurs de cybermenace tentent d'influencer les Canadiens et de briser la confiance accordée aux espaces virtuels 17
- Des auteurs de cybermenace tirent profit de la technologie pour diffuser la MDM et tromper les Canadiens 18
- Des auteurs étrangers utilisent une forme de MDM pour influencer le discours international 19

Des technologies perturbatrices entraînent de nouvelles possibilités et menaces 20
- Des actifs numériques sont des cibles et des outils pour les auteurs de cybermenace 21
- L'automatisation de l'apprentissage automatique peut être trompée et exploitée 21
- L'informatique quantitative menace la cryptographie moderne 22

Conclusion 23

Notes de fin de texte 24

À propos du présent document

Le présent document fait état des cybermenaces qui visent les citoyens et les entreprises du Canada. Il fournit une mise à jour de l'Évaluation des cybermenaces nationales 2018[6] (ECMN 2018) et de l'Évaluation des cybermenaces nationales 2020[7] (ECMN 2020), ainsi qu'une analyse des années intermédiaires et des prévisions d'ici 2024. Nous recommandons la lecture de l'ECMN 2023-2024, de l'Introduction à l'environnement de cybermenace[8] mise à jour, et des avis et conseils adaptés que nous avons publiés pour donner des renseignements complémentaires à cette évaluation.

Conformément à l'optique de la Stratégie nationale de cybersécurité,[9] nous avons préparé ce document pour aider à façonner et à soutenir la résilience de notre nation en matière de cybersécurité. Ce n'est que lorsque le gouvernement, le secteur privé et les particuliers travaillent ensemble que nous pouvons instaurer une résilience face aux cybermenaces au Canada.

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 les citoyens et les organisations canadiennes. Des conseils sur la cybersécurité[10] se trouvent sur le site Web du Centre pour la cybersécurité et sur le site Web de Pensez cybersécurité.[11]

Sources

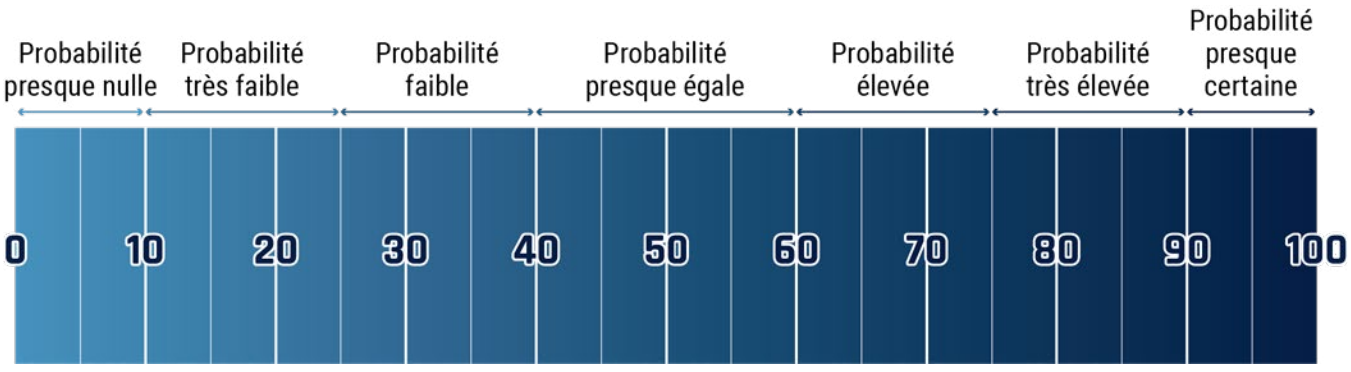
Les avis formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise du Centre pour la cybersécurité en matière de cybersécurité. Le rôle que joue le Centre pour la cybersécurité dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans l'environnement de cybermenace, ce qui a contribué à la présente évaluation. Le mandat de renseignement étranger du CST lui procure de précieuses informations sur le comportement des adversaires dans le cyberespace. Bien que le Centre pour la cybersécurité soit toujours tenu de protéger les sources et méthodes classifiées, il fournira au lecteur, dans la mesure du possible, les justifications qui ont motivé ses avis.

Processus d'évaluation

Les évaluations des cybermenaces effectuées sont basées sur un processus d'analyse 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 », « susceptible », « probable » et « très probable » pour exprimer les probabilités.

La présente évaluation des menaces se fonde sur des renseignements disponibles en date du 4 octobre 2022.

Lexique des estimations



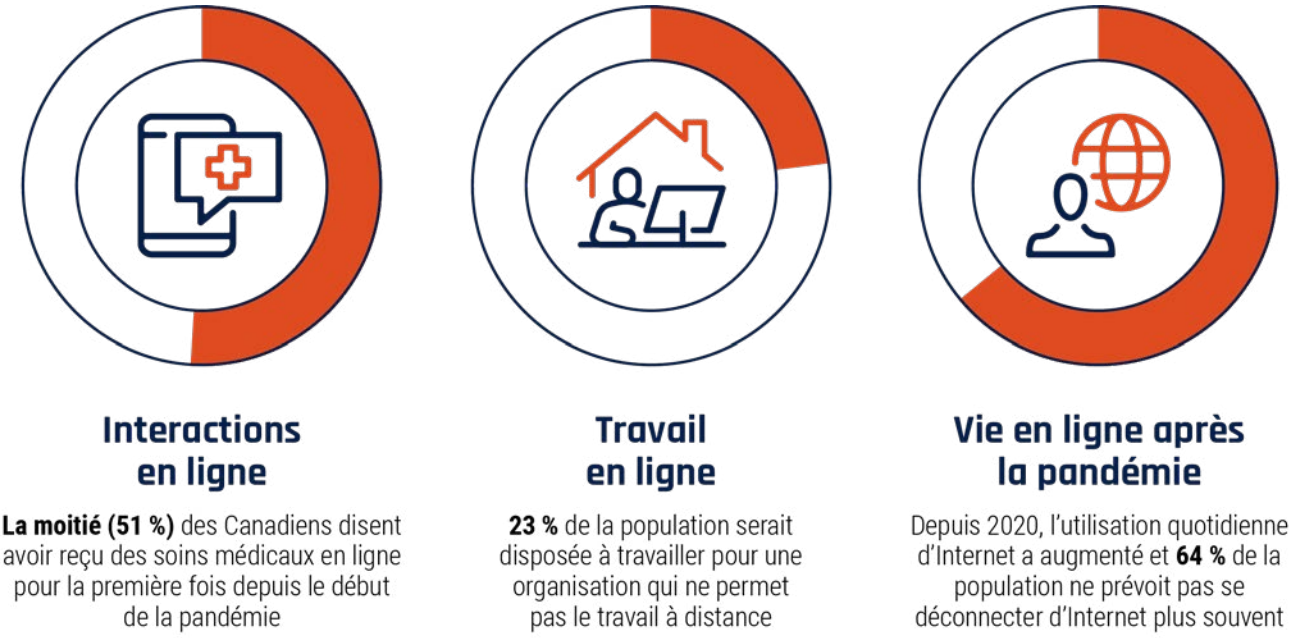
Introduction – Évolution des cybermenaces

Les éditions précédentes de l'Évaluation des cybermenaces nationales (ECMN) décrivaient les cybermenaces auxquelles ont fait face les citoyens, les organisations et les fournisseurs d'infrastructures essentielles du Canada. Elles annonçaient également comment ces menaces allaient évoluer au cours des prochaines années. Plusieurs des menaces que nous avons identifiées demeurent pertinentes aujourd'hui, mais la nature de ces menaces a changé. Les auteurs de menace ont adapté leurs techniques, de nouvelles technologies ont donné lieu à de nouvelles cybercapacités, et les Canadiens n'auront jamais autant utilisé Internet.

La COVID-19 et le contexte des cybermenaces

En 2020, nous avons discuté de la façon dont la pandémie de COVID-19 a rapidement changé le contexte des cybermenaces. Plus de deux ans après le début de la pandémie, les Canadiens ont une approche différente à l'égard d'Internet. Plus de gens utilisent Internet pour effectuer des achats, se procurer de la nourriture, communiquer avec leurs proches, recevoir des consultations médicales et travailler. Aujourd'hui, les Canadiens combinent le travail en personne et le travail rn mode virtuel. Depuis 2020, de plus en plus d'organisations ont adopté des services infonuagiques pour travailler efficacement dans un environnement hybride.

Figure 1 : La COVID-19 a une incidence durable sur la façon dont les Canadiens utilisent Internet[12]



Selon nos observations, l'exposition aux cybermenaces s'est accrue depuis 2020. À l'heure actuelle, le volume de données recueilli sur chaque Canadien est important. Ce volume ne fera qu'augmenter à mesure que de nouvelles technologies entreront sur le marché, créant une foule d'occasions pour les auteurs de menace qui cherchent à voler des renseignements personnels. Par ailleurs, le contexte mondial des cybermenaces est en pleine évolution tandis que des États-nations ont de plus en plus recours aux cyberactivités comme outil de concurrence stratégique et de conflit.

Pour aider les Canadiens à mieux comprendre le contexte des cybermenaces, nous avons également mis à jour et étoffé la publication intitulée *Introduction à l'environnement de cybermenace*.[13]

Dans la présente section, nous décrivons les tendances qui sous-tendent le contexte actuel des cybermenaces et nous évaluons la direction que devraient prendre ces tendances.

Le travail hybride et le travail depuis n'importe quel endroit impliquent une exposition accrue aux menaces tant pour les particuliers que pour les organisations

Plus d'un tiers des Canadiens ont travaillé de la maison plus souvent durant la pandémie.[14] Maintenant, plus de deux ans plus tard, beaucoup de Canadiens passent de manière plus permanente à un environnement de travail hybride.[15] Le travail depuis n'importe quel endroit implanté et maintenu de façon sécuritaire offre aux employés et à leurs employeurs une certaine souplesse, mais il crée également une plus grande exposition aux menaces. En effet, cette exposition offre plus de possibilités aux auteurs de menace d'accéder aux réseaux et aux dispositifs d'organisations et de particuliers.

Les réseaux des entreprises sont de plus en plus intégrés dans les résidences des employés et dans les espaces publics. Toujours selon nos observations, il est très probable que les auteurs de cybermenace continuent d'exploiter l'infrastructure de travail hybride et de cibler les réseaux domestiques ainsi que les dispositifs personnels des employés pour accéder aux organisations canadiennes. Ces auteurs tirent parti de l'accessibilité à distance des organisations pour tenter de compromettre les réseaux d'entreprise par des connexions à distance.[16] Lorsque les employés accèdent aux réseaux et à l'information d'entreprise à partir de leurs réseaux domestiques et de leurs dispositifs, ils créent des conditions favorables pour que les auteurs de cybermenace en fassent de même. Ils peuvent ainsi accéder à des renseignements commerciaux sensibles et à des renseignements sur les employés.[17]

Des connexions plus rapides, plus larges et plus de dispositifs connectés à Internet

On compte plus de Canadiens qui utilisent des technologies connectées à Internet pour les interactions quotidiennes

Les Canadiens sont devenus des utilisateurs plus compétents en matière d'Internet, et ils utilisent davantage Internet pour le divertissement, l'information, le travail et les interactions sociales.[18] Les Canadiens sont aussi plus nombreux à être connectés tandis que des initiatives gouvernementales permettent à des régions éloignées de profiter d'un réseau Internet haute vitesse fiable, et de nouvelles technologies, comme l'Internet par satellite, facilitent l'aspect géographique du clivage informatique.[19] La pandémie de COVID-19 a fait valoir l'importance des connexions Internet accessibles et fiables. La pandémie a rendu nécessaire de déplacer en ligne les interactions qui se faisaient auparavant en personne, et la situation a également obligé l'adhésion rapide à des technologies liées au télétravail et à l'éducation, à la recherche de contacts, et aux services bancaires et de vente au détail en ligne. L'adoption généralisée de technologies sans contact pour les activités quotidiennes des Canadiens augmente leur exposition aux activités de cybermenace, comme le vol de données, la fraude et l'extorsion.

Les technologies opérationnelles connectées à Internet et les systèmes intelligents augmentent la portée des activités de cybermenace

La tendance se poursuit vers la connexion de dispositifs qui interagissent avec le monde réel, notamment le déploiement de dispositifs qui composent l'Internet des objets (IdO) et l'Internet industriel des objets (IIoT pour *Industrial Internet of Things*), ce qui étend l'exposition aux cybermenaces. Ces types de dispositifs sont appelés à se répandre à mesure que le Canada adopte la technologie cellulaire de cinquième génération (5G). Cette technologie apporte des améliorations considérables par rapport à la technologie 4G/LTE, et elle permettra la connexion d'un plus grand nombre de dispositifs, et ce, à des vitesses beaucoup plus élevées. Ce phénomène a des implications pour les villes intelligentes, l'agriculture de précision et d'autres utilisations de systèmes « intelligents » comme les applications qui dépendent de capteurs, d'automatisation et de grandes quantités de données.[20] Avec le Canada qui adopte des systèmes intelligents et qui adhère davantage à l'ère du numérique, de plus en plus de secteurs et de services deviendront vulnérables aux activités de cybermenace, y compris l'espionnage, la fraude, l'extorsion et le sabotage. Les systèmes intelligents produisent de grandes quantités de données qui, dans certaines applications, peuvent comprendre des renseignements personnels détaillés provenant des utilisateurs. Les systèmes intelligents sont aussi intégrés aux services physiques et exposés à Internet, ce qui augmente le potentiel d'interruption de service causée par des activités de cybermenace.

La cybercriminalité représente une menace sophistiquée pour le Canada

Comme nous l'avons observé dans les éditions précédentes de l'ECMN, la cybercriminalité demeure l'activité de cybermenace la plus susceptible de toucher les Canadiens. Cela s'explique en partie par un marché florissant pour les outils et les services de cybercriminalité facilement accessibles sur les marchés et les forums en ligne, ou dans des communautés de cybercriminalité privées. De tels outils et services comprennent l'accès initial au réseau, les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*), les outils de défiguration de sites Web, les maliciels (y compris les rançongiciels) et les technologies de blanchiment d'argent. Les cybercriminels peuvent ainsi acheter des capacités spécialisées au lieu de développer leurs propres compétences au fil du temps. Les obstacles à l'entrée sont ainsi réduits pour les cybercriminels, ce qui permet même à des auteurs de menace sans expérience de tirer parti d'outils et de services plus efficaces et spécialisés.

Il devient de plus en plus facile d'accéder à des renseignements volés ou ayant fait l'objet d'une fuite, comme des justificatifs d'ouverture de session, des renseignements financiers et des renseignements personnels, sur les forums de cybercriminalité.[21] Ces données volées ouvrent la porte d'autres cybercrimes, notamment la fraude, l'escroquerie et des cyberactivités plus perturbatrices comme les rançongiciels. Les rançongiciels font partie des cybermenaces ayant le plus de répercussions pour le Canada. Les opérateurs de rançongiciels profitent considérablement de l'économie de la cybercriminalité spécialisée et de l'accessibilité grandissante à des renseignements volés. Les cybercriminels tirent parti de la cryptomonnaie et utilisent des communications chiffrées pour garder leur anonymat et se soustraire à l'application de la loi.[22] Ils sont prompts à adopter et à manipuler les nouvelles technologies dans leur propre intérêt. Par exemple, les cybercriminels ont tiré parti d'un système financier décentralisé, qui utilise la cryptomonnaie pour permettre des emprunts et du financement à grande échelle sans passer par des intermédiaires, pour voler d'importantes sommes d'argent.[23] Il est très probable que les gains importants générés par la cybercriminalité, y compris les gains résultant des rançongiciels, de fraudes et d'escroqueries, comme la compromission de courriel d'affaires (BEC pour *Business Email Compromise*), continueront d'attirer l'attention de nouveaux groupes de cybercriminels même si les activités de certains groupes sont limitées par les efforts accrus des organismes chargés de l'application de la loi.

Les auteurs de menace attaquent leurs cibles indirectement en exploitant les vulnérabilités de la chaîne d'approvisionnement et de l'infrastructure d'Internet

Plutôt que de cibler directement les organisations, ces auteurs visent de plus en plus les outils et les services logiciels qu'utilisent les organisations en compromettant la chaîne d'approvisionnement. La menace émanant de compromissions de la chaîne d'approvisionnement augmente lorsque les fournisseurs ont un accès de niveau élevé aux réseaux de leurs clients. Ce type de relation devient de plus en plus courant avec la prolifération des logiciels infonuagiques, des infrastructures dans le nuage et des modèles de plateforme-service. En propageant un maliciel par l'entremise des mises à jour et des services d'un fournisseur, les auteurs de cybermenace implantent des vulnérabilités sur les réseaux clients du fournisseur. Les compromissions de la chaîne d'approvisionnement sont, de manière générale, plus complexes que les compromissions directes. Ainsi, selon nos observations, elles demeureront vraisemblablement un outil utilisé principalement par les auteurs de menace parrainés par des États et les cybercriminels dotés de moyens sophistiqués.

Les auteurs de cybermenace profitent également des faiblesses liées au code utilisé partout sur Internet et dans le développement logiciel. Les services Web et les applications informatiques comptent souvent sur du code source ouvert géré par des tiers. Lorsque des vulnérabilités sont trouvées dans un code tiers courant, tout projet utilisant ce code devient vulnérable.

Pour des applications comme Log4J, un logiciel de source ouverte populaire présentant une vulnérabilité dévoilée vers la fin de 2021 et exploitée à grande échelle par des auteurs de cybermenace, l'étendue des répercussions peut s'avérer complexe.[24] Pendant les quatre mois avant que l'exploit ne se soit fait largement connaître, l'application Log4J a été téléchargée plus de 28 millions de fois.[25] L'exploit, Log4Shell, a été rendu public, ce qui a donné aux auteurs de cybermenace un vaste accès aux outils permettant de compromettre tout service utilisant Log4J.[26]

On considère qu'il est presque certain que les vulnérabilités dans les services courants et les composants logiciels continueront de faire l'objet de découvertes et d'exploitations de la part d'auteurs de menace, et ce, à grande échelle. Nous sommes également d'avis que même après que des correctifs ont été développés, les auteurs de menace continueront sans doute de balayer Internet pour trouver de façon opportune les systèmes non corrigés.

La concurrence géopolitique dans le cyberespace expose tout le monde à un risque accru

Des États-nations ont recours à des cyberactivités malveillantes comme tactique de subversion et pour affirmer leur puissance afin d'atteindre leurs objectifs géopolitiques. Les activités de cybermenace malveillantes menées par des auteurs de cybermenace parrainés par des États sont devenues un outil important dont se servent des pays pour influencer des événements tout en restant sous le seuil du conflit, et pour appuyer une guerre conventionnelle.

Les infrastructures essentielles canadiennes sont presque assurément les cibles de cyberactivités malveillantes cautionnées par des nations. Bien que nous estimions qu'il est très probable que les auteurs de cybermenace parrainés par des États s'abstiennent de perturber ou de détruire intentionnellement les infrastructures essentielles du Canada en l'absence d'hostilités, ces auteurs développent quand même les capacités pour leur permettre de perturber les systèmes essentiels du Canada et de ses alliés. Si elles sont menées à bien, ces activités peuvent avoir d'importantes répercussions sur la capacité des Canadiens de communiquer et de recevoir des biens et des services essentiels. De même, les auteurs de cybermenace parrainés par des États multiplient la mésinformation, la désinformation et la malinformation (MDM) pour influencer les populations internationales et tirer profit des divisions sociales.[27] Ces activités servent à justifier ou à rallier des appuis pour l'atteinte des objectifs idéologiques des pays, à avoir un impact sur le discours international en lien avec les événements actuels ou à inciter à la méfiance pour fragiliser les institutions démocratiques canadiennes.

INVASION DE L'UKRAINE PAR LA RUSSIE – UNE NOUVELLE CYBERPERSPECTIVE

L'invasion russe de l'Ukraine en février 2022 a changé la compréhension mondiale de la façon dont les cyberactivités sont utilisées pour appuyer des opérations en temps de guerre. Les cyberactivités malveillantes contre l'Ukraine parrainées par la Russie ont perturbé ou ont tenté de perturber les activités d'organisations dans les secteurs publics, financiers et énergétiques, et elles coïncidaient souvent avec des opérations militaires conventionnelles. Ces attaques se sont étendues au-delà de l'Ukraine pour impliquer également les infrastructures essentielles européennes. Par exemple, l'attaque de la Russie visant un fournisseur de services Internet par satellite européen a entraîné une importante panne dans plusieurs pays d'Europe.[28] Des opérations de désinformation coordonnées en appui au discours de la Russie au sujet de l'invasion ont également accompagné les activités militaires et les cyberactivités.[29]

L'Internet mondial continue de diverger

Dans l'ECMN 2020, nous avons décrit comment les États-nations développaient des normes concurrentes pour encadrer la diffusion de l'information sur Internet. Une approche, axée sur la souveraineté nationale, considère l'information en ligne principalement sur le plan de la stabilité et de la sécurité nationale, et elle favorise un réseau Internet qui permettra aux pays de surveiller leurs citoyens et de censurer l'information. Utiliser Internet pour censurer et surveiller des populations met en péril l'approche d'ouverture, de transparence et de multilatéralité adoptée par le Canada et d'autres pays aux vues similaires. Pourtant, un nombre croissant de pays gèrent leur Internet à l'échelle nationale de cette façon. En 2021, AccessNow rapportait que 34 pays ont eu recours à des interruptions du réseau Internet pour réprimer des troubles sociaux et politiques ou pour contrôler la diffusion de l'information durant des élections et en période de conflit.[30] Freedom House estime que 56 % des utilisateurs d'Internet à travers le monde vivent dans des pays où les contenus politiques, sociaux ou religieux ont été bloqués en ligne.[31]

Il est fort probable qu'au cours des deux prochaines années, les divergences continuent de s'accroître entre un Internet ouvert et transparent, et un Internet axé sur la souveraineté nationale. La Russie et la Chine ont investi dans leur propre infrastructure Internet et, avec d'autres pays, ils veulent préconiser des normes technologiques en matière d'information et de communications. Ces normes permettraient un plus grand contrôle d'Internet dirigé par l'État de chaque pays respectif.[32] En 2022, la Chine a présenté une nouvelle organisation à l'origine de la Conférence mondiale sur l'Internet qui est consacrée à la gouvernance d'Internet. L'organisation compte des membres provenant de 20 pays.[33] Bien que la gouvernance d'Internet puisse sembler être un concept abstrait qui s'éloigne du quotidien, nous croyons que les écosystèmes technologiques concurrents et les environnements disparates axés sur l'information empêchent la libre circulation de l'information, créent de la méfiance et font en sorte qu'il est plus difficile de combattre la mésinformation et la désinformation.

Les rançongiciels représentent une menace omniprésente pour les organisations canadiennes

Comme nous l'avons observé dans des éditions précédentes de l'ECMN, la cybercriminalité continue d'être l'activité de cybermenace la plus susceptible de toucher les Canadiens et les organisations canadiennes. La fraude et les escroqueries sont presque assurément les formes les plus courantes de cybercriminalité auxquelles seront confrontés les Canadiens au cours des deux prochaines années en raison des auteurs de menace qui tentent de voler des renseignements personnels, financiers et commerciaux par Internet. La fraude et les escroqueries, y compris les activités de cybermenace malveillantes comme l'hameçonnage, entraînent d'importantes pertes financières. Selon le Centre antifraude du Canada, plus de 150 000 incidents de fraude ont été signalés au Canada, ce qui totalise des vols se chiffrant à plus de 600 millions de dollars depuis janvier 2021.[34]

En raison de son incidence sur la capacité d'une organisation de fonctionner, les rançongiciels sont presque assurément la forme la plus perturbatrice de cybercriminalité à laquelle sont confrontés les Canadiens. Outre le coût financier de la rançon, un rançongiciel peut interrompre le fonctionnement de systèmes importants, endommager ou détruire les données d'une organisation, et révéler de l'information sensible, en plus d'imposer des coûts et du temps de reprise après une attaque. L'interruption que cause une attaque par rançongiciel peut empêcher l'accès à des services essentiels et, dans certains cas, menacer la sécurité physique des Canadiens.

Les rançongiciels ont presque assurément une incidence plus importante sur les organisations canadiennes aujourd'hui qu'en 2020. Depuis 2020, la fréquence des attaques par rançongiciel à travers le monde a augmenté, et les demandes de rançon réclamées aux grandes entreprises sont en hausse.[35]

Les rançongiciels permettent d'autres activités de cybermenace malveillantes

Un rançongiciel est un programme malveillant qui permet de bloquer l'accès à un ordinateur ou à un dispositif et à son fonctionnement; l'accès au système sera potentiellement rendu après le versement d'une rançon. Généralement, les auteurs de menace vont compromettre une victime, chiffrer ses données et exiger une rançon en échange de la clé de déchiffrement. De nos jours, la plupart des attaques par rançongiciel sont des attaques à double extorsion. Cela signifie que les opérateurs de rançongiciels vont exfiltrer des fichiers avant de les chiffrer et menacer de mettre de l'information sensible à la disposition du public si une rançon n'est pas versée.[36]

Au-delà des répercussions liées à un rançongiciel en tant que tel, les données volées lors d'une attaque par rançongiciel permettent presque assurément à un large éventail d'auteurs de mener d'autres activités de cybermenace. L'information qui fait l'objet d'une fuite contient souvent des renseignements personnels et commerciaux sensibles qui peuvent être accessibles librement sur les sites Web d'opérateurs de rançongiciels ou être vendus à un acheteur sur des marchés de cybercriminalité privés ou en ligne.[37] D'autres auteurs de menace peuvent se servir de cette information pour mener à bien d'autres activités de cybercriminalité, comme le vol d'identité commis à l'encontre de particuliers ou même l'utilisation d'autres rançongiciels. Ces auteurs peuvent également tirer parti des renseignements commerciaux pour soutenir des activités d'espionnage commercial. En mai 2022, une société canadienne dans le secteur de la défense a confirmé dans le cadre d'un reportage qu'elle enquêtait sur une possible attaque par rançongiciel.[38] Compte tenu de la nature délicate des données de l'organisation, cette information pourrait intéresser d'autres auteurs de menace à des fins d'espionnage ou pour mener d'autres activités de cybercriminalité.

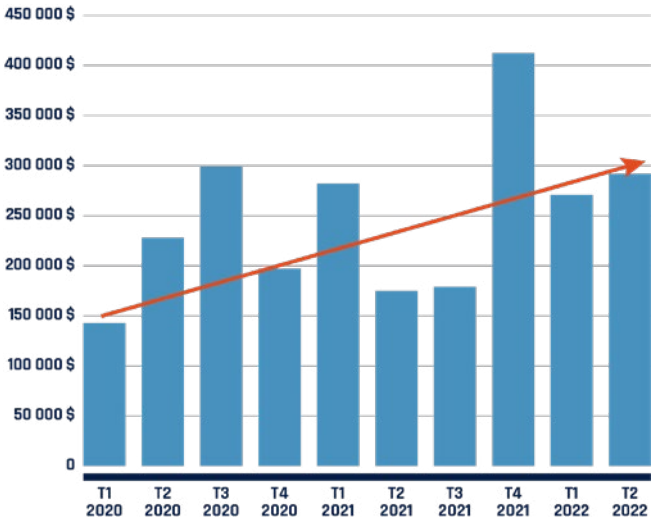
Les rançongiciels perturbent les infrastructures essentielles

Les infrastructures essentielles sont des cibles particulièrement attrayantes pour les rançongiciels. Comme nous l'avons souligné dans la discussion sur les menaces à l'endroit des infrastructures essentielles, les organisations sont perçues par les cybercriminels comme étant prêtes à payer de lourdes rançons pour limiter ou éviter une interruption et les répercussions que pourraient subir leurs clients. En mai 2021, des attaques par rançongiciel commises contre Colonial Pipeline aux États-Unis, et les activités nord-américaines et australiennes de JBS Foods, ont rapporté plusieurs millions de dollars en gains aux auteurs de menace. Ces attaques ont causé des perturbations majeures au sein de la chaîne d'approvisionnement en carburant et de la chaîne agroalimentaire.[39] Au Canada, une attaque par rançongiciel a causé une interruption des services essentiels dans un hôpital de l'Ontario en juin 2021. En octobre 2021, en raison de serveurs qui ont été chiffrés et verrouillés, un service municipal de transport a été dans l'impossibilité de diffuser les renseignements sur les horaires et les trajets.[40] Le Centre pour la cybersécurité a été avisé d'une activité de rançongiciel touchant plusieurs industries au Canada depuis 2020, ce qui comprend la majorité des secteurs des infrastructures essentielles du Canada. Bien que les infrastructures essentielles et les grandes entreprises soient des cibles attrayantes, les cybercriminels sont opportunistes, et c'est pour cette raison qu'il est presque certain qu'ils ne limiteront pas leurs activités à ces secteurs au Canada au cours des deux prochaines années.

L'impact des rançongiciels

Les signalements en matière de cybersécurité indiquent que les rançons obtenues sont en hausse depuis 2020; cela s'explique en partie par des demandes de rançon de plus en plus importantes réclamées aux grandes entreprises.[41] Même si les victimes acceptent de payer la rançon, il n'est pas garanti qu'ils récupéreront leurs données. Une enquête menée sur des entreprises canadiennes a indiqué que seulement 42 % des entreprises qui paient la rançon sont en mesure de récupérer complètement leurs données.[42] La valeur de la rançon ne représente souvent qu'une partie du coût total pour l'entreprise. Une perte de valeur associée à des temps d'arrêt, à des données irrécupérables, à des coûts pour la réparation des systèmes et à une atteinte à la réputation n'est que quelques-uns des coûts additionnels que peut impliquer un rançongiciel.

Figure 2 : Paiements moyens d'extorsions par rançongiciel depuis 2020 (données de Coveware avec conversion de $ US à $ CA)[43]



MESURES JUDICIAIRES CONTRE LES CYBERCRIMINELS UTILISANT DES RANÇONGICIELS

En mai 2021 et encore une fois au début de 2022, nous avons observé une diminution des incidents de rançongiciel dirigés contre les Canadiens. Selon nos observations, cette diminution serait attribuable au fait que les auteurs de menace cherchent à éviter l'attention accrue de la police à la suite de mesures internationales.

Bien que les mesures judiciaires perturbent presque assurément les activités des cybercriminels, nous croyons que ces perturbations ont rarement des effets durables sur l'environnement des rançongiciels. Plusieurs semaines après que, au début de 2022, la Russie a arrêté 14 personnes associées à un gang de rançongiciels bien connu, des chercheurs en cybersécurité ont noté que ce groupe avait repris du service.[44]

Le modèle opérationnel du rançongiciel comme service a rendu les rançongiciels plus accessibles et rentables

Il est fort probable que la majorité des rançongiciels qui touchent les Canadiens appartiennent à des groupes de cybercriminels qui adhèrent au modèle du rançongiciel comme service (RaaS pour *Ramsomware-as-a-Service*). Ces groupes créent et assurent le maintien de variantes de rançongiciels et ils en vendent l'accès à d'autres cybercriminels qui déploient le rançongiciel contre une victime. Les groupes qui offrent des rançongiciels comme service peuvent demander un paiement initial, des frais d'abonnement ou un pourcentage des profits, ou exiger les trois en échange d'un accès à leurs rançongiciels.[45] Nous croyons qu'avec ce modèle de service, les obstacles à l'entrée sont réduits pour les cybercriminels, permettant ainsi aux auteurs de menace dotés de moyens moins sophistiqués d'accéder plus facilement à des capacités de rançongiciel et d'extorquer de l'argent aux victimes.

Figure 3 : La chaîne d'approvisionnement du rançongiciel comme service

Les cybercriminels continueront à adapter leurs méthodes dans le but de maximiser les profits

Tant que les rançongiciels demeureront rentables, il est fort probable que nous verrons les cybercriminels les déployer. Une combinaison de comportements permissifs de la part de nations, particulièrement en Russie, à l'égard de la cybercriminalité ciblant des victimes à l'extérieur des pays formant l'ancienne Union soviétique, et un bassin de talents composé de cybercriminels, facilitent la croissance et le développement d'organisations criminelles dédiées à l'élaboration et au déploiement de rançongiciels. Les auteurs de cybermenace font également preuve de souplesse en tirant parti de la chaîne d'approvisionnement en rançongiciel, et ce, de manière innovante afin de s'assurer que leurs activités restent réalisables. Par exemple, des reportages médiatiques et des rapports de fournisseurs indiquent que certains opérateurs de rançongiciels passent à l'utilisation d'une monnaie privée (une cryptomonnaie qui assure des niveaux élevés d'anonymat) pour cacher plus efficacement leurs activités, bien que le bitcoin demeure le mode de paiement le plus courant pour les rançongiciels.[46]

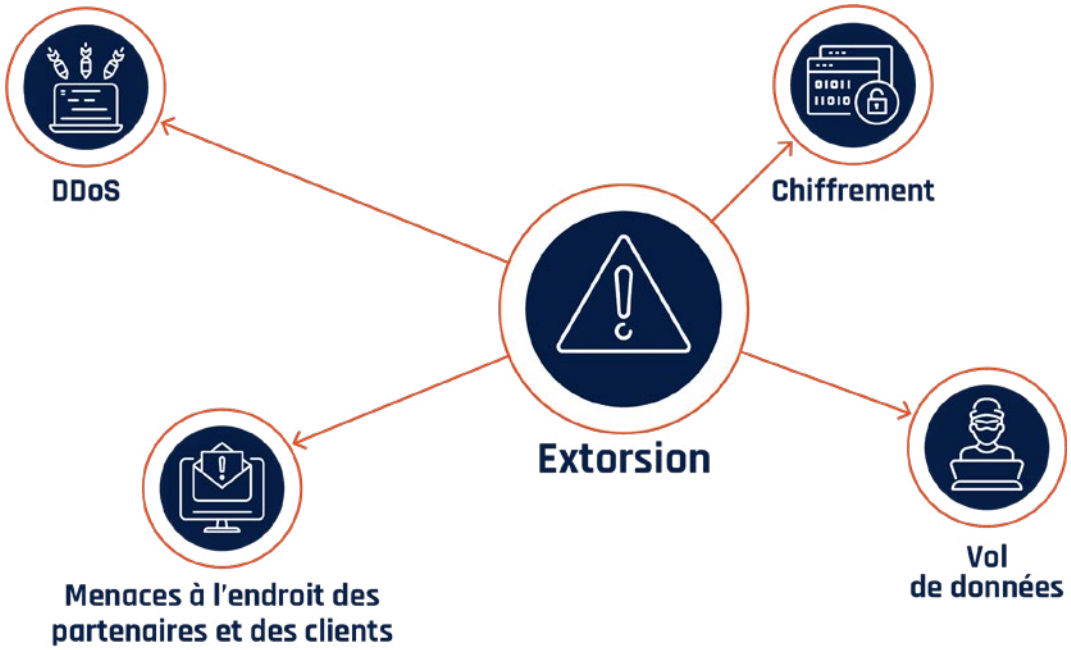
Cibler les chaînes d'approvisionnement et les fournisseurs de services gérés

Il est fort probable que les cybercriminels continuent de cibler les fournisseurs de services gérés (FSG), entreprises qui hébergent et gèrent les ressources TI de leurs clients, et les chaînes d'approvisionnement des logiciels pour maximiser la portée des opérations visées par des rançongiciels. En 2021, des reportages dans les médias indiquaient que des cybercriminels avaient compromis et propagé un rançongiciel en ayant recours à la solution *Virtual System Administrator* de Kaseya, un système qu'utilisent les FSG pour gérer les réseaux de leurs clients. Des cybercriminels ont été en mesure de distribuer le rançongiciel à environ 60 FSG et 1 500 de leurs clients.[47]

Les méthodes d'extorsion évoluent

Selon nos observations, au cours des deux prochaines années, les auteurs de cybermenace utiliseront fort probablement diverses techniques d'extorsion pour s'attaquer à leurs victimes et maximiser leurs chances de recevoir les sommes demandées. Outre le chiffrement des systèmes et le vol de données, dans certains cas les opérateurs de rançongiciels utiliseront d'autres techniques, comme le fait de menacer les partenaires ou les clients d'une organisation et le recours aux attaques par déni de service distribué (DDoS). En menaçant les partenaires commerciaux ou les clients d'une victime, il est très probable que les cybercriminels s'attendent à ce que ces organisations fassent pression sur la victime pour qu'elle paie la rançon, de peur que leurs renseignements commerciaux sensibles ou leurs opérations se retrouvent entre les mains d'un auteur de menace.[48] Le DDoS ajoute de la pression sur une victime en ajoutant une couche supplémentaire de perturbation au réseau d'une organisation. Un groupe de cybercriminels, qui a ciblé des victimes au Canada, a mené des attaques DDoS durant les négociations de paiement.[49] Même si les nombreuses attaques à l'origine d'extorsions sont courantes, certains auteurs de cybermenace préfèrent s'éloigner du chiffrement traditionnel des systèmes de leurs victimes pour se concentrer uniquement sur les méthodes d'extorsion uniques.[50]

Figure 4 : Méthodes d'extorsion par rançongiciel



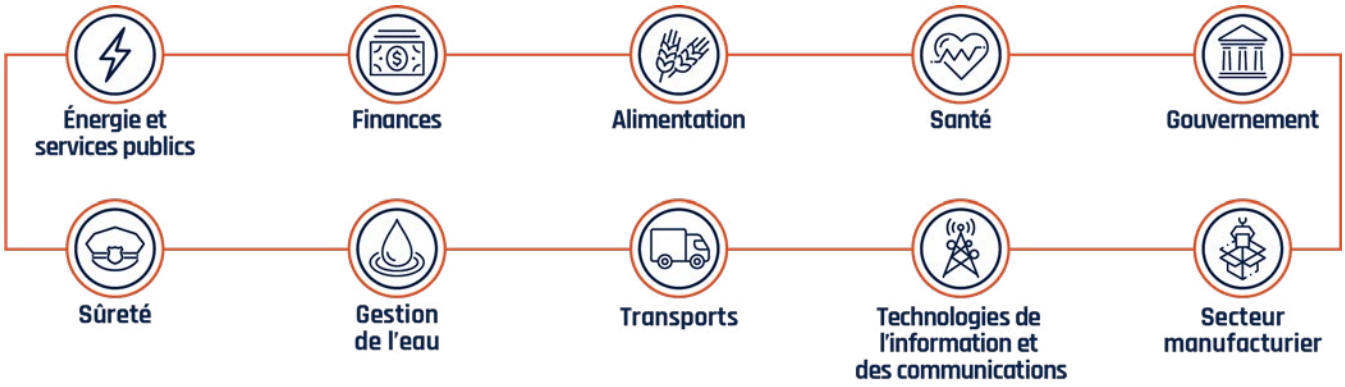
Les activités de cybermenace représentent un risque de plus en plus grand pour les infrastructures essentielles

Les infrastructures essentielles sont employées pour appuyer beaucoup des services qu'utilisent les Canadiens tous les jours. Lorsque se produisent des interruptions de service, les répercussions peuvent s'avérer considérables. Bien qu'elles ne soient pas liées à des cyberactivités malveillantes, les pannes concernant les cellulaires et Internet qui ont touché le Canada en 2021 et en 2022 ont bien illustré l'importance de la connectivité et de l'interconnectivité entre les secteurs des infrastructures essentielles.[51] Outre les incidences sur les particuliers, les pannes ont également eu des répercussions sur le traitement des paiements et les lignes d'urgence.[52] Les occasions de perturber les infrastructures essentielles s'étendent à mesure que les opérateurs exposent les technologies opérationnelles (TO) sous-jacentes aux procédés industriels à l'Internet. Les TO connectées à Internet augmentent l'exposition aux cybermenaces des organisations qui l'utilisent et augmentent également les risques qu'une activité de cybermenace ait des effets dans le monde réel.

Les auteurs de cybermenace sont conscients de l'impact que peut avoir le ciblage des infrastructures essentielles. Ils exploitent ainsi la fragilité des infrastructures essentielles face à des interruptions de service pour extorquer une rançon. Les auteurs de cybermenace parrainés par des États ciblent les infrastructures essentielles afin d'obtenir de l'information en se livrant à l'espionnage, de se prépositionner en cas d'éventuelles hostilités et de faire acte de force et d'intimidation. Toutefois, selon nos observations, il est très probable que les auteurs de cybermenace parrainés par des États s'abstiennent de perturber ou de détruire intentionnellement les infrastructures essentielles du Canada en l'absence d'hostilités.

Les fournisseurs d'infrastructures essentielles hébergent de grandes quantités de renseignements sensibles importants qui peuvent être ciblés par des auteurs de cybermenace, y compris la propriété intellectuelle sur la conception et la maintenance de TO et les renseignements personnels que le fournisseur a pu recueillir des consommateurs. Des renseignements sensibles peuvent également être révélés au profit d'une activité de cybermenace motivée par un intérêt financier. Des chercheurs estiment que près d'une attaque par rançongiciel sur sept perpétrée contre les infrastructures essentielles au cours de laquelle des renseignements sont volés et divulgués, révèlent des renseignements sensibles sur les TO.[53] Les auteurs de menace peuvent avoir recours à de l'information technique sur les TO pour planifier d'éventuelles cyberactivités, ou cette information peut devenir un élément précieux pour la vente ou comme cible pour mener des activités d'espionnage commercial.

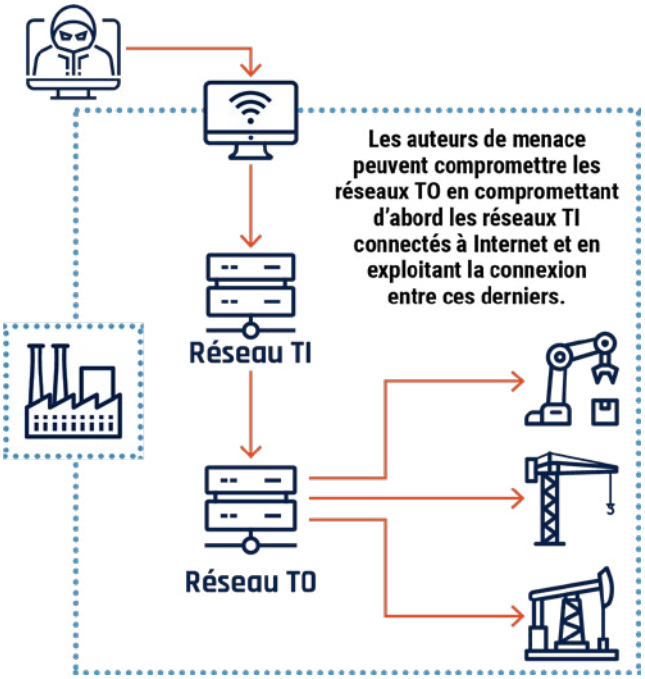
Figure 5 : Secteurs des infrastructures essentielles[54]



Les TO connectées augmentent l'exposition aux cybermenaces des infrastructures essentielles

Dans l'ECMN 2020, nous avons décrit comment les fournisseurs d'infrastructures industrielles et essentielles connectent de plus en plus les TO, qui sont utilisées pour contrôler et surveiller les processus physiques, aux technologies de l'information (TI). Qu'elles soient connectées ou intelligentes, les TO augmentent l'efficacité des processus grâce à l'échange de données amélioré, à la gestion centralisée et à l'automatisation. Le marché mondial de la technologie intelligente était évalué en 2020 à environ 280,05 milliards de dollars canadiens et il devrait connaître une croissance de plus d'un billion de dollars canadiens d'ici le début des années 2030.[55] Cela s'ajoute à la tendance générale vers la numérisation dans l'ensemble des industries pour prendre en compte les défis soulevés par la pandémie de COVID-19.[56] L'adoption des TO connectées a été accélérée par des améliorations en technologie qui rendent plus facile la connexion de dispositifs à distance et à grande échelle; on peut penser notamment au réseau 5G et à l'infrastructure Internet par satellite. Bien que les TO connectées apportent de nombreux avantages, elles augmentent également la vulnérabilité des fournisseurs d'infrastructures essentielles à l'égard des activités de cybermenace.

Figure 6 : Compromission de TO par l'entremise de réseaux TI

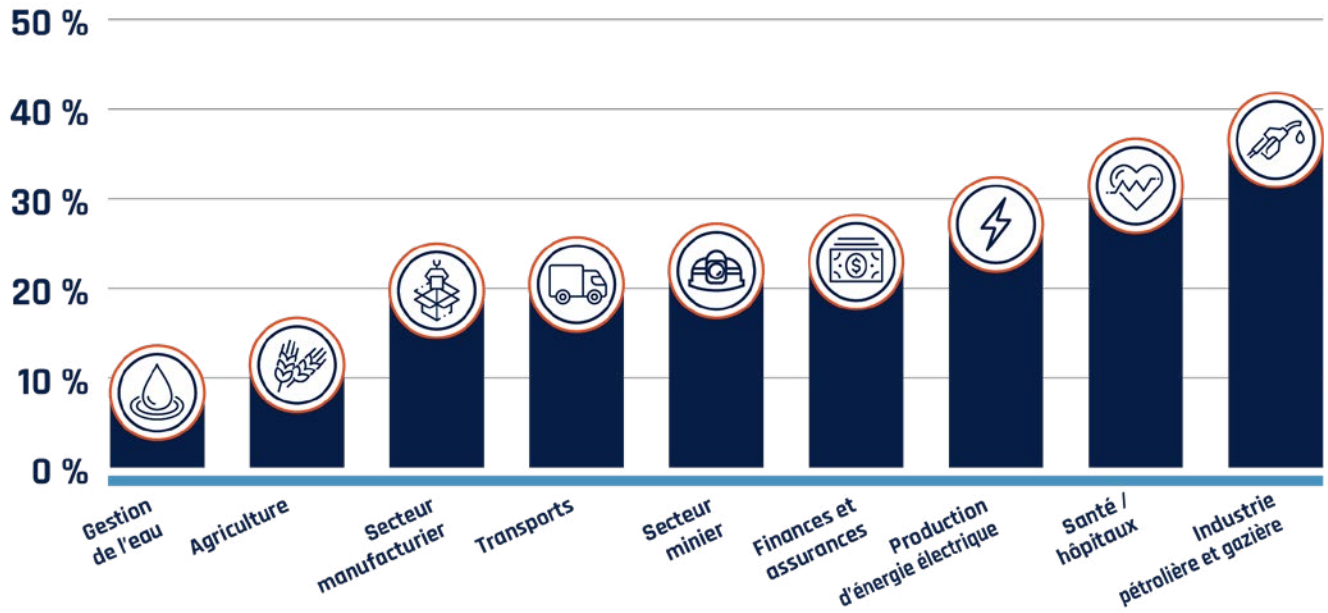


La connexion de TO à des réseaux TI connectés à Internet ouvre la voie aux auteurs de menace qui cherchent à accéder à des dispositifs et à des processus TO sensibles et à les perturber. Une menace visant un réseau TI peut avoir des effets indirects sur le réseau TO. Les opérateurs peuvent arrêter les processus TO par souci de prudence, car un maliciel peut accidentellement se propager et toucher les TO.[57] Nous observons également une augmentation de l'utilisation de maliciels qui ciblent et neutralisent directement les TO. Des cybercriminels ont déployé des rançongiciels propres aux TO, et des auteurs de menace parrainés par des États ont montré qu'ils étaient en mesure de déployer des maliciels ciblant les infrastructures essentielles pour dégrader leur rendement et endommager les actifs TO et TI.[58] Des auteurs de menace parrainés par des États russes ont été particulièrement actifs dans l'élaboration et les essais de ces capacités contre leurs voisins, y compris des pays membres de l'OTAN.[59]

Les infrastructures essentielles dépendent de leur chaîne d'approvisionnement

Les fournisseurs d'infrastructures essentielles, plus particulièrement dans les secteurs de l'énergie et des services publics, comptent sur l'expertise de leurs fournisseurs et fabricants ainsi que sur leur équipement pour exploiter, entretenir et moderniser leurs processus TO. Selon nos observations, cela les rend particulièrement vulnérables aux compromissions de la chaîne d'approvisionnement, alors que les auteurs de cybermenace commencent par compromettre un fournisseur et utilisent ensuite cet accès pour compromettre au moins un de ses clients. Les auteurs de cybermenace ciblent les chaînes d'approvisionnement des infrastructures essentielles pour deux raisons : voler la propriété intellectuelle et les renseignements concernant les TO déployées par un fournisseur d'infrastructures essentielles et obtenir un accès indirect aux réseaux.

Figure 7 : Pourcentage des secteurs des IE qui ont signalé un cyberincident (2019)[60]



Les cybercriminels ciblent les infrastructures essentielles

Les auteurs de cybermenace motivés par un intérêt financier exploitent principalement les infrastructures essentielles puisqu'ils savent que les temps d'arrêt peuvent nuire aux procédés industriels et aux clients qui dépendent du bon fonctionnement de ces infrastructures. Les activités de cybercriminalité visant les infrastructures essentielles peuvent provoquer l'interruption des activités qui prennent en charge les services essentiels, les services publics et la production de biens importants, notamment les aliments, le carburant et les équipements médicaux, pour soutenir leurs tentatives d'extorsion.

En particulier, pour le secteur de la santé, les répercussions de la cybercriminalité peuvent s'avérer considérables.[61] Depuis mars 2020, plus de 400 organismes de santé au Canada et aux États-Unis ont fait face à des attaques par rançongiciel.[62] En 2021, un cyberincident a fortement touché le système de santé de Terre-Neuve-et-Labrador, en perturbant les services médicaux de l'ensemble de la région sanitaire de l'Est.[63]

Nous avons également observé une augmentation des menaces visant les gouvernements municipaux et provinciaux.[64] Le Centre pour la cybersécurité a été informé de plus de 100 cas d'activités de cybermenace ciblant des municipalités canadiennes depuis le début de 2020. La plupart des cas impliquaient le piratage psychologique, un accès réseau non autorisé ou le déploiement de code malveillant, comme un rançongiciel. Des compromissions visant n'importe quel palier de gouvernement peuvent mettre en cause des renseignements personnels de citoyens, la continuité des services et la confiance dans les institutions compromises.[65]

COMPROMISSION DANS LE SECTEUR DE LA SANTÉ À TERRE-NEUVE-ET-LABRADOR

Le système de santé de Terre-Neuve-et-Labrador a été paralysé le 30 octobre 2021 à la suite de la compromission de ses réseaux. Cette compromission a été causée par des cybercriminels. Les professionnels de la santé étaient incapables d'avoir accès aux communications internes ou aux renseignements sur les diagnostics, ce qui les a obligés à adopter une approche axée sur le support papier pour gérer les rendez-vous et les interventions d'urgence. Des milliers d'interventions médicales et de rendez-vous médicaux ont été retardés. Outre les interruptions de services, les renseignements sensibles relatifs à des milliers de membres du personnel et de patients ont été volés.[66]

Des auteurs parrainés par des États ciblent les infrastructures essentielles

Des auteurs parrainés par des États ciblent les infrastructures essentielles pour recueillir des renseignements en menant des activités d'espionnage visant à se prépositionner en cas d'éventuelles hostilités et ils s'en servent comme moyen pour affirmer leur puissance et dans le but d'intimider. Dans des éditions précédentes de l'ECMN, nous avons noté qu'il était peu probable que des auteurs de menace parrainés par des États perturbent intentionnellement les infrastructures essentielles canadiennes. Selon nos observations, au cours des deux prochaines années, cette situation devrait demeurer la même en l'absence d'hostilités avec le Canada. L'invasion de l'Ukraine a démontré que la Russie est de plus en plus disposée à utiliser les cyberactivités contre les infrastructures essentielles pour exercer une influence politique étrangère. Le Centre pour la cybersécurité a publié des bulletins sur les cybermenaces en 2022 pour signaler l'existence de cybermenaces, notamment par des auteurs parrainés par la Russie, ayant pour cible les TO et les opérations des réseaux d'infrastructures essentielles canadiennes.[67]

Les activités de cybermenace parrainées par des États ont des répercussions sur les Canadiens

Selon nos observations, les cyberprogrammes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord continueront d'être les plus grandes cybermenaces stratégiques ciblant le Canada. Les activités de cybermenace parrainées par des États visant le Canada représentent une menace constante et continue qui sous-tend souvent des campagnes mondiales plus vastes qu'entreprennent ces États. Les campagnes ciblent le Canada pour diverses raisons, y compris en raison de son association avec des groupes tels l'OTAN et le G7. Tandis que les cyberactivités parrainées par des États ciblent directement le Canada, la forte connectivité du Canada à l'échelle mondiale et son intégration technologique avec ses alliés font également en sorte que son exposition aux menaces est également accrue. Les activités de cybermenace malveillantes parrainées par des États ont presque assurément des incidences sur les organisations et les citoyens canadiens, qu'ils soient ou non les cibles.

Des États étrangers ciblent les citoyens canadiens

Cibler des membres de la diaspora et des activistes au Canada

Des États rivaux veulent surveiller et perturber les activités des personnes qui, selon eux, menacent leur sécurité et leur stabilité nationales. Les auteurs de cybermenace parrainés par des États visent presque assurément des étrangers, des groupes de la diaspora, des activistes et des journalistes pour les surveiller et les contrôler. Ces activités sont susceptibles de menacer la sécurité des citoyens, en plus de renforcer la méfiance et la polarisation au sein de la société canadienne.

Selon nos observations, il est probable que des auteurs de menace aient recours à des cyberoutils contre ces populations au Canada. Ces activités prennent plusieurs formes, notamment la surveillance des contenus sur les applications basées à l'étranger, les activités permises par les médias sociaux et l'espionnage contre des personnes au moyen d'un logiciel espion. On considère que des auteurs de cybermenace parrainés par la Chine, l'Iran et l'Arabie Saoudite ont certainement dû surveiller des populations de la diaspora et des activistes à l'étranger en combinant ces moyens.[68] Selon nos observations, il est très probable que ces auteurs de cybermenace ciblent des citoyens au Canada.

Selon un rapport de The Citizen Lab de l'Université de Toronto, un organisme de recherche qui se spécialise dans la cybersécurité et les droits de la personne, des cybermenaces ciblent des activistes au Canada en ayant recours à la désinformation ou à l'intimidation sur les réseaux sociaux, à des attaques par déni de service contre des organisations et à la compromission de leurs dispositifs personnels.[69] Les espiogiciels qu'utilisent les auteurs de cybermenace pour compromettre un dispositif personnel peuvent s'avérer hautement sophistiqués; certains permettent l'accès à un dispositif personnel sans que son propriétaire ait à cliquer sur un lien malveillant ou à ouvrir une pièce jointe malveillante.[70]

Au-delà du recours à des activités de cybermenace contre des citoyens, il est fort probable que des pays utilisent des applications de messagerie et de médias sociaux étrangers populaires auprès de la diaspora au Canada et à travers le monde pour surveiller les communications. Des pays profitent de conditions d'utilisation permissives et de leurs propres pouvoirs législatifs pour forcer le partage de données.[71] Cette façon de faire menace la vie privée des communautés qui emploient ces applications.

LES SERVICES ET LES CYBEROUTILS COMMERCIAUX EN EXPANSION

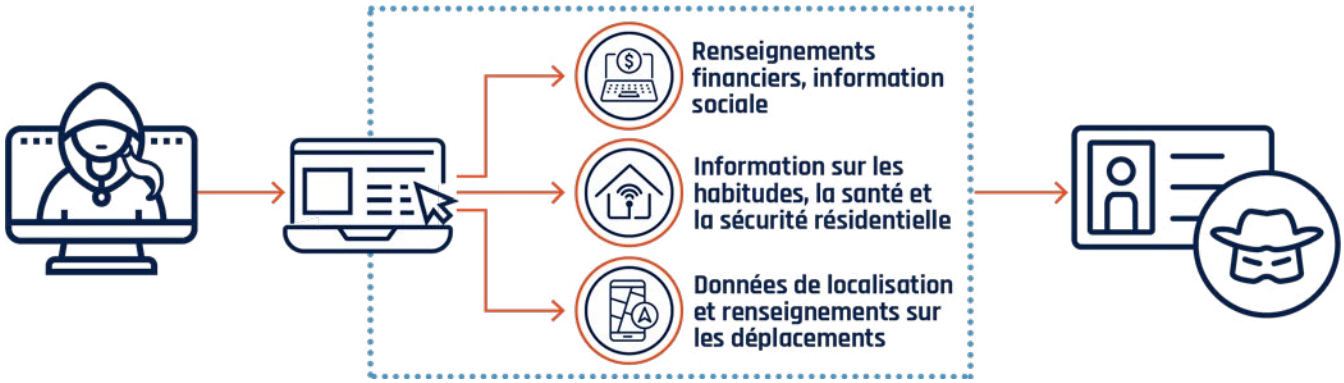
Les États-nations qui ne disposent pas de cybercapacités peuvent acheter des outils et des services auprès de fournisseurs commerciaux. Nous croyons que des gouvernements étrangers ont fort probablement tiré parti de logiciels commerciaux, comme l'espiogiciel Pegasus de l'entreprise NSO Group, dans le but de surveiller des dissidents, des activistes, des journalistes et des groupes de la diaspora. Il est fort probable que des gouvernements étrangers ont utilisé ces outils commerciaux contre des Canadiens et des groupes d'intérêt au Canada.

Cibler les renseignements personnels des Canadiens

Dans l'ECMN 2020, nous avons discuté de la façon dont les auteurs de cybermenace parrainés par des États ciblaient d'importantes bases de données de renseignements personnels et se servaient de la science des données pour identifier, faire le profil et suivre des personnes, pour ainsi permettre d'éventuelles activités de cybermenace. À mesure qu'augmente la quantité de renseignements personnels en ligne, les auteurs de menace ont plus de facilité à recueillir et à analyser ces renseignements. Lorsque des données sont transmises ou stockées sur un serveur se trouvant physiquement dans un pays étranger, il est plus facile pour ce pays d'obliger les organisations privées à fournir ces données, ce qui met en péril la vie privée des Canadiens.[72] Le caractère indissociable des technologies de communications et du traitement de données signifie que, sans mesures de protection adéquates, les renseignements personnels des Canadiens peuvent être compromis lorsque des auteurs de cybermenace compromettent des organisations étrangères.[73]

Figure 8 : Utilisation des grands ensembles de données et des renseignements personnels par les auteurs de cybermenace

Les services en ligne recueillent souvent les renseignements personnels des utilisateurs pour assurer la fonctionnalité des services. Lorsque des renseignements personnels sont exposés à la suite d'une atteinte à la protection des données ou lorsque ceux-ci ont été divulgués volontairement par l'utilisateur, les auteurs de cybermenace peuvent s'en servir pour faciliter le vol d'identité ou la fraude ciblée contre l'utilisateur.

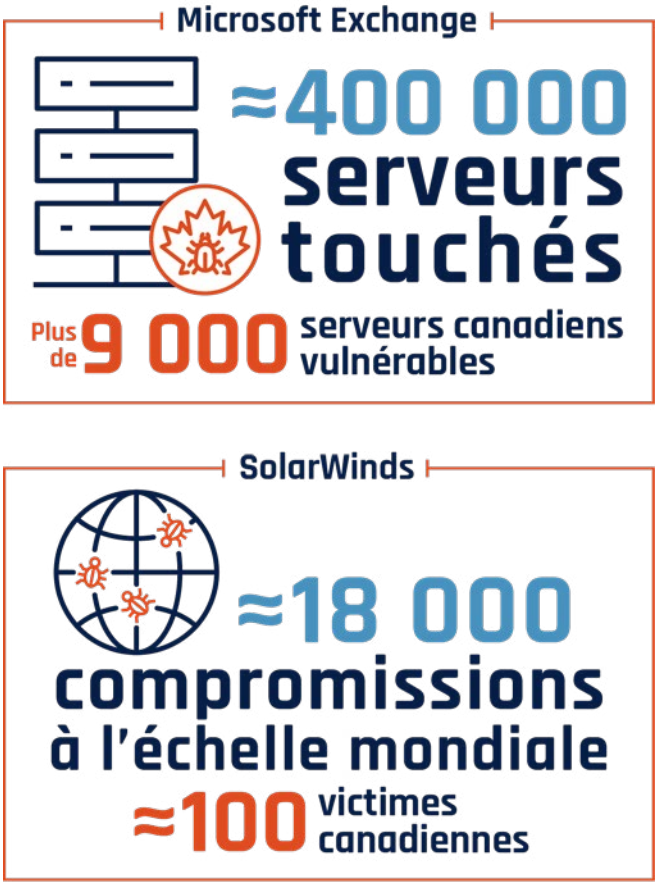


Les auteurs de menace parrainés par des États tentent de compromettre les Canadiens dans le cadre de vastes campagnes à l'échelle mondiale

Depuis la publication de l'ECMN 2020, nous avons observé que des auteurs de menace parrainés par des États exploitent des plateformes logicielles fréquemment utilisées pour cibler des milliers, voire des centaines de milliers de victimes à travers le monde. Nous remarquons de plus en plus que les auteurs de menace parrainés par des États tirent parti des vulnérabilités du jour zéro pour compromettre des victimes à grande échelle. En ciblant des vulnérabilités non signalées dans des systèmes fréquemment utilisés, les auteurs de menace arrivent à maximiser l'étendue de leurs victimes potentielles et à donner la priorité à celles qui possèdent des renseignements de valeur pour réaliser d'éventuelles cybermenaces. En mars 2021, des auteurs de cybermenace parrainés par la Chine ont compromis à l'échelle mondiale les serveurs Microsoft Exchange dans ce qui est très probablement un effort visant à voler la propriété intellectuelle et à obtenir des renseignements personnels. On évalue à 400 000 le nombre de serveurs dans le monde qui ont été touchés par cette attaque.[74] Bien qu'il soit difficile de déterminer exactement le nombre de compromissions, nous croyons que près de 9 000 serveurs canadiens ont probablement été vulnérables.

Selon nos observations, les auteurs de cybermenace parrainés par des États vont très certainement continuer à exploiter des victimes dans le cadre de cybercampagnes mondiales à grande échelle. Même si les organisations et les citoyens canadiens ne sont pas ciblés précisément, l'utilisation généralisée de technologies Internet et de logiciels courants par nos alliés et à l'échelle mondiale signifie que les Canadiens vont probablement être touchés par d'éventuelles campagnes de cette nature.

Figure 9 : Les Canadiens sont exposés à des cybercampagnes mondiales[75]



VULNÉRABILITÉS LOGICIELLES ET EXPLOITS

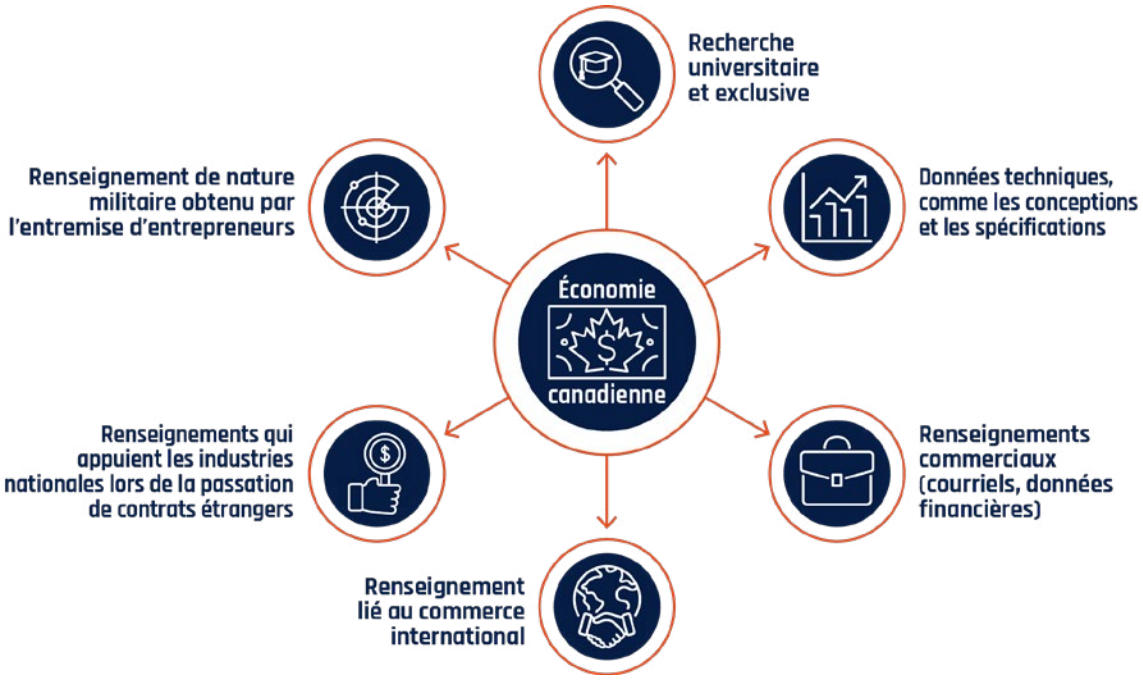
Les vulnérabilités logicielles sont des lacunes ou des défauts dans la conception, la mise en œuvre, l'exploitation ou la gestion d'un système de technologies de l'information, d'un dispositif ou d'un service qui peuvent fournir un accès aux auteurs de cybermenace. Les vulnérabilités du jour zéro sont des vulnérabilités qui sont inconnues du public ou du fournisseur de logiciels, ce qui signifie qu'aucun correctif n'est disponible. Un **exploit** est un code malveillant qui tire avantage d'une vulnérabilité non corrigée.

Des États ciblent la valeur économique du Canada

Des auteurs de menace parrainés par des États se livrent à de l'espionnage commercial et ciblent la propriété intellectuelle et d'autres renseignements commerciaux importants dans le but de partager les renseignements volés avec des entreprises appartenant à des États ou avec des industries nationales de leur pays d'origine. Le cyberespionnage commercial fait souvent partie d'un large éventail d'activités comprenant le vol de propriété intellectuelle, les opérations de renseignement étranger, l'acquisition d'équipement et de matériel discrets, et des violations du contrôle des exportations. Si elles sont fructueuses, ces activités peuvent entraîner une perte de revenus, une atteinte à la réputation et une perte d'investissements dans la recherche et le développement. On considère qu'au cours des deux prochaines années, les organisations canadiennes ayant des renseignements importants pouvant intéresser des États étrangers continueront assurément à être ciblées par des activités de cybermenace malveillantes provenant de criminels parrainés par des États.

Les auteurs de cybermenace parrainés par la Chine, la Russie, l'Iran et la Corée du Nord posent tous des menaces pour la sécurité des organisations canadiennes. Il est probable qu'au cours des deux prochaines années, ces États continueront de cibler des secteurs importants pour assurer leur propre développement économique national. Cela dit, la menace provenant de la Chine est très probablement la plus importante du point de vue du volume, de la capacité et de l'intention. Il est fort probable que les auteurs de cybermenace parrainés par la Chine continueront de cibler des industries et des technologies au Canada qui contribuent aux priorités stratégiques du pays.[76] En 2021, le Département de la Justice des États-Unis a déposé une mise en accusation contre des auteurs de cybermenace parrainés par la Chine qui ont ciblé la recherche en science et en technologie dans 12 pays, dont le Canada, entre 2011 et 2018. Les secteurs touchés comprennent les technologies maritimes, les vaccins et les traitements contre les virus, les technologies de l'information, l'aviation et la défense.[77] Les renseignements volés par les criminels étaient fort probablement destinés à appuyer les efforts de la Chine visant à obtenir des contrats étrangers pour ses entreprises d'État et pour ses propres programmes de recherche.

Figure 10 : Cibles d'intérêt pour l'espionnage



Des États cherchent à obtenir un gain financier par des moyens virtuels

En 2021 et 2022, nous avons observé des auteurs de cybermenace parrainés par des États mener des opérations à des fins de gains financiers. Leur objectif était certainement en partie d'atténuer l'impact des sanctions économiques mondiales. L'ingérence des États dans les activités de cybermenace motivées par l'appât du gain accroît la probabilité de voir des organisations et des citoyens canadiens être touchés par de telles activités étatiques. Par exemple, il est fort probable que des auteurs de cybermenace parrainés par la Corée du Nord continuent de cibler des institutions financières afin de générer des revenus au cours des deux prochaines années. Ces criminels nord-coréens ont ciblé des personnes et des organisations, y compris au Canada, en développant des applications commerciales malveillantes de cryptomonnaie pouvant servir à saisir les justificatifs d'identité des utilisateurs et à voler des fonds.[78]

Des États utilisent des activités et des outils de la cybercriminalité pour éviter l'attribution

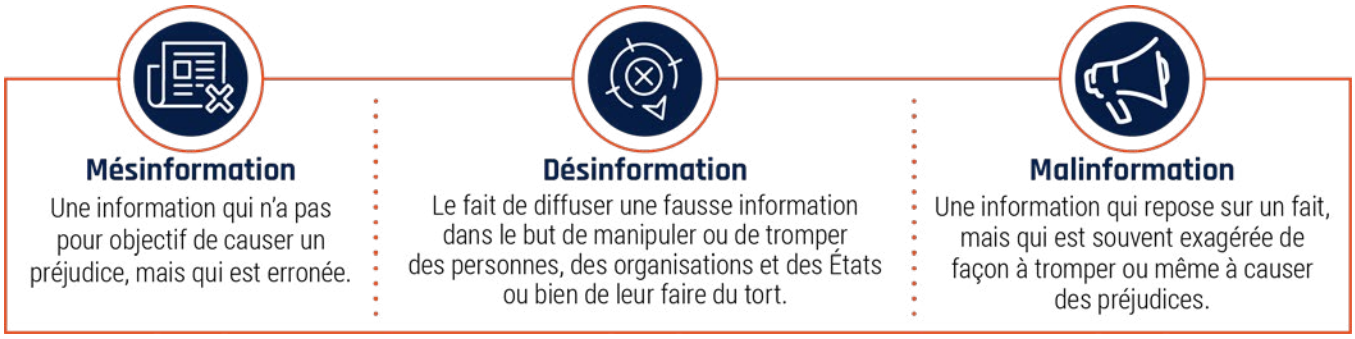
Des auteurs de menace parrainés par des États ont également eu recours à des activités associées à des cybercriminels pour atteindre des objectifs géopolitiques, notamment en perturbant des adversaires. Ils ont utilisé des rançongiciels pour perturber les opérations de leurs victimes et voler de précieux renseignements commerciaux, et recueillir des fonds à même le paiement d'une rançon. En adoptant les tactiques, les techniques et les procédures des cybercriminels, les auteurs de cybermenace parrainés par des États prennent les moyens nécessaires pour éviter de porter le blâme et pour cacher leurs activités. Par exemple, des auteurs de cybermenace parrainés par l'Iran ont déployé un rançongiciel contre des organisations au Moyen-Orient et aux États-Unis. Entre la fin de 2020 et 2021, des chercheurs ont identifié plusieurs auteurs de cybermenace iraniens qui ont déployé des rançongiciels. Généralement, ces attaques sont utilisées pour permettre des activités d'espionnage, et elles rapportent également des gains aux auteurs.[79]

Les auteurs de cybermenace tentent d'influencer les Canadiens et de briser la confiance accordée aux espaces virtuels

Internet constitue une source essentielle d'information pour les Canadiens. Depuis le début de la pandémie de COVID-19, 90 % des Canadiens ont consulté des sources en ligne pour rester bien informés des taux d'infection, des mesures de santé publique et du développement de vaccins.[80] L'intégrité de l'information que reçoivent les Canadiens des sources en ligne est importante. Elle contribue à leur faire prendre des décisions éclairées concernant les mesures de santé publique et des événements internationaux, et elle influence la façon dont ils prennent part aux processus démocratiques. La mésinformation, la désinformation et la malinformation (MDM, voir la figure 11) polluent l'espace d'information en ligne en propageant de l'information fausse et potentiellement nuisible, ce qui rend difficile pour les Canadiens de séparer la vérité des mensonges. Parmi les Canadiens qui ont cherché de l'information en ligne sur la COVID-19, 96 % ont déclaré avoir été exposés à du contenu qu'ils soupçonnaient d'être trompeur, faux et inexact.[81]

Il est possible que des personnes soient ciblées par des campagnes de MDM pour entraîner une atteinte à la réputation, ou elle peut servir à influencer des groupes plus importants. Certaines activités liées aux campagnes de MDM sont axées sur un événement, comme une élection ou un recensement, alors que d'autres sont des campagnes constantes. Des algorithmes de médias sociaux ont certes contribué à la circulation de MDM, et des efforts déployés par certaines plateformes de médias sociaux visant à modérer le contenu diffusé ont entraîné la création d'un marché pour de nouvelles plateformes fermées. Nous avons observé que le recours par les auteurs de cybermenace à un discours de MDM a évolué au cours des deux dernières années. Les technologies d'apprentissage automatique font en sorte qu'il est plus facile de créer de faux contenus et plus difficile de les différencier des contenus légitimes. Par ailleurs, les États-nations démontrent de plus en plus de capacité et de volonté envers l'utilisation de MDM pour défendre leurs intérêts géopolitiques. On considère que l'exposition des Canadiens aux campagnes de MDM devrait presque assurément augmenter au cours des deux prochaines années.

Figure 11 : Définitions de mésinformation, de désinformation et de malinformation [82]



Des auteurs de cybermenace tirent profit de la technologie pour diffuser la MDM et tromper les Canadiens

Les algorithmes amplifient la MDM

Le flux de l'information sur Internet est influencé par des algorithmes qui envoient aux utilisateurs du contenu ciblé et des messages publicitaires susceptibles de susciter un engagement. Le contenu MDM comporte souvent du texte à charge émotive et controversé qui semble avoir la cote pour susciter l'implication des utilisateurs.[83] À mesure que ces algorithmes s'adaptent au fil du temps pour prendre en compte les opinions et les préférences des gens, ils peuvent faciliter la propagation de MDM en les transmettant à ceux qui sont enclins à les croire.[84] Les auteurs de cybermenace profitent presque assurément des algorithmes de médias sociaux pour propager leurs messages. Il est aussi probable que ces auteurs tirent parti de voix légitimes sur les médias sociaux pour secrètement promouvoir leurs activités d'influence. Par exemple, en août 2021, une publication parue sur Facebook laissait entendre qu'une campagne d'influence liée à la Russie avait créé plusieurs faux comptes faisant la promotion de désinformation en lien à la vaccination pour la COVID-19, qui a ensuite été partagée par des influenceurs sur Instagram.[85]

Alors que de plus en plus de plateformes conventionnelles s'efforcent de retirer le contenu trompeur, des cas de MDM ont été signalés sur des plateformes de réseaux sociaux offrant à un auditoire restreint un espace pour permettre à des gens aux vues similaires d'interagir et de perpétuer des discours extrémistes. Par exemple, durant l'élection présidentielle américaine de 2020, des auteurs russes ont ciblé des utilisateurs américains d'extrême droite sur des applications comme Gab et Parler en menant une activité d'influence étrangère en ligne visant à promouvoir l'ancien président Donald Trump et à dénigrer celui qui était alors candidat à la présidence, Joe Biden.[86] Des applications de messagerie fermées principalement non modérées, comme Telegram, servent de plus en plus de tribune pour la distribution de contenu MDM.[87]

Le contenu synthétique remet en question toute information

Dans l'ECMN 2020 et la mise à jour 2021 de l'évaluation des Cybermenaces contre le processus démocratique du Canada,[88] nous avons décrit comment la technologie permettant de créer des vidéos par hypertrucage représentant des personnalités publiques ou des événements est devenue non seulement plus accessible aux auteurs de cybermenace, mais elle donne également des résultats plus convaincants. Nous avons continué d'observer à quel point la technologie qui se cache derrière l'hypertrucage avait évolué et pouvons témoigner de son utilisation dans le cadre d'importants événements sur la scène internationale. Lorsqu'il vise des personnes, le contenu synthétique est destiné à intimider et à porter atteinte à la réputation de ses victimes. Par exemple, la technologie de l'hypertrucage est utilisée pour cibler des politiciens et des journalistes, principalement des femmes, pour créer du contenu pornographique non consensuel dans le but de les discréditer.[89] Comme il devient plus difficile de différencier le contenu hypertruqué du contenu véritable, et compte tenu du fait que les outils servant à créer ces hypertrucages sont plus largement accessibles, il est fort probable que les auteurs de cybermenace continueront à intégrer cette technologie à leurs campagnes de MDM, ce qui leur permettra d'accroître la portée, l'ampleur et la crédibilité de leurs activités d'influence.

Le contenu synthétique augmente les campagnes de MDM en présentant une preuve visuelle appuyant des faussetés. Les générateurs de texte ont progressé à un tel point que le contenu qu'ils produisent est souvent quasi indéchiffrable du contenu légitime.[90] Il est toujours possible d'identifier les méthodes les plus courantes de production de vidéos hypertruquées et d'images synthétiques qui sont fausses et, dans certains cas, il est même facile de différencier le faux contenu du contenu réel. Toutefois, des exemples plus sophistiqués ont démontré une amélioration en matière de qualité, et ils sont plus difficiles à détecter.[91] Au cours de l'invasion de l'Ukraine par la Russie, nous avons remarqué que du contenu synthétique était distribué parallèlement à une campagne de désinformation concertée menée par la Russie.

INCIDENCE DISPROPORTIONNÉE DES HYPERTRUCAGES SUR LES FEMMES

Selon nos observations, il est probable que l'utilisation illicite des technologies d'hypertrucage a été dirigée vers des femmes qui courent un plus grand risque d'être dépeintes dans un contenu synthétique sexuellement explicite sans leur consentement. Des chercheurs estiment que 95 % de toutes les vidéos par hypertrucage sur Internet comportent de la pornographie synthétique non consensuelle et qu'environ 90 % de celles-ci représentent des femmes.[92] Certains des outils d'hypertrucage les plus populaires sont de nos jours des applications qui « déshabillent numériquement » des photos et produisent du matériel pornographique hypertruqué et personnalisé.[93]

Des auteurs étrangers utilisent une forme de MDM pour influencer le discours international

Nous avons décrit dans l'ECMN 2020 comment les activités d'influence étrangère en ligne sont devenues la nouvelle normalité, alors que des adversaires cherchent à influencer des élections et à avoir un impact sur le discours international en lien avec les événements actuels. Cette tendance se poursuit depuis 2020. Des nations adversaires font constamment circuler et amplifier des campagnes de MDM pour appuyer leurs intérêts entourant des événements importants comme l'invasion de l'Ukraine par la Russie. Selon nos observations, ces campagnes de MDM propagées par des auteurs de cybermenace parrainés par des États représentent une menace constante et persistante pour les Canadiens. La participation active du Canada au sein de la communauté internationale et en tant que membre d'organisations clés, comme l'OTAN et le G7, fait des Canadiens une cible pour les campagnes d'influence étrangère en ligne.

Bien que nous croyions que le Canada n'est pas particulièrement visé par les activités de MDM russes, la désinformation de la Russie cible malgré tout les pays de l'Ouest, et elle s'est ingérée, de façon opportune, dans des événements impliquant le Canada. En avril 2022, le CST a révélé que la Russie propageait des campagnes de MDM au sujet de membres des Forces armées canadiennes qui commettaient des crimes de guerre en Ukraine et qu'elle utilisait des images altérées pour renforcer ses faussetés au sujet de l'implication du Canada dans le conflit.[94] Dans le cadre d'une enquête en ligne menée auprès d'utilisateurs de médias sociaux canadiens, plus de la moitié des répondants ont déclaré avoir fait face à des campagnes de MDM en lien à l'invasion russe de l'Ukraine sur les médias sociaux.[95]

Les activités d'influence étrangère en ligne ciblent fort probablement également les minorités linguistiques et les communautés de la diaspora au Canada. Des auteurs de cybermenace parrainés par des États visent à influencer ces groupes dans le but de réduire au minimum la dissidence ou d'appuyer les politiques de leur pays d'origine.[96] Ces groupes interagissent souvent sur des plateformes semi-fermées et censurées en fonction de règlements restrictifs en matière de contenu, ce qui signifie que la mésinformation, la désinformation et la malinformation peuvent se propager plus facilement au sein de ces groupes.[97] Par exemple, WeChat, une application de médias sociaux de Chine utilisée par des milliards de personnes à travers le monde, a été utilisée pour diffuser des campagnes de MDM et de la propagande s'adressant spécifiquement à la diaspora chinoise.[98]

L'HYPERTRUCAGE ET L'INVASION RUSSE EN UKRAINE

L'invasion russe en Ukraine a impliqué une campagne soutenue de désinformation conçue pour créer de la confusion et affecter la perception de la communauté internationale à l'égard de la guerre. Le 16 mars 2022, une vidéo truquée circulait sur les plateformes de médias sociaux montrant le président ukrainien, Zelenskyy. L'hypertrucage montrait le président Zelenskyy demandant aux soldats ukrainiens de se livrer à la Russie.[99] Plus tôt en 2022, des auteurs inconnus se sont fait passer pour le maire de Kyiv et ont réussi à piéger plusieurs maires européens lors de téléconférences. Les participants aux appels n'avaient aucune idée que la personne à l'autre bout du fil était le produit d'un hypertrucage jusqu'à ce que le soi-disant maire de Kyiv commence à faire des commentaires douteux.[100]

Des technologies perturbatrices entraînent de nouvelles possibilités et menaces

Le développement rapide de la technologie offre de nombreuses perspectives à ceux qui savent créer, déployer et mettre en œuvre des innovations. Certains de ces développements peuvent s'avérer « perturbateurs » parce qu'ils modifient fondamentalement leur champ d'application, permettant ainsi des améliorations considérables par rapport aux technologies existantes ou à de nouvelles approches qui rendent les technologies en place obsolètes. Toutefois, la réglementation a souvent de la difficulté à rester au fait des développements technologiques de pointe, et les implications et les risques de leur adoption ne sont pas clairs, du moins initialement.

Tout comme des technologies évoluées peuvent venir appuyer des objectifs commerciaux publics, elles peuvent également être déployées de manière malveillante par des auteurs de menace dotés de moyens sophistiqués. La présente section traite de trois des tendances technologiques qui, selon nous, ont le potentiel de perturber leurs domaines respectifs : les actifs numériques et le système financier décentralisé, l'apprentissage automatique et l'informatique quantique. Bien que ces technologies en soient à diverses étapes de leur processus de développement et de réalisation, elles ont toutes des répercussions sur la prospérité économique du Canada et la sécurité nationale, ainsi que sur la sécurité des citoyens et la vie privée des Canadiens.

Des actifs numériques sont des cibles et des outils pour les auteurs de cybermenace

Depuis que les bitcoins sont devenus la première cryptomonnaie en 2008, le nombre de cryptomonnaies et la valeur des marchés de la cryptomonnaie ont explosé. Il existe maintenant plus de 10 000 différentes cryptomonnaies sur le marché. Le marché a atteint des sommets avec près de 3 billions de dollars américains durant la pandémie de COVID-19, avant de tomber sous la barre d'un billion de dollars au milieu de 2022, mais toujours à un niveau bien supérieur par rapport aux niveaux avant la COVID-19.[101] Les cryptomonnaies et les technologies de chaînes de blocs connexes ont contribué au développement d'un écosystème économique numérique, dans lequel les actifs numériques ont une valeur concrète. Un aspect émergent de ce système est la fonction de gestion financière décentralisée (DeFi pour *Decentralized Finance*), qui permet des emprunts et du financement à grande échelle sans passer par des intermédiaires. Ces activités se produisent sur des plateformes DeFi qui offrent une vaste gamme de services et sont une solution de rechange aux systèmes financiers centralisés traditionnels que l'on retrouve dans les banques et autres institutions financières.

Selon des analyses de fournisseurs, le vol de cryptomonnaie en 2021 a atteint une valeur de près de 3,2 milliards de dollars. Ces valeurs proviennent des échanges de cryptomonnaies et des plateformes DeFi.[102] Outre le fait de voler de la cryptomonnaie en ayant recours à la fraude, à des escroqueries et à des compromissions par portefeuille numérique, les auteurs de cybermenace se basent sur la cryptomonnaie pour payer des marchandises et des services illicites, pour recevoir des paiements provenant de victimes de rançongiciel et pour blanchir le produit d'actes criminels. Bien que les services policiers connaissent un certain succès lorsque vient le temps de retracer, et dans certains cas, de récupérer des sommes volées, les auteurs de cybermenace continuent de perfectionner et de développer des techniques pour masquer des transactions financières illicites, comme l'utilisation de mixeurs de cryptomonnaie ou de monnaies privées.[103] Selon nos observations, le blanchiment d'argent au moyen de cryptomonnaie continuera à faciliter la montée de la cybercriminalité et d'autres activités illicites, et cette pratique va également entraver la capacité des forces de l'ordre à retracer et à récupérer les sommes volées.

Figure 12 : Termes liés à la cryptomonnaie

Monnaie privée

Les cryptomonnaies comme le bitcoin fonctionnent sur une chaîne de blocs publique, ce qui signifie que tous les transferts et toutes les transactions sont publics. Des monnaies privées comme la cryptomonnaie Monero ont été spécialement conçues pour masquer les transactions et assurer l'anonymat des utilisateurs. Les auteurs de cybermenace trouvent les monnaies privées attrayantes, eux qui sont déterminés à ne pas être détectés pour qu'il soit difficile pour la police de suivre la circulation illicite de l'argent.[104]

Mixeurs

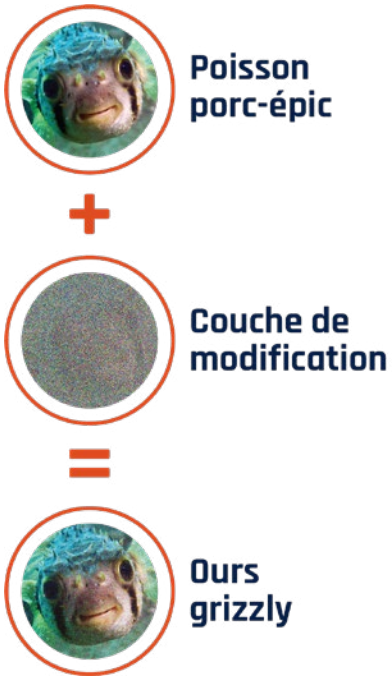
Les mixeurs permettent aux auteurs de cybermenace de dissimuler l'origine de la cryptomonnaie obtenue de manière illicite. Les mixeurs acceptent des cryptomonnaies des utilisateurs et les combinent dans un regroupement pour les « mixer » efficacement. Les utilisateurs retirent ensuite la valeur de leur dépôt du regroupement mélangé, moins des frais de service. On note une augmentation de l'utilisation de mixeurs. Leur valeur trimestrielle a dépassé le milliard de dollars américains à la fin de 2020, et la valeur est passée de 2 milliards de dollars à un peu plus de 3 milliards de dollars américains tous les trimestres depuis cette date. Cette augmentation a été entraînée par les fonds reçus de sources présumées illicites, ce qui, au cours du deuxième trimestre de 2022, a représenté près de 28 % de valeur, ou 700 millions de dollars américains, envoyés à des mixeurs.[105]

L'automatisation de l'apprentissage automatique peut être trompée et exploitée

L'apprentissage automatique est un sous-ensemble de l'intelligence artificielle qui se développe rapidement et qui occupe déjà une place omniprésente dans les services aux consommateurs et l'analyse de données. Les techniques liées à l'apprentissage automatique présentent un changement fondamental dans l'automatisation des tâches comme la reconnaissance d'image, la traduction de langue et la modération ou la conservation de contenus en ligne. Des chercheurs ont démontré plusieurs autres applications prometteuses relatives à l'apprentissage automatique pour l'avenir, notamment pour les véhicules autonomes et les diagnostics médicaux.[106] À mesure que l'apprentissage automatique s'intègre aux processus décisionnels et a des répercussions sociales et personnelles, une attention particulière sera nécessaire pour veiller à ce que son application soit équitable, objective et sécuritaire. Les applications axées sur l'apprentissage automatique comportent des vulnérabilités uniques comparativement aux programmations conventionnelles. Les auteurs de cybermenace peuvent exploiter celles-ci pour accroître l'exposition aux menaces des organisations qui les utilisent.

Les auteurs de cybermenace attaquent les modèles d'apprentissage automatique au moyen de techniques d'apprentissage automatique nuisible.[107] D'une manière générale, ces techniques exploitent les failles de la logique du modèle d'apprentissage automatique pour tromper le système ou le forcer à retourner de l'information non désirée et parfois confidentielle.

Figure 13 : Apprentissage automatique contradictoire dans la reconnaissance d'images



Tel qu'il est illustré dans la figure 13, les modèles d'apprentissage automatique par reconnaissance d'image peuvent être amenés par la ruse à identifier de façon erronée des objets en modifiant l'image. Certaines modifications sont invisibles pour l'œil humain, ce qui les rend difficiles à détecter.[108] Le même principe s'applique à d'autres applications d'apprentissage automatique, comme la détection de maliciel. En modifiant subtilement le code du maliciel de manière à confondre l'algorithme, les auteurs de cybermenace peuvent amener le logiciel de sécurité à faire une classification erronée en présentant le maliciel comme étant inoffensif. Selon nos observations, il est aussi fort probable que les auteurs de menace trompent les algorithmes d'apprentissage automatique pour faciliter une autre cyberactivité, comme la distribution de mésinformation et de campagnes de fraude par courriel à grande échelle.[109]

En indiquant au modèle d'apprentissage automatique des questions soigneusement élaborées, les auteurs de cybermenace peuvent être en mesure de déduire des renseignements à partir des données de formation.[110] Lorsque le modèle d'apprentissage automatique est appliqué au diagnostic médical ou à la protection contre la fraude, les données de formation peuvent comprendre des renseignements personnels sensibles, y compris des détails financiers sur un historique de santé. Une exposition de ces renseignements, ou de renseignements d'une personne dans le cadre des données de formation, peut servir à la conduite d'autres activités de menace sur mesure, comme des fraudes ou des escroqueries. Les renseignements personnels ainsi volés sont à risque d'une exposition ultérieure si ces renseignements devaient être vendus ou rendus publics.

L'informatique quantitative menace la cryptographie moderne

L'informatique quantique est une technologie émergente conçue pour contourner les limitations physiques de l'informatique conventionnelle par l'application de la physique quantique. Les ordinateurs quantiques menacent nos méthodes actuelles permettant d'assurer la cybersécurité des systèmes d'information et de protéger les données sensibles transmises par Internet. La cryptographie est utilisée pour protéger des données au moyen de problèmes mathématiques qui attestent la source et brouillent leur contenu pour en empêcher une lecture non intentionnelle. Sans la clé de déchiffrement, porter atteinte à la sécurité en résolvant le problème mathématique ne pourrait pas se faire dans un délai raisonnable avec des ordinateurs classiques. Toutefois, les problèmes mathématiques reposant sur les normes cryptographiques actuelles sont facilement exécutés par des ordinateurs quantiques. Des dispositifs quantiques suffisamment puissants pour percer la cryptographie moderne pourraient être offerts dès le début des années 2030. Il sera alors impossible de transmettre de manière sécuritaire de l'information sensible si des modifications à nos méthodes actuelles de cryptographie ne sont pas apportées.[111] Cependant, nous n'avons pas encore observé d'ordinateur quantique capable de terminer un problème offrant un avantage commercial qui ne pouvait pas également être terminé par des ordinateurs classiques.[112]

La cryptographie est essentielle pour les systèmes numériques courants de confiance qui nécessitent des transferts de données sensibles, comme des détails personnels ou des renseignements financiers. Nous croyons que le développement proactif et l'adoption d'une cryptographie post-quantique permettront de diminuer la menace qui pourrait éventuellement peser sur l'information et les communications si l'informatique quantique venait à offrir plus de capacités et devenait plus courante. Le Centre pour la cybersécurité a travaillé activement à l'élaboration d'une solution au défi quantique en collaborant avec le National Institute of Standards and Technology des États-Unis pour attester des normes en matière de cryptographie post-quantique.[113] Toutefois, les renseignements chiffrés qui ont été volés par des auteurs de menace aujourd'hui peuvent être conservés et déchiffrés lorsque des ordinateurs quantiques deviendront disponibles. Pour la plupart des Canadiens, il se peut que cette situation ne représente pas une menace importante; cependant, un vol de renseignements commerciaux et de données gouvernementales liées aux affaires étrangères ou à la sécurité nationale peut devenir un atout précieux ou entraîner une situation sensible ultérieurement.[114]

Conclusion

Le contexte des cybermenaces au Canada continue d'évoluer. Les Canadiens utilisent Internet couramment et pour accomplir un plus grand nombre de tâches. Plus il y a des dispositifs connectés à Internet, plus grande sera l'exposition aux cybermenaces. Les auteurs de cybermenace adaptent leurs activités et utilisent de nouvelles technologies pour réaliser leurs objectifs financiers, géopolitiques ou idéologiques.

Dans le cadre de cette Évaluation des cybermenaces nationales, nous avons établi des tendances relatives au contexte des cybermenaces et nous avons donné une vue d'ensemble de 5 thèmes qui vont continuer de dominer les activités de cybermenace au Canada au cours des deux prochaines années. Bien que la cybercriminalité demeure la menace la plus susceptible de toucher les Canadiens et les organisations canadiennes, les cybermenaces parrainées par des États entraînent aussi des répercussions sur les Canadiens. Les infrastructures essentielles risquent de plus en plus d'être visées par des activités de cybermenace émanant de cybercriminels et d'auteurs de menace parrainés par des États, tandis que des États-nations adaptent leur utilisation de la mésinformation, de la désinformation et de la malinformation dans le but d'influencer les Canadiens. Le contexte des cybermenaces évoluera certainement au cours des deux prochaines années, à mesure que des technologies comme les actifs numériques, l'apprentissage automatique et l'informatique quantique créent de nouvelles possibilités et de nouvelles menaces.

Un grand nombre de cybermenaces peuvent être atténuées grâce à la sensibilisation et à l'adoption de pratiques exemplaires en matière de sécurité et de continuité des activités. De nos jours, les cybermenaces et les opérations d'influence sont souvent fructueuses, car elles ne reposent pas uniquement sur les vulnérabilités technologiques, mais exploitent des habitudes sociales et des comportements humains profondément ancrés. Pour défendre le Canada contre les cybermenaces et les opérations d'influence connexes, il faut se pencher sur les aspects techniques et sociaux des activités de cybermenace. Des investissements en cybersécurité permettront aux Canadiens de bénéficier de nouvelles technologies tout en s'assurant de ne pas exposer indûment à des risques la sécurité, la vie privée, la prospérité économique et la sécurité nationale.

Le Centre pour la cybersécurité s'est engagé à faire avancer la cybersécurité et à accroître la confiance des Canadiens dans 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 invitons les lecteurs à consulter nos conseils sur la cybersécurité[115] pour obtenir de plus amples renseignements sur les cybermenaces et les tendances exposées dans le présent document.

Le Centre pour la cybersécurité a recours à une approche collaborative en matière de sécurité qui permet de combiner l'expertise du gouvernement, du secteur privé et du milieu universitaire. En travaillant ensemble, nous rendrons le Canada plus fort et plus résilient face aux cybermenaces.

Notes de fin de texte

1 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx

2 https://cyber.gc.ca/fr

3 https://twitter.com/CentreCyber_ca

4 https://cyber.gc.ca/fr/orientation

5 https://www.pensezcybersecurite.gc.ca/fr

6 https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2018

7 https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020

8 https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces

9 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx

10 https://cyber.gc.ca/fr/orientation

11 https://www.pensezcybersecurite.gc.ca/fr/homepage

12 https://www.cira.ca/fr/resources/letat-de-linternet/rapport/canadas-internet-factbook-2022

13 https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces

14 Statistique Canada. ***L'utilisation d'Internet à l'ère de la COVID-19 : la pandémie a incité les Canadiens à passer davantage de temps en ligne***, 24 juin 2021.
https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00027-fra.htm

15 Amazon Canada. ***OOO Until TBD? Majority of Canadian Office Workers Want Remote Work to Stay***, 10 mars 2020.
https://www.newswire.ca/news-releases/ooo-until-tbd-majority-of-canadian-office-workers-want-remote-work-to-stay-897250807.html

16 Kaspersky. ***COVID-19: Examining the threat landscape a year later***, 15 mars 2021.
https://securelist.com/covid-19-examining-the-threat-landscape-a-year-later/101154/

17 Microsoft. ***Microsoft Digital Defense Report***, octobre 2021.
https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

18 Statistique Canada. ***L'utilisation d'Internet et des technologies numériques par les Canadiens avant et pendant la pandémie de COVID-19***, 28 avril 2022.
https://www150.statcan.gc.ca/n1/pub/36-28-0001/2022004/article/00004-fra.htm

19 CBC News. ***Federal, Quebec governments to spend $826 million to expand high-speed internet***, 22 mars 2021.
https://www.cbc.ca/news/canada/montreal/trudeau-quebec-high-speed-internet-1.5959741
WHITE, Erik. ***Satellite internet a 'game changer' for rural and northern Ontario, but some say fibre should still come first.***
https://www.cbc.ca/news/canada/sudbury/starlink-satellite-internet-northern-ontario-1.6263474

20 Gouvernement du Canada. ***Les Villes Intelligentes et la Sécurité Nationale***, 16 février 2022.
https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/villes-intelligentes-la-securite-nationale/villes-intelligentes-la-securite-nationale.html

21 RUFFIO, Patricia. ***Dark Web Price Index 2022***, Privacy Affairs, 7 juillet 2022.
https://www.privacyaffairs.com/dark-web-price-index-2022/

22 Chainanalysis. ***The 2022 Crypto Crime Report***, février 2022.
https://go.chainalysis.com/2022-Crypto-Crime-Report.html
Digital Shadows. ***Initial Access Brokers Report***.
https://resources.digitalshadows.com/whitepapers-and-reports/initial-access-brokers-report?utm_source=blog&utm_medium=website&utm_campaign=initial_access_brokers_report

23 Chainanalysis. ***The 2022 Crypto Crime Report***, février 2022
https://go.chainalysis.com/2022-Crypto-Crime-Report.html

24 Centre canadien pour la cybersécurité. ***Alerte – Exploitation active de la vulnérabilité Apache Log4j – Mise à jour 7***, 29 décembre 2021.
https://www.cyber.gc.ca/fr/alertes-avis/exploitation-active-de-la-vulnerabilite-apache-log4j

25 TURUNEN, Ilkka. ***Log4shell by the numbers – Why did CVE-2021-44228 set the Internet on Fire?***, Sonatype, 14 décembre 2021.
https://blog.sonatype.com/why-did-log4shell-set-the-internet-on-fire

26 MENACHE, Shachar, Or PELES et Ori HOLLANDER. ***Log4j Log4Shell 0-Day Vulnerability: All You Need to Know***, JFrog, 28 décembre 2021.
https://jfrog.com/blog/log4shell-0-day-vulnerability-all-you-need-to-know/

27 Compte Twitter officiel du CST @cse_cst, avril 2022.
https://twitter.com/cst_cse
NIMMO, Ben, Ira HUBERT et Yang CHENG. ***Spamouflage Breakout***, Graphika, février 2021.
https://graphika.com/reports/spamouflage-breakout/

28 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

29 Compte Twitter officiel du CST @cse_cst, avril 2022.
https://twitter.com/cst_cse

30 DIAZ HERNANDEZ, Marianne, et coll. ***Internet shutdowns in 2021: the return of digital authoritarianism***, AccessNow, 28 avril 2022.
https://www.accessnow.org/internet-shutdowns-2021/

31 Freedom House. ***Freedom on the Net 2021***.
https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

32 Flashpoint. ***Understanding Russia's, 'Sovereign Internet': What Happens if Russia Isolates Itself from the Global Internet***, 11 mars 2022.
https://flashpoint.io/blog/russian-runet-sovereign-internet/

33 Yahoo Finance. ***China's World Internet Conference goes 'international' as Beijing seeks to promote its own vision of global cyberspace***, 13 juillet 2022.
https://finance.yahoo.com/news/chinas-world-internet-conference-goes-093000698.html

34 Centre antifraude du Canada. ***Répercussions de la fraude depuis le début de l'année***, mise à jour du 30 juin 2022.
https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

35 SEALS, Sara. ***Ransomware Volumes Hit Record Highs as 2021 Wears On***, Threat Post, 3 août 2021.
https://threatpost.com/ransomware-volumes-record-highs-2021/168327/
Sophos. ***Ransomware hit 66% of Organizations Surveyed for Sophos' Annual 'State of Ransomware 2022'***, 27 avril 2022.
https://www.sophos.com/en-us/press-office/press-releases/2022/04/ransomware-hit-66-percent-of-organizations-surveyed-for-sophos-annual-state-of-ransomware-2022
ABRAMS, Lawrence. ***Computer giant Acer hit by $50 million ransomware attack***, Bleeping Computer, 19 mars 2021.
https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/

36 TELUS. ***Étude de TELUS sur les rançongiciels***, 2022.
https://www.telus.com/fr/bc/business/ransomware-study?INTCMP=VAN_ransomwarestudy

37 Recorded Future. ***The Business of Fraud: Sales of PII and PHI***, 17 février 2021.
https://go.recordedfuture.com/hubfs/reports/cta-2022-0217.pdf
Mandiant. ***1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information***, 31 janvier 2022.
https://www.mandiant.com/resources/ransomware-extortion-ot-docs

38 GREIG, Jonathan. ***Canadian fighter jet training company investigating ransomware attack***, The Record, 11 mai 2022.
https://therecord.media/top-aces-ransomware-attack-lockbit/

39 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/
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

40 Humber River Hospital. ***Code Grey Update***, 15 juin 2021.
https://www.hrh.ca/2021/06/15/code-grey/
VELLA, Erica. ***Toronto's Humber River Hospital under code grey after ransomware attack***, Global News, 18 juin 2021.
https://globalnews.ca/news/7963652/humber-river-hospital-ransomware-attack-toronto/
Toronto Transit Commission. ***TTC provides update on cybersecurity incident***, 8 novembre 2021.
https://www.ttc.ca/news/2021/November/TTC-provides-update-on-cyber-security-incident
CBC News. ***Toronto transit system hit by ransomware attack, TTC says no significant disruptions***, 29 octobre 2021.
https://www.cbc.ca/news/canada/toronto/ttc-ransomware-attack-1.6231349

41 MEHROTRA, Kartikay, et William TURTON. ***CNA Financial Paid $40 Million in Ransom After March Cyberattack***, Bloomberg, 20 mai 2021.
https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

42 TELUS. ***Étude de TELUS sur les rançongiciels***, 2022.
https://www.telus.com/fr/bc/business/ransomware-study?INTCMP=VAN_ransomwarestudy

43 Coveware. ***Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022***, 28 juillet 2020.
https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

44 ESET Digital Security. ***Threat Report T1 2022***, 2022.
https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

45 Palo Alto Networks. ***2021 Palo Alto Networks Canada Ransomware Barometer***, 2 juin 2021.
https://www.paloaltonetworks.ca/apps/pan/public/downloadResource?pagePath=/content/pan/en_CA/resources/research/2021-palo-alto-networks-canada-ransomware-barometer

46 Financial Times. ***Monero emerges as crypto of choice for cybercriminals***, 22 juin 2021.
https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6

47 Malwarebytes Labs. ***Updated: Kaseya hijacked, thousands attacked by REvil, fix delayed again***, 7 juillet 2021.
https://blog.malwarebytes.com/cybercrime/2021/07/shutdown-kaseya-vsa-servers-now-amidst-cascading-revil-attack-against-msps-clients/#thousands-affected

48 ABRAMS, Lawrence. ***Ransomware gang plans to call victim's business partners about attacks***, Bleeping Computer, 6 mars 2021.
https://www.bleepingcomputer.com/news/security/ransomware-gang-plans-to-call-victims-business-partners-about-attacks/

49 United States Government. ***Indicators of Compromise Associated with AvosLocker Ransomware***, 17 mars 2022.
https://www.ic3.gov/Media/News/2022/220318.pdf

50 LYONS HARDCASTLE, Jessica. ***FBI, CISA: Don't get caught in Karakurt's extortion web***, The Register, 3 juin 2022.
https://www.theregister.com/2022/06/03/fbi_cisa_warn_karakurt_extortion/

51 Rogers. ***An updated message from Jorge Fernandes, Chief Technology Officer at Rogers***, 19 avril 2021.
https://about.rogers.com/news-ideas/a-message-from-jorge-fernandes-chief-technology-officer-at-rogers/
Rogers. ***An Update from Rogers President and CEO***, 13 juillet 2022.
https://about.rogers.com/news-ideas/an-update-from-rogers-president-and-ceo/
EVANS, Pete. ***What happened at Rogers? Day-long outage is over, but questions remain***, CBC News, 20 avril 2021.
https://www.cbc.ca/news/business/rogers-outage-analysis-1.5994851
MAJOR, Darren. ***Ottawa calls on telecom companies to shore up networks after Rogers outage***, CBC News, 11 juillet 2022.
https://www.cbc.ca/news/politics/ottawa-demanding-improve-network-rogers-outage-1.6516970

52 ABRAMS, Lawrence. ***Massive Rogers outage disrupts mobile service, payments in Canada***, Bleeping Computer, 8 juillet 2022.
https://www.bleepingcomputer.com/news/technology/massive-rogers-outage-disrupts-mobile-service-payments-in-canada/

53 ZAFRA, Daniel, et coll. ***1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information***, Mandiant, 31 janvier 2022.
https://www.mandiant.com/resources/ransomware-extortion-ot-docs

54 Sécurité publique Canada. ***Stratégie nationale sur les infrastructures essentielles***, 10 novembre 2011.
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-fr.aspx

55 PLACEK, Martin. ***Industrial IoT – market size worldwide 2022-2028***, Statista, 14 mars 2022.
https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/
GlobeNewswire. ***Industrial IoT Market to reach US$ 1.3 Tn by 2032 - Comprehensive Research Report by FMI***, 6 avril 2022.
https://www.globenewswire.com/en/news-release/2022/04/07/2418081/0/en/Industrial-IoT-Market-to-reach-US-1-3-Tn-by-2032-Comprehensive-Research-Report-by-FMI.html

56 McKinsey & Company. ***How COVID-19 has pushed companies over the technology tipping point—and transformed business forever***, 5 octobre 2020.
https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

57 SANGER, David, Clifford KRAUSS et Nicole PERLROTH. ***Cyberattack Forces a Shutdown of a Top U.S. Pipeline***, The New York Times, 13 mai 2021.
https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
Centre de la sécurité des télécommunications. ***Déclaration du CST concernant l'affaire du maliciel NotPetya***, 15 février 2018.
https://cse-cst.gc.ca/fr/ressources-et-information/nouvelles/declaration-du-cst-concernant-laffaire-du-maliciel-notpetya;
GREENBERG, Andy. ***The Untold Story of NotPetya, the Most Devastating Cyberattack in History***, Wired, 22 août 2018.
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

58 BRUBAKER, Nathan, et coll. ***Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families***, Mandiant, 15 juillet 2020.
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot

59 Cybersecurity and Infrastructure Security Agency. ***Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure***, 20 avril 2022.
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

60 Statistique Canada. ***Tableau 22-10-0076-01 Types d'incidents de cybersécurité touchant les entreprises par industrie et taille de l'entreprise***.
https://www150.statcan.gc.ca/t1/tbl1/fr/cv.action?pid=2210007601&request_locale=fr

61 POULSEN, Kevin, Robert MCMILLAN et Melanie EVANS. ***A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death***, Wall Street Journal, 30 septembre 2021.
https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

62 DREES, Jackie. ***Meet the ransomware gang behind 235 attacks on US hospitals: 7 things to know, Becker's Health IT***, 10 juin 2021.
https://www.beckershospitalreview.com/cybersecurity/meet-the-ransomware-gang-behind-235-attacks-on-us-hospitals-7-things-to-know.html
POULSEN, Kevin et Melanie EVANS. ***The Ruthless Hackers Behind Ransomware Attacks on U.S. Hospitals: 'They Do Not Care'***, Wall Street Journal, 10 juin 2021.
https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215

63 Newfoundland and Labrador Health and Community Services. ***Information and Updates on Cyber Incident***, 30 mars 2022.
https://www.gov.nl.ca/hcs/information-and-updates-on-cyber-incident/
SMELLIE, Sarah. ***N.L. rebuilding systems downed by cyberattack from scratch, Eastern Health says***, CBC News, 16 décembre 2021.
https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cp-cyberattack-rebuilding-1.6287934

64 Elgin County. ***Information Privacy***, 13 mai 2022.
https://www.elgincounty.ca/services/privacy-information/
TREVITHICK, Matthew. ***Sensitive personal data among thousands of files exposed in Elgin Cybersecurity incident: Gonyou***, Global News, 16 mai 2022.
https://globalnews.ca/news/8838788/personal-data-files-elgin-cybersecurity-exposure/

65 Packetlabs. ***Are Municipal Cyber Attacks Threatening Citizens' Privacy?***, 13 décembre 2021.
https://www.packetlabs.net/posts/municipal-cyber-attacks/

66 SOLOMON, Howard. ***Newfoundland and Labrador health system attackers copied 200,000 patient and employee files***, IT World Canada, 31 mars 2022.
https://www.itworldcanada.com/article/newfoundland-and-labrador-health-system-attackers-copied-200000-patient-and-employee-files/478645

67 Centre canadien pour la cybersécurité. ***Bulletin sur les cybermenaces : Le CCC exhorte les exploitants des infrastructures essentielles du Canada à prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et à prendre des mesures d'atténuation contre celles-ci***, 26 janvier 2022.
https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-le-ccc-exhorte-les-exploitants-des-infrastructures
Centre canadien pour la cybersécurité. ***Bulletin sur les cybermenaces : Le CCC rappelle aux exploitants des infrastructures essentielles du Canada de prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et de prendre des mesures d'atténuation contre celles-ci***, 13 février 2022.
https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-le-ccc-rappelle-aux-exploitants-des-infrastructures

68 Check Point Research. ***Rampant Kitten – An Iranian Espionage Campaign***, 18 septembre 2020.
https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/
Département de la Justice des États-Unis. ***Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election***, 18 novembre 2021.
https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed
The Citizen Lab. ***The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil***, 1er octobre 2018.
https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/
The Citizen Lab. ***WeChat Surveillance Explained***, 7 mai 2020.
https://citizenlab.ca/2020/05/wechat-surveillance-explained/

69 The Citizen Lab. ***Psychological and Emotional War: Digital Transnational Repression in Canada***, 1er mars 2022.
https://tspace.library.utoronto.ca/bitstream/1807/120575/1/Report%23151--dtr_022822_lowres.pdf

70 The Citizen Lab. ***The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit***, 20 décembre 2020.
https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

71 Australian Strategic Policy Institute. ***TikTok and WeChat: Curating and controlling global information flows***, septembre 2020.
https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHImPVE_6KKcBP1JRD5fRnAVTZ=
The Citizen Lab. ***We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus***, 7 mai 2020.
https://citizenlab.ca/2020/05/we-chat-they-watch/

72 Australian Strategic Policy Institute. ***TikTok and WeChat: Curating and controlling global information flows***, septembre 2020.
https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHImPVE_6KKcBP1JRD5fRnAVTZ=

73 Commissariat à la protection de la vie privée du Canada. ***Enquête sur la conformité d'Equifax Inc. et d'Equifax Canada à la LPRPDE à la suite de l'atteinte à la sécurité des renseignements personnels en 2017***, 9 avril 2019.
https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lprpde-2019-001/
Département de la Justice des États-Unis. ***Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax***, 10 février 2020.
https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

74 Affaires mondiales Canada. ***Déclaration sur les campagnes cybernétiques de la Chine***, 19 juillet 2021.
https://www.canada.ca/fr/affaires-mondiales/nouvelles/2021/07/declaration-sur-les-campagnes-cybernetiques-de-la-chine.html

75 Affaires mondiales Canada. ***Déclaration sur les campagnes cybernétiques de la Chine***, 19 juillet 2021.
https://www.canada.ca/fr/affaires-mondiales/nouvelles/2021/07/declaration-sur-les-campagnes-cybernetiques-de-la-chine.html
Affaires mondiales Canada. ***Déclaration sur la cybercompromission de SolarWinds***, 15 avril 2021.
https://www.canada.ca/fr/affaires-mondiales/nouvelles/2021/04/declaration-sur-la-cybercompromission-de-solarwinds.html
GOODIN, Dan. ***SolarWinds hackers breach new victims, including a Microsoft support agent***, ArsTechnica, 26 juin 2021.
https://arstechnica.com/gadgets/2021/06/solarwinds-hackers-breach-new-victims-including-a-microsoft-support-agent/

76 Cybersecurity and Infrastructure Security Agency. ***Potential for China Cyber Response to Heightened U.S. – China Tensions***, 1er octobre 2020.
https://www.cisa.gov/uscert/ncas/alerts/aa20-275a

77 Département de la Justice des États-Unis. ***Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research***, 19 juillet 2021.
https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

78 Cybersecurity and Infrastructure Security Agency. ***AppleJeus: Analysis of North Korea's Cryptocurrency Malware***, 17 février 2021.
https://www.cisa.gov/uscert/ncas/alerts/aa21-048a

79 GATLAN, Sergiu. ***Iranian nation-state hackers linked to Pay2Key ransomware, Bleeping Computer***, 17 décembre 2020.
https://www.bleepingcomputer.com/news/security/iranian-nation-state-hackers-linked-to-pay2key-ransomware/
Microsoft Threat Intelligence Center. ***Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021***, 16 novembre 2021.
https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

80 Statistique Canada. ***La désinformation pendant la pandémie de COVID-19***, 2 février 2021.
https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00003-fra.htm
KEMP, Simon. ***Digital 2021 Canada***, 9 février 2021.
https://datareportal.com/reports/digital-2021-canada

81 Statistique Canada. ***La désinformation pendant la pandémie de COVID-19***, 2 février 2021.
https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00003-fra.htm
KEMP, Simon. ***Digital 2021 Canada***, 9 février 2021.
https://datareportal.com/reports/digital-2021-canada

82 Centre canadien pour la cybersécurité. ***Repérer les cas de mésinformation, désinformation et malinformation (ITSAP.00.300)***, février 2022. https://cyber.gc.ca/fr/orientation/reperer-les-cas-de-mesinformation-desinformation-et-malinformation-itsap00300

83 MESEROLE, Chris. ***How misinformation spreads on social media—And what to do about it***, Brookings Institute, 9 mai 2018. https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it/

84 FOURNIER, Jim. ***How algorithms are amplifying misinformation and driving a wedge between people***, The Hill, 10 novembre 2021. https://thehill.com/changing-america/opinion/581002-how-algorithms-are-amplifying-misinformation-and-driving-a-wedge/

85 Meta. ***July 2021 Coordinated Inauthentic Behaviour Report***, 10 août 2021. https://about.fb.com/news/2021/08/july-2021-coordinated-inauthentic-behavior-report/
CULLIFORD, Elizabeth. ***Facebook removes Russian networks that targeted influences to peddle anti-vax messages***, Reuters, 10 août 2021. https://www.reuters.com/technology/facebook-removes-russian-network-that-targeted-influencers-peddle-anti-vax-2021-08-10/

86 Graphika. ***Step into My Parler***, 1er octobre 2020. https://graphika.com/reports/step-into-my-parler/

87 TIMBERG, Craig, et Elizabeth DWOSKIN. ***With Trump gone, QAnon groups focus fury on attacking coronavirus vaccines***, The Washington Post, 11 mars 2021. https://www.washingtonpost.com/technology/2021/03/11/with-trump-gone-qanon-groups-focus-fury-attacking-covid-vaccines/
HERASIMENKA, Aliaksandr, et coll. ***Misinformation and professional news on largely unmoderated platforms: the case of telegram***, Journal of Information Technology and Politics, 25 mai 2022. https://www.tandfonline.com/doi/full/10.1080/19331681.2022.2076272

88 https://cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

89 PRATAP, Aayushi. ***Deepfake Epidemic Is Looming—And Adobe Is Preparing For The Worst***, Forbes, 29 juin 2022. https://www.forbes.com/sites/aayushipratap/2022/06/29/deepfake-epidemic-is-looming-and-adobe-is-preparing-for-the-worst/?sh=4cdf6ea5b81d

90 NGUYEN, Thanh, et coll. ***Deep Learning for Deepfakes Creation and Detection: A Survey***, arXiv, 25 septembre 2019. https://arxiv.org/abs/1909.11573v2?utm_campaign=AI%20Scholar%20Weekly%20&utm_medium=email&utm_source=Revue%20newsletter

91 NGUYEN, Thanh, et coll. ***Deep Learning for Deepfakes Creation and Detection: A Survey***, arXiv, 25 septembre 2019. https://arxiv.org/abs/1909.11573v2?utm_campaign=AI%20Scholar%20Weekly%20&utm_medium=email&utm_source=Revue%20newsletter

92 BERCZYK, Franziska. ***Deepfake porn is ruining women's lives. Now the law may finally ban it***, MIT Technology Review, 12 février 2021. https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/amp/?utm_medium=search&utm_source=google&utm_campaign=BL-ACQ-DYN&utm_content=categories&gclid=CjwKCAjwo_KXBhAaEiwA2RZ8hI3MIiDJNuYcDe5BcDr55qfUagpguO6PJgFTTIZBIfz6NfZ_V8KuSxoC5KMQAvD_BwE

93 HAO, Karen. ***A deepfake bot is being used to "undress" underage girls***, MIT Technology Review, 20 octobre 2020. https://www.technologyreview.com/2020/10/20/1010789/ai-deepfake-bot-undresses-women-and-underage-girls/

94 Compte Twitter officiel du CST @cse_cst, avril 2022. https://twitter.com/cst_cse

95 MAI, Philip, et coll. ***Russian propaganda is making inroads with right-wing Canadians***, The Conversation, 17 juillet 2022. https://theconversation.com/russian-propaganda-is-making-inroads-with-right-wing-canadians-186952

96 Mécanisme de réponse rapide du G7. ***Rapport annuel 2021***, 2021. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2021-annual-report-rapport-annuel.aspx?lang=fra

97 CHAN, Esther, et Stevie ZHANG. ***Disinformation, stigma and Chinese diaspora: policy guidance for Australia***, First Draft News, 31 août 2021.
https://firstdraftnews.org/long-form-article/disinformation-stigma-and-chinese-diaspora-policy-guidance-for-australia/
KENYON, Miles. ***WeChat Surveillance Explained***, Citizen Lab, 7 mai 2020.
https://citizenlab.ca/2020/05/wechat-surveillance-explained/

98 HONG, Nicole. ***WeChat, Wild Rumors and All, Is Their Lifeline. Washington May End That***, The New York Times, 5 octobre 2020.
https://www.nytimes.com/2020/10/05/nyregion/us-wechat-ban.html
MOZUR, Paul. ***Forget TikTok, China's Powerhouse App is WeChat, and Its Power Is Sweeping***, The New York Times, 4 septembre 2020.
https://www.nytimes.com/2020/09/04/technology/wechat-china-united-states.html
FITZGERALD RODRIGUEZ, Joe, Shannon LIN et Jessica HUSEMAN. ***Misinformation Image on WeChat Attempts to Frighten Chinese Americans Out of Voting***, ProPublica, 2 novembre 2020.
https://www.propublica.org/article/misinformation-image-on-wechat-attempts-to-frighten-chinese-americans-out-of-voting
WANG, Yaqiu. ***WeChat Is a Trap for China's Diaspora***, Human Rights Watch, 14 août 2020
https://www.hrw.org/news/2020/08/14/wechat-trap-chinas-diaspora
WHALEN, Jeanne. ***Chinese censorship invades the U.S. via WeChat***, Washington Post, 7 janvier 2021.
https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban/

99 ALLYN, Bobby. ***Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn***, NPR, 16 mars 2022.
https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia

100 OLTERMANN, Philip. ***European politicians duped into deepfake video calls with mayor of Kyiv***, The Guardian, 25 juin 2022.
https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko

101 CoinMarketCap. ***Global Cryptocurrency Charts; Total Cryptocurrency Market Cap***, récupéré le 16 août 2022.
https://coinmarketcap.com/charts/
DE BEST, Reynor. ***Quantity of cryptocurrencies as of February 3, 2022***, Statista, 22 mars 2022.
https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

102 Chainanalysis. ***The 2022 Crypto Crime Report***, février 2022.
https://go.chainalysis.com/2022-Crypto-Crime-Report.html

103 BUNGE, Jacob. ***JBS Paid $11 Million to Resolve Ransomware Attack***, Wall Street Journal, 9 juin 2021.
https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781
Département de la Justice. ***Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency***, 8 février 2022.
https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

104 CLARCK, Richard, Sarah KREPS et Adi RAO. ***Shifting crypto landscape threatens crime investigations and sanctions***, Brookings Institute, 7 mars 2022.
https://www.brookings.edu/techstream/shifting-crypto-landscape-threatens-crime-investigations-and-sanctions/

105 Chainalysis. ***Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume***, 14 juillet 2022.
https://blog.chainalysis.com/reports/cryptocurrency-mixers/

106 ZEWE, Adam. ***Anticipating others' behaviour on the road***, MIT News, 21 avril 2022.
https://news.mit.edu/2022/machine-learning-anticipating-behavior-cars-0421
AHSAN, Manjurul, Shahana LUNA et Zahed SIDDIQUE. ***Machine-Learning Based Disease Diagnosis: A Comprehensive Review,*** Healthcare, 15 mars 2022.
https://doi.org/10.3390/healthcare10030541

107 Microsoft. ***The 2021 Microsoft Digital Defence Report***, Microsoft (octobre 2021) à la page 43.
https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

108 MACHADO, Gabriel, Eugênio SILVA et Ronaldo GOLDSCHMIDT. ***Adversarial Machine Learning in Image Classification: A Survey Towards the Defender's Perspective***, arXiv, 8 septembre 2020.
https://arxiv.org/abs/2009.03728

109 HAY NEWMAN, Lily. ***AI Wrote Better Phishing Emails Than Humans in a Recent Test***, Wired, 7 août 2021.
https://www.wired.com/story/ai-phishing-emails/

110 HU, Hailong, et Jun PANG. ***Stealing Machine Learning Models: Attacks and Countermeasures for Generative Adversarial Networks***, ACSAC '21: Annual Computer Security Applications Conference, décembre 2021.
https://dl.acm.org/doi/10.1145/3485832.3485838

111 Centre canadien pour la cybersécurité. ***Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie (ITSAP.00.017)***, février 2021.
https://cyber.gc.ca/fr/orientation/preparez-votre-organisation-la-menace-que-pose-linformatique-quantique-pour-la

112 McKinsey & Company. ***Quantum computing: An emerging ecosystem and industry use cases***, décembre 2021.
https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20use%20cases%20are%20getting%20real%20what%20you%20need%20to%20know/quantum-computing-an-emerging-ecosystem.pdf
CHO, Adrian. ***Ordinary computers can beat Google's quantum computer after all***, Science, 2 août 2022.
https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all

113 Centre canadien pour la cybersécurité. ***Évaluation sommaire des candidats à la cryptographie post-quantique du NIST réalisée par le Centre pour la cybersécurité***, 1er mars 2021.
https://cyber.gc.ca/fr/nouvelles-evenements/evaluation-sommaire-des-candidats-la-cryptographie-post-quantique-du-nist-realisee-par-le-centre

114 Security Week. ***Predictions: SecurityWeek's 2022 Cybersecurity Outlook***, 4 janvier 2022.
https://www.securityweek.com/predictions-securityweeks-2022-cybersecurity-outlook
SHANKLAND, Stephen. ***Quantum computers could crack today's encrypted messages. That's a problem***, CNET, 24 mai 2021.
https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/

115 https://cyber.gc.ca/fr/orientation