Infrastructures essentielles après la COVID-19 : prévoir et mitiger l'augmentation des cybermenaces

*Critical infrastructure after COVID-19: predicting and mitigating the rise of
cyber threats*

Marianne Grenier

Édition électronique

URL : <https://journals.openedition.org/eccs/5200>

DOI : 10.4000/eccs.5200

ISSN : 2429-4667

Éditeur

Association française des études canadiennes (AFEC)

Édition imprimée

Date de publication : 30 décembre 2021

Pagination : 119-139

ISSN : 0153-1700

Référence électronique

Marianne Grenier, « Infrastructures essentielles après la COVID-19 : prévoir et mitiger l'augmentation des cybermenaces », *Études canadiennes / Canadian Studies* [En ligne], 91 | 2021, mis en ligne le 30 décembre 2021, consulté le 05 février 2022. URL : <http://journals.openedition.org/eccs/5200> ; DOI : <https://doi.org/10.4000/eccs.5200>

Infrastructures essentielles après la COVID-19 : prévoir et mitiger l'augmentation des cybermenaces

Marianne GRENIER, Université de Calgary

Les cybermenaces contre les infrastructures essentielles (IE) sont en augmentation depuis l'émergence de la COVID-19. Les IE canadiennes se retrouvent dans des positions précaires du fait de la difficulté pour les autorités canadiennes à gérer les risques associés aux cyberattaques. L'approche du gouvernement fédéral en matière de cybersécurité témoigne d'un processus de sécurisation incomplet, limitant la capacité des organisations nationales à faire face aux menaces. Cet article explore les conséquences de la pandémie de la COVID-19 sur la sécurisation des IE canadiennes en examinant les discours liés à la cyberprotection des IE dans la sphère politique, publique et médiatique.

Cyber threats to critical infrastructure (CI) have been rising since the beginning of the COVID-19 health crisis. Canadian CI find themselves in precarious positions considering the difficulty Canadian authorities have in managing the risks associated with cyberattacks. The federal government's approach to cybersecurity demonstrates an incomplete securitization process, limiting the ability of national organizations to deal with threats. This article explores the ramifications of the COVID-19 pandemic on the Canadian CI securitization process by examining the discourse related to cyber protection of CI in the political, public and media spheres.

Le premier aspect que mentionne la page web de Sécurité publique Canada concernant les infrastructures essentielles (IE) est leur objectif : « [a]ccroître la résilience des infrastructures essentielles du Canada. Partenaires, partage d'informations, exercices, résilience et risques. » Pourtant, la capacité des IE, publiques et privées, à investir adéquatement dans le domaine de la cybersécurité fut grandement affectée durant l'année 2020, en partie du fait de la diminution des ressources financières et humaines. Même avant la crise sanitaire de la COVID-19, les efforts préventifs et proactifs en matière de cybersécurité étaient rares parmi tous types d'industries, ces derniers se contentant souvent de réagir aux menaces (MILLER 2016, 23). Cela dit, les conséquences possibles des cyberattaques, brèches ou erreurs humaines ont, depuis longtemps, été reconnues comme dangereuses et pouvant perturber le bon fonctionnement des IE (GENDRON et RUDNER 2012, 14). Lorsque vient le temps de considérer le sort des IE, les répercussions liées à des cyberattaques peuvent directement impacter la société.

Avec l'arrivée de la COVID-19, les cybermenaces ont augmenté, plaçant les IE canadiennes dans une position précaire. En effet, l'emploi de plateformes en ligne a bondi en réponse aux restrictions sanitaires, entraînant une augmentation des vulnérabilités et des attaques (PASSERI 2021). Ainsi, la réévaluation de l'utilisation, de la dépendance et de la protection des IE est essentielle afin d'anticiper et prévenir les menaces auxquelles sont confrontées les infrastructures et la population canadienne. Depuis mars 2020, la capacité des

MARIANNE GRENIER

autorités canadiennes à gérer les risques associés aux cyberattaques dans un contexte d'enjeux émergents est mise à rude épreuve. L'approche du gouvernement canadien en matière de cybersécurité illustre un processus de sécurisation incomplet, limitant l'aptitude des organisations nationales à faire face aux obstacles naissants et en constante évolution. La théorie de la sécurisation, mise de l'avant par l'école de Copenhague, souligne une distinction entre les discours de sécurisation et les réalités du terrain.

Cet article vise à examiner les discours liés à la cyberprotection des IE dans les sphères politique, publique et médiatique à travers cette première question : *quelles sont les conséquences de la pandémie de la COVID-19 sur la sécurisation des IE canadiennes ?* En réfléchissant à une deuxième question : *pourquoi les IE canadiennes sont-elles actuellement limitées dans leur capacité à résister à la menace ?* il sera possible d'illustrer les tendances présentes et futures en matière de cybersécurité qui fragilisent l'environnement sécuritaire du Canada. Nous utiliserons pour cela les données sur les cybermenaces, ainsi que les données publiques concernant les incidents et la protection des IE.

Il est d'abord primordial de préciser le concept d'IE en considérant les nombreuses définitions existantes. Sécurité publique Canada les caractérise comme telles :

[...] les processus, les systèmes, les installations, les technologies, les réseaux, les biens et les services qui sont essentiels à la santé, à la sécurité ou au bien-être économique des Canadiens et des Canadiennes, ainsi qu'au fonctionnement efficace du gouvernement. Les IE peuvent être autonomes ou interconnectées et interdépendantes dans les administrations provinciales, territoriales ou nationales ou entre celles-ci. La perturbation de ces IE pourrait se traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public (2021).

Considérant l'objectif de cette recherche, soit d'approfondir les raisons liées aux limitations du processus de sécurisation des IE canadiennes, la définition utilisée par le gouvernement canadien sera privilégiée. Cependant, il est aussi crucial de prendre en compte d'autres conceptualisations des IE. Gendron et Rudner proposent trois principales caractéristiques qui permettent de déterminer quelles infrastructures peuvent être jugées essentielles (2012, 11). Tout d'abord, les infrastructures ont un pouvoir ou une importance symbolique. Deuxièmement, le fonctionnement des communautés est lié par un considérable degré de dépendance et d'immédiateté aux IE. Finalement, les dépendances complexes de la société sur les IE ont des effets connus et imprévus, ainsi que des conséquences

au-delà du local. Ces caractéristiques permettent d'élargir la compréhension de ce que signifie l'expression « essentielle » (ou critique).

Différents domaines de production et de travail sont souvent englobés dans la locution IE, par exemple, le secteur de l'agriculture et de la nourriture, les technologies de l'information, les systèmes de santé, la défense, les télécommunications, les installations gouvernementales, les services d'urgences, les finances, l'énergie, ainsi que le secteur comportant le traitement des eaux, produits chimiques, nucléaires, etc. (ALAGAPPAN *et al.* 2020, 1091) Plusieurs débats existent quant à ce qui devrait être inclus ou non dans les domaines essentiels. Considérant les objectifs de la recherche, nous utiliserons la liste des IE émise par les autorités canadiennes.

Théorie de sécurisation

La théorie de la sécurisation de l'école de Copenhague, issue des écrits de Buzan, Weaver et De Wilde, est au cœur des études de sécurité et des théories des relations internationales (1998). Elle propose l'idée que les menaces à la sécurité sont conceptualisées et verbalisées principalement par une autorité, comme les décideurs politiques, les responsables des États, les personnes influentes, etc., à travers des actes de discours. Par exemple, les sujets sécurisés vont être accompagnés de termes associés à l'urgence, tels que « dangereux, menaçant, alarmant » (EROUKHMANOFF 2018). Ces termes sont utilisés dans le but de présenter une situation comme un problème de sécurité. Les actes de sécurisation visent à convaincre une audience (ou un public) qu'un sujet précis est un danger urgent et imminent pour la protection de l'État, afin de promouvoir certaines politiques. Une sécurisation réussie implique que l'audience accepte le sujet à titre de menace et soutienne la mise en place de mesures extraordinaires pour contrer ce danger (EROUKHMANOFF 2018).

En utilisant le modèle de Buzan sur les types de menaces auxquelles les États font face, on peut conclure que le Canada est un État où la cohésion sociopolitique est forte tandis que la puissance militaire est relativement faible, laissant ainsi le pays vulnérable aux attaques militaires (1991). Selon Hare, cela s'exprimerait dans le cyberspace par des attaques contre les IE, par exemple (2010). Cette logique implique que les autorités canadiennes devraient sécuriser les cybermenaces de types militaires, y compris celles contre les IE, puisqu'elles se présentent comme les principales cybervulnérabilités de l'État.

Dans le cas des cybermenaces contre les IE, les chercheurs et universitaires s'interrogent pour savoir si le processus de sécurisation s'avère un

succès ou plutôt un échec. Pour certains, le processus a été réussi, car les cyberattaques contre les IE sont perçues comme des problèmes de sécurité nationale. Pour d'autres, le processus est un échec, puisque le public n'a pas accepté le concept des cybermenaces comme un défi central et urgent pour le fonctionnement des systèmes (FRIIS et REICHBORN-KJENNERUD 2016, 32). Le résultat de ce refus aurait conduit à des allocations réduites ou limitées des ressources à la protection contre les cyberattaques. Cependant, de nombreuses études se penchent principalement sur la perspective américaine (BABAR et ALI 2021, 2). Bien que le processus aux États-Unis doive être exploré, du fait de leur position sur l'échiquier mondial et leurs capacités techniques, analyser l'attitude et les actions d'autres pays, tels que le Canada, est primordial pour améliorer la compréhension des cyberphénomènes, en constants changements et évolution.

Revue de littérature

Selon Aradau, la protection des IE en tant que problème de sécurité émergea au milieu des années 1990, mais la manière dont elle est comprise varie considérablement (2010, 492). Dans son évaluation des IE et de la cybersécurité, Aradau suggère également que l'ajout du mot « essentielles » après infrastructures (« *critical* » en anglais) puisse être interprété comme une tentative de sécurisation. Divers auteurs mentionnent la complexité du concept, conduisant à une approche éclectique quant à la sécurité des systèmes essentiels (ARADAU 2010, 501). Malgré les efforts de sécurisation des IE en les déclarant comme cibles à travers le monde, les mesures étatiques et les positionnements internationaux sur leur protection sont loin d'être homogènes.

Un immense défi concernant la gestion des IE est le nombre significatif d'infrastructures entre les mains du secteur privé (BAGGETT et SIMPKINS 2018, 173). Comme les domaines publics et privés se côtoient dans le fonctionnement de services essentiels liés directement aux activités de l'État et de sa population, la complexité est grande pour les gouvernements, chargés d'équilibrer les dynamiques sécuritaires. La privatisation de multiples secteurs vitaux au fonctionnement de la société canadienne alourdit aussi la tâche d'assurer une couverture de protection standardisée aux IE (RUDNER et GENDRON 2012). Cette situation n'est pas unique au Canada, mais doit être prise en compte en considérant les vulnérabilités qui peuvent en résulter. Tout d'abord, la privatisation peut entraîner un délaissement des mesures de sécurité et des investissements à long terme en lien avec la protection de la clientèle et des services, pour potentiellement atteindre d'autres objectifs en termes de capital (DEAN 2015). Deuxièmement, le domaine privé peut aussi engendrer une fragmentation au sein d'un même secteur économique ou technique. Cela signifie qu'un manque de règles communes peut mener au développement ou à

INFRASTRUCTURES ESSENTIELLES APRÈS LA COVID-19 : PRÉVOIR ET MITIGER
L' AUGMENTATION DES CYBERMENACES

l'augmentation de fragilités (DEAN 2015). Par ailleurs, les actes de dissimulation peuvent également être la norme dans les secteurs privés lorsque des vulnérabilités, des attaques ou des brèches d'information et de données sont identifiées, empêchant ainsi l'amélioration future de la sécurité de toutes les IE (RICE et MAUNU 2017).

Il est aussi vital de considérer que le pays est grandement affecté par les positions politiques et militaires de ses alliés occidentaux, principalement par celles des États-Unis, sans compter certaines politiques des puissances européennes. Il est donc difficile de complètement isoler les positions canadiennes de celles d'autres pays. Au Canada, de nombreux secteurs d'IE sont fortement interconnectés à ceux des États-Unis (RUDNER et GENDRON 2012, 15). L'approvisionnement canadien en produits médicaux (vaccins, médicaments, etc.) est particulièrement dépendant des États-Unis (SLAUGHTER 2021). Par ailleurs, le secteur de l'énergie est un autre exemple de cette proximité où les deux nations peuvent être touchées par les conséquences de cyberattaques. La récente cyberattaque contre l'oléoduc américain, Colonial Pipeline, paralysant temporairement l'afflux de pétrole en Amérique du Nord, mais principalement aux États-Unis, a aussi impacté le Canada (YUN 2021). Ce dernier n'est donc pas isolé des effets liés à l'arrêt de fonctionnement d'une si grande industrie, même à l'étranger. Cette connectivité permet de partager des biens et ressources, mais présente également des vulnérabilités qui pourraient affecter de nombreuses nations.

De plus, le développement et l'accessibilité croissante aux technologies augmentent les craintes liées à la protection des IE. Certains chercheurs soulignent que l'expression « cybersécurité » est principalement basée sur les menaces extérieures, alors qu'elle devrait inclure des sujets beaucoup plus complexes (c.-à-d. accidents techniques, erreurs internes, etc.) souvent mis de côté par les agences de défense nationale (NISSENBAUM 2005, 65). D'une autre manière, les IE et leurs cyberspaces sont perçus comme des structures fixes ou rigides (ARADAU 2010, 506-507). En réalité, ces systèmes sont dynamiques, agissant et réagissant aux événements, innovations et sociétés, pouvant influencer les vulnérabilités, tout comme les menaces contre eux.

Au Canada, les domaines qui sont impliqués dans la définition d'IE par la sécurité publique sont les suivants : l'énergie et les services publics, les finances, l'alimentation, le transport, le gouvernement, les technologies de l'information et de la communication, la santé, l'eau, la sécurité et le secteur manufacturier (SÉCURITÉ PUBLIQUE CANADA 2021). Le Canada présente

MARIANNE GRENIER

une liste beaucoup moins exhaustive comparativement aux 16 secteurs inclus par les États-Unis¹, englobant ainsi différents domaines dans de mêmes secteurs (CISA 2021).

Cybersécurité des IE

Entre 2019 et mai 2020, une augmentation des cyberattaques contre les secteurs de la défense, les secteurs publics et le secteur de la santé a été observée à travers le monde (ALAGAPPAN *et al.* 2020, 1099). Malgré la temporalité restreinte de ces recherches, ces tendances se multiplient et sont démontrées par nombreuses sources (THIBODEAU 2020). Il est impossible d'identifier et de rassembler les données de l'ensemble des cyberattaques durant une certaine période, mais plusieurs médias spécialisés visent à illustrer les schémas et tendances des attaques disponibles publiquement. Les principales motivations derrière ces intrusions, depuis quelques années, sont la cybercriminalité, le cyberespionnage, l'hacktivisme et la guerre (THIBODEAU 2020, 1102). En outre, les cyberattaques contre les IE prennent diverses formes, allant des logiciels malveillants aux hameçonnages, en passant par des attaques ciblées ou des fuites internes.

Depuis le début de la pandémie de COVID-19, il y a eu une augmentation incomparable concernant l'utilisation d'Internet, la visioconférence, la dépendance au courrier électronique et plus encore, créant ainsi un terrain toujours plus attrayant pour les pirates. Par ailleurs, la hausse du nombre d'hôpitaux et d'infrastructures de soins de santé ciblés par des attaques de type rançongiciel a aussi été constatée, au Canada comme dans le reste du monde (HOROWITZ 2021). Ce type d'attaques signifie que les pirates bloquent l'accès légitime aux systèmes et données internes, tout en demandant une rançon en échange de l'accès.

Le Centre canadien pour la cybersécurité affirme que les cyberattaques parrainées par des États contre des IE canadiennes entraînant des pertes de vies sont peu probables sans hostilités ouvertes (CENTRE CANADIEN POUR LA CYBERSÉCURITÉ 2020). D'ailleurs, Brewster a établi que les principaux acteurs étatiques derrière les cyberattaques contre les IE nord-américaines sont toujours la Chine, la Russie et la Corée du Nord (BREWSTER 2020). Malgré ces informations, les systèmes essentiels au pays sont davantage victimes d'attaques, ce qui laisse croire que la possibilité des cyberattaques provoquant des victimes

¹ Les secteurs regroupés le terme sous « critical infrastructure » sont « chemical; commercial; communication; critical manufacturing; dams; defense; emergency services; energy; financial; food and agriculture; government; healthcare and public health; IT; nuclear waste; transportation; and water and wastewater. »

INFRASTRUCTURES ESSENTIELLES APRÈS LA COVID-19 : PRÉVOIR ET MITIGER
L' AUGMENTATION DES CYBERMENACES

ou des blessures physiques n'est pas négligeable et doit être prise en compte quand vient le temps d'adresser la sécurité des dispositifs.

De plus, avec l'arrivée de COVID-19, des pressions d'autant plus importantes sont exercées sur les IE. Les nouvelles mesures sanitaires, telles que la distanciation physique ou les fermetures imposées des industries « non essentielles », ajoutent des difficultés et complexités au travail des IE, tandis que les cybermenaces se multiplient. Protéger et identifier toutes les potentielles vulnérabilités d'un système est une tâche colossale, qui est demandée aux entreprises, infrastructures et employés. En revanche, les attaquants n'ont besoin que de trouver une vulnérabilité qui n'est pas protégée pour mener à bien leurs offensives. Cette notion est regroupée sous le concept d'asymétrie, souvent abordé dans les domaines d'ingénierie, de sécurités digitales et logicielles (RUDNER et GENDRON 2012, 40).

Méthodologie

Dans le but d'analyser le processus de sécurisation des IE canadiennes, les débats à la chambre des communes fédérales ont été collectés via Hansard. Spécifiquement, les données de l'année 2019 et des mois de janvier et février 2020 ont été comparées à celles de la période allant de mars 2020 à mai 2021. Ainsi, les deux périodes d'environ 14 mois ont pu être comparées à travers 87 documents pour la première période et 120 pour la seconde. Des recherches textuelles ont été faites pour comparer l'utilisation de termes liés à la cyberprotection et sécurité des IE au pays. Il fut alors possible d'observer les tendances et différences entre les discussions politiques au niveau fédéral pendant les périodes précédant et suivant le début de la pandémie de COVID-19. Cela permit d'évaluer le processus de « speech act » (discours) qui tente de sécuriser des cybermenaces contre les IE en manifestant l'imminence des dangers des cyberattaques et l'urgence d'agir.

Les résultats pourraient démontrer une différence entre les discours de la Chambre des communes pré COVID-19 et ceux post mars 2020 (début des restrictions sanitaires en Amérique du Nord). En effet, il est attendu que le nombre et la fréquence d'utilisation d'expressions liées à la cyberprotection des infrastructures soient beaucoup plus importants après mars 2020.

De plus, la couverture des événements concernant des problèmes de sécurité des IE nationales depuis l'année 2019 par les médias de grande envergure au Canada a été analysée. Plus précisément, des termes tels que « cybersécurité », ainsi qu'« infrastructure essentielle », ont été utilisés pour rassembler les

MARIANNE GRENIER

mentions sur le sujet. Un survol de la littérature abordant la sécurité des IE a aussi été fait, spécifiquement celle qui s'intéresse aux infrastructures canadiennes, ainsi qu'aux tendances cyber des dernières années. Les brèches d'information des compagnies ou des industries privées ne seront pas prises en compte dans le cadre de cette recherche, pour des raisons de ressources limitées et en raison du nombre impressionnant d'événements de la sorte. En revanche, il est important de considérer que ces attaques sont aussi de grande envergure et peuvent avoir des conséquences insoupçonnées. Les rapports d'incidents majeurs concernant les IE au Canada seront observés à la fois dans les importants médias de masse canadiens ainsi que les principaux médias spécialisés en cybersécurité.

Ce travail tente de combler un manque de recherche et de connaissances par rapport aux réalités nationales des IE et leur cyberprotection. Une condition typiquement canadienne est l'absence de travaux sur certaines failles de sécurité, en raison du manque de données canadiennes ou de l'utilisation de nombreuses données américaines. De ce fait, cette recherche vise à explorer la vision et le processus de sécurisation de la cybersécurité des IE uniquement canadiennes.

Finalement, une analyse des différentes explications pour les résultats obtenus lors de la recherche a été faite, permettant ainsi d'ouvrir la discussion sur de potentielles solutions et approches publiques et privées au Canada.

Résultats

Les résultats obtenus, basés sur les débats de la chambre des communes fédérales (tableau 1), présentent d'abord une disparité temporelle. En effet, durant les 14 mois précédents le début de la crise sanitaire en Amérique du Nord en mars 2020, le nombre de débats où les IE et les termes rattachés à « cyber » ont été mentionnés s'élevait à 27. Le terme « cyber » pouvait être associé à toute autre expression, tel que cybersécurité, cybervulnérabilités, cybermenaces, etc. Les résultats de cette recherche textuelle révèlent 27 débats parmi les 87 débats de l'année 2019 jusqu'à mars 2020 où les deux termes (IE et cyber) ont été mentionnés. Cependant, il est important de noter que cela ne signifie pas que chacun de ces débats liait ces termes. Il est possible qu'ils aient été énoncés durant le même débat, sans autres liens connexes. D'autre part, la période de 14 mois suivant le début de la crise de COVID-19 (post mars 2020) comprenant un total de 120 débats, présente des résultats surprenants quant aux mentions des expressions IE et cyber. Vingt-trois mentions totales ont été faites. Ainsi, les débats concernant les problématiques liées aux phénomènes cyber et les IE à la Chambre des communes fédérales ont diminué depuis le début de la crise sanitaire.

INFRASTRUCTURES ESSENTIELLES APRÈS LA COVID-19 : PRÉVOIR ET MITIGER
L' AUGMENTATION DES CYBERMENACES

Tableau 1. Nombre de débats à la Chambre des communes fédérale mentionnant la cybersécurité des IE comparativement aux cyberattaques contre des IE canadiennes

	Nombre de débats mentionnant « cybersécurité » et « infrastructures essentielles » à la Chambre des communes fédérale ²	Cyberattaques contre des IE au Canada répertoriées par des médias spécialisés en cybersécurité ³		
		Hackmageddon (PASSERI 2021)	Bleeping Computer (2021)	SiliconANGLE (2021)
Pré COVID-19	27	14	1	4
Post COVID-19	23	15	5	5
Variance	-14,81 %	7,14 %	400,00 %	25,00 %

Les positions officielles des branches gouvernementales liées à la sécurité semblent décrire une réalité contraire à ces données récoltées. Le Centre canadien pour la cybersécurité (CCC) présente les cybermenaces ciblant les IE en tant que sujet important et urgent à considérer (2020). Elles sont en effet considérées comme un obstacle grandissant à la sécurité de la nation et de la population canadienne, leurs données et fonctionnements. Comme précédemment mentionné, le rapport annuel 2020 de l'évaluation des cybermenaces nationales du CCC estime que les principaux adversaires seraient des nations ennemies dans un contexte sans « climat d'hostilité à l'échelle internationale. » (CENTRE CANADIEN POUR LA CYBERSÉCURITÉ 2020, 21) Il est par contre difficile de mettre de côté le potentiel des cyberincidents dirigés contre des entreprises privées ou même publiques dont les activités sont directement liées au fonctionnement de la nation. Des fragilités internes et des erreurs digitales ou humaines peuvent aussi mener à une hausse des cybervulnérabilités.

² De janvier 2019 à mai 2021

³ Excluant les brèches de données

MARIANNE GRENIER

Par ailleurs, les médias spécialisés en matière de cybersécurité et de technologies de communication ont reporté une plus grande fréquence de cyberincidents affectant le Canada depuis mars 2020, comparativement à la période de 2019 à février 2020 (PASSERI 2021). Comme le présente le tableau, trois grands sites spécialisés, Hackmageddon, Bleeping Computer et SiliconANGLE, répertorient tous une augmentation des attaques contre les IE canadiennes suivant mars 2020. Cette comparaison permet aussi de corroborer la hausse des cyberattaques mentionnée par de nombreux médias traditionnels (THIBODEAU 2020). Cette réalité semble en contradiction avec le manque d'intérêt et de mentions de ces problématiques par les élus fédéraux. Il n'est actuellement possible d'identifier aucune corrélation entre les mentions par les membres du parlement fédéral canadien à propos des aspects cyber des IE et le nombre ou la fréquence des cyberattaques, vulnérabilités et incidents des IE canadiennes. Ces résultats sont peu logiques, compte tenu de la réalité des incidents et menaces ciblant les IE canadiennes. Les élus font preuve de peu d'intérêt à mettre en avant le débat public sur la nécessité d'aborder ces problématiques.

Les données rassemblées sur le site de Paolo Passeri (*hackmageddon*) démontrent clairement une multiplication des cyberattaques reportées sur le site

INFRASTRUCTURES ESSENTIELLES APRÈS LA COVID-19 : PRÉVOIR ET MITIGER
L' AUGMENTATION DES CYBERMENACES

chaque année depuis 2018 à travers le monde. Passeri montre aussi une augmentation en nombre des attaques reportées contre tous les milieux d'IE répertoriés sur le site. Une autre notion à souligner est la croissance des incidents de cyberwarfare et espionnage, chacune des instances difficiles à identifier dans le domaine de la cybersécurité (PASSERI 2021). De plus, ces dernières sont significativement plus liées à des attaques contre des IE. Il est possible de supposer un intérêt particulier des pays ennemis envers les IE, dans l'objectif d'augmenter le pouvoir de levier dans un cas potentiel de tensions grandissantes (CENTRE CANADIEN POUR LA CYBERSÉCURITÉ 2020, 21).

D'autre part, les médias traditionnels les plus consultés par la population canadienne présentent un portrait tout aussi vital.⁴ Tout d'abord, les grands réseaux d'information et journaux canadiens portent une attention particulière aux nouvelles internationales majeures liées à la cybersécurité (AHMED 2021). Ainsi, ils rapportent les incidents et piratages d'envergure dans le monde, parfois indépendamment des répercussions nationales, bien que différents liens soient souvent mis en avant quant aux possibles impacts que ces événements pourraient avoir au Canada (LABINE 2021). Les piratages visant les IE canadiennes sont, pour leur part, très médiatisés, menant les médias à inviter des experts en cybersécurité pour analyser les événements et les conséquences potentielles de telles attaques (RADIO-CANADA 2021). Par contre, les attaques perçues comme ayant peu de répercussions directes sur les citoyens canadiens, que ce soit sur les plans économiques ou de vie privée, semblent peu attrayantes pour les médias canadiens traditionnels. De plus, les médias tentent de toucher la population canadienne, peu informée par rapport au milieu de la cybersécurité, ou de la sécurité générale des IE (BEAUCERON SECURITY 2020). Ainsi, une explication possible du nombre limité de rapports sur des cyberincidents au Canada est le manque d'intérêt direct pour les lecteurs des grands médias ou la perception de ces derniers que ces informations et incidents sont négligeables. Il est d'ailleurs possible de remarquer dans les journaux canadiens une chute significative de leurs mentions des expressions « cyber » et « infrastructures » après le début de la pandémie (Tableau 3). Cela peut s'expliquer par le fait que les informations sur la crise sanitaire aient été considérées comme plus pressantes et plus demandées par les lecteurs.

⁴ Les médias canadiens d'envergure qui ont été observés sont *Radio-Canada*, *TVA Nouvelles*, *La Presse*, *Le Journal de Montréal*, *CBC*, *CTV News*, le *Globe and Mail* et le *Toronto Star*.

Tableau 3. Articles canadiens mentionnant « cyber » et « infrastructure » avant et après le début de la COVID-19 (PROQUEST 2021)

	Janvier 2019 à mars 2020	Mars 2020 à mai 2021
Nombre d'articles	512	217

Quelles sont les conséquences de la pandémie de la COVID-19 sur la cybersécurité des IE canadiennes ?

Tout d'abord, concernant les conséquences de la pandémie sur le processus de sécurisation des IE canadiennes, différentes pistes peuvent être explorées. Les membres élus du parlement fédéral canadien mettent peu l'accent sur la sécurité des IE canadiennes et leur cyberprotection. Cela signifie que le discours de sécurisation dans le domaine politique est peu présent ; il est absent des allocutions qui présentent les plus grandes menaces ciblant la société et la population, et ne provient pas des élus fédéraux. Deuxièmement, les discours et mentions en Chambre des communes ne sont pas compatibles avec les réalités des IE dans le monde ainsi qu'au Canada. En effet, le nombre d'attaques répertoriées dans l'ensemble est élevé, et particulièrement celles contre les IE. Tandis que les élus abordent moins le sujet, les dangers augmentent (PASSERI 2021).

Sur la base de ces données, il est clair que le processus de sécurisation, selon la théorie de l'école de Copenhague, n'est pas complet et ne réussit pas à atteindre la population. Le public n'est pas encouragé à considérer les cyberattaques comme un problème de sécurité urgent et menaçant la nation. Les cyberattaques sont un problème globalement accepté comme une menace de sécurité, ce qui est aussi vrai pour la population canadienne (BROOKS 2021). Par contre, la prise de conscience par la population des répercussions potentielles, ainsi de la réelle possibilité que les IE canadiennes soient attaquées et leurs fonctionnements altérés, ne semble pas totale. La cybersécurité des IE est un problème perçu comme lointain, arrivant aux autres nations ou individus, et n'est pas à prendre en compte urgemment, encore moins durant une période de crise sanitaire. Pourtant, les IE sont limitées dans leur capacité à résister à la menace pour l'instant, dû en grande partie au manque de sécurisation.

Pourquoi les IE canadiennes sont-elles actuellement limitées dans leur capacité à résister à la menace ?

Les facteurs empêchant une meilleure protection des IE peuvent être englobés sous quatre principaux concepts, soit : l'augmentation des vulnérabilités des IE, la croissance des inégalités, la réduction des investissements et intérêts en sécurité ainsi que l'interdépendance grandissante des IE.

En premier lieu, la croissance des vulnérabilités est liée au fait que de nombreuses entreprises et infrastructures ont vu leurs activités se transférer en ligne et à distance, suite aux restrictions physiques pour limiter la propagation de la COVID-19. En raison de ces changements drastiques et rapides, plusieurs vulnérabilités n'ont pu être identifiées et effacées immédiatement. L'utilisation des plateformes de communication numérique à distance, des applications de sauvegarde nuagique et l'accessibilité aux données personnelles d'employés sont des cybervulnérabilités qui ont augmenté de manière fulgurante après mars 2020 (ALAGAPPAN *et al.* 2020). Les employés de nombreuses IE ont vu leurs rôles et tâches changer, sans compter ceux dont le travail fut déplacé à domicile (FRANKLIN 2020). Ces bouleversements dus à la pandémie ont eu des répercussions directes sur les formes et les cibles des cyberattaques :

The growing dependence on remote application software during the COVID 19 also saw an increased attack on various videoconferencing platforms. The uncharted territory of the platform getting big attracted attackers and saw vulnerabilities being exploited. A classic example is Zoom. Zooms online platform became a target of attackers exposing zooms security vulnerabilities. The password attacks led users to compromise user accounts and as many as half a million accounts, and passwords were up for sale in dark web platform (ALAGAPPAN *et al.* 2020, 1095).

En effet, en possession de données telles que les noms d'utilisateurs combinés aux mots de passe, spécifiquement ceux d'individus ayant des postes liées aux IE, les attaquants peuvent pénétrer des systèmes fragiles. L'augmentation fulgurante de travail à distance depuis mars 2020 a directement contribué à l'amplification de vulnérabilités préalablement ignorées ou laissées de côté. Une des raisons expliquant cette situation est liée au fait que les activités de nombreuses IE étaient physiquement et numériquement centralisées, conditions rarissimes depuis le début des mesures d'isolement social.

Deuxièmement, les inégalités ont souvent fait l'objet de recherches liées aux phénomènes criminels et cyber (HEIMER 2019). La pandémie, les restrictions et les pertes d'emplois ont d'ailleurs exacerbé les inégalités dans le monde, et particulièrement en Amérique du Nord (FERREIRA 2021). En raison de ces pertes d'emplois, les inégalités sociales ont bondi en 2020, laissant la place à une montée de la criminalité, plus spécifiquement en ligne considérant les restrictions physiques en place. La notion de corrélation entre les inégalités sociales et les délits n'est pas nouvelle ; en revanche, les capacités offertes dans l'univers digital ont su multiplier les opportunités de commettre des actes criminels (CONSEIL DES ACADEMIES CANADIENNES 2021). Malgré les efforts canadiens pour réduire la prévalence des crimes grâce à divers programmes et en tentant de diminuer les inégalités sociales et économiques au pays, la sphère digitale permet à n'importe quel individu ou groupe de pirater des installations et des informations partout dans le monde. La réalité internationale du monde digital complique grandement la tâche des pays occidentaux qui visent à réduire les impacts des inégalités sur leur territoire, quand de nombreux attaquants sont originaires des régions où les variables criminogènes sont plus importantes. Par ailleurs, il est aussi important de considérer que plus de temps libre alloué aux attaquants signifie que les individus intéressés par les cybercrimes peuvent alors utiliser ce temps pour développer leurs capacités ou simplement perpétrer davantage d'attaques.

Troisièmement, les limitations des IE en matière de cybersécurité au Canada sont aussi expliquées par le manque et la réduction des ressources, humaines, techniques, ou financières, pour faire face aux cybermenaces. Les difficultés économiques liées à la pandémie ont entraîné plusieurs coupures d'emplois ou d'investissement dans certains sous-secteurs, en particulier celui de la sécurité (AIELLO 2020). Cela résulte en la mise de côté des activités de sécurité, autant sur le plan physique que cyber. Les fragilités des secteurs essentiels sont alors disproportionnellement affectées, puisque les efforts de protection sont transférés pour répondre à d'autres besoins.

Pistes de solutions

En matière d'approches potentielles visant à réduire les vulnérabilités des IE canadiennes, différentes solutions doivent être explorées. Premièrement, la société canadienne doit prioriser la protection de ses IE *avant* et *après* les crises. Réagir à une crise, telle que celle de la COVID-19, uniquement lorsqu'elle survient empêche la réflexion et l'amélioration efficace des protections en place. Différentes méthodes, comme enquêter, tirer des leçons des erreurs passées, bonifier les plans d'urgence, examiner les situations d'autres pays ou industries

INFRASTRUCTURES ESSENTIELLES APRÈS LA COVID-19 : PRÉVOIR ET MITIGER
L' AUGMENTATION DES CYBERMENACES

et leurs difficultés, etc., doivent être mises en avant et encouragées pour prévenir de futurs incidents.

Deuxièmement, il est primordial d'assurer l'excellence des employés au service de la sécurité des IE canadiennes. Cela signifie, par exemple, attirer l'innovation, embaucher des travailleurs de différents horizons ou formations, mettre en avant des incitations salariales ou sociales, développer la réputation de la sécurité des IE, encourager le développement des compétences, et plus encore. Les systèmes essentiels doivent savoir rivaliser avec des secteurs qui sont actuellement plus intéressants pour la main-d'œuvre qualifiée et expérimentée, ainsi que pour les diplômés et les jeunes professionnels innovants.

Troisièmement, les dirigeants canadiens doivent envisager des moyens de diversifier l'utilisation et les interdépendances des IE. Cela signifie éviter de s'appuyer sur un secteur ou une installation uniques, tout en augmentant la diversité des employés, des innovations et des sources d'approvisionnements. En réduisant la dépendance à une seule IE, cela aiderait à diminuer les effets des attaques réussies ainsi les impacts des vulnérabilités. Il serait également possible de repenser notre approche de l'interconnexion et de prioriser des systèmes analogiques dans certains cas. D'autres solutions potentielles incluent le cryptage, différents audits, des systèmes d'authentification plus résistants et la meilleure formation des travailleurs. Considérant que 95 % des intrusions sont dues à des erreurs humaines, les individus sont en effet le maillon faible en ce qui concerne les cybervulnérabilités (AHOLA 2019).

De nombreux organismes d'application de la loi suggèrent que du renseignement de qualité supérieure aideraient à prévenir les cybermenaces (CENTRE CANADIEN POUR LA CYBERSÉCURITÉ 2020, 9). Cependant, plus d'information n'équivaut pas nécessairement à de meilleures décisions. Il serait plutôt possible qu'en savoir plus sur l'ennemi, qu'il s'agisse d'un État ou d'un groupe malveillant, sur ses intentions et de ses tactiques, concentre l'attention sur une direction, laissant des failles et faiblesses inaperçues et non résolues. Les pays occidentaux s'appuient particulièrement sur le renseignement, ce qui laisse croire que les principales menaces viennent d'États ennemis, tandis peu ou pas d'intérêt est manifesté pour se préparer aux effets secondaires de catastrophes majeures. Au lieu de cela, l'attention et les efforts pourraient consister à repenser le modèle national, laissant de côté les tendances des autres puissances ou de l'Internet pour se concentrer sur le succès et la protection des IE.

MARIANNE GRENIER

Pour mettre en place ces solutions potentielles, la classe dirigeante doit, tout d'abord, mettre l'accent sur les problématiques des IE, que ce soit au niveau fédéral, provincial ou même régional. Cela permettrait ainsi d'étoffer le processus de sécurisation qui est actuellement incomplet. Par ailleurs, un aspect à considérer pour améliorer la protection des IE est la différence de normes d'une province à l'autre. Certains secteurs sont régis par les provinces, créant des disparités au Canada. Ainsi, la mise en place de certaines normes de cybersécurité pancanadiennes pour les industries privées et publiques permettrait une amélioration des conditions actuelles des infrastructures vitales à la société canadienne. Une manière d'arriver à cette fin est d'investir et mettre l'accent sur les motivations des IE à être proactives en ce qui concerne la protection de leurs produits et infrastructures. Finalement, une autre proposition permettant le développement du processus de sécurisation des cyberstructures des IE touche le secteur de la sécurité. Les agences et professionnels du domaine doivent être plus attentifs aux enjeux cyber, diversifier leurs approches en matière de sécurité physique et digitale, et ce, dans tous les milieux d'activités.

Conclusion

L'impact de la pandémie de COVID-19 en matière de cybersécurité ne semble guère avoir servi de leçon aux élus politiques fédéraux. Cette recherche démontre que peu de changements réels, voire aucun, dans la façon dont la classe dirigeante aborde les cybermenaces, ne sont observables. Ainsi, il est possible d'identifier un échec de sécurisation des cyberattaques contre les IE canadiennes. Les élus canadiens et la population ne perçoivent pas ces vulnérabilités et attaques comme des dangers urgents et imminents contre la nation et contre lesquels il faut agir et investir pour les prévenir. D'autres problématiques liées à la pandémie, telles que les mesures sanitaires, la vaccination et les impacts économiques ont su éclipser les préoccupations sécuritaires des EI.

L'approche des autorités canadiennes ne répond pas aux critères de la théorie de sécurisation de l'école de Copenhague, car le discours n'est pas mis en avant adéquatement pour atteindre l'audience. La population canadienne est au courant de quelques notions liées à la cyberprotection des IE nationales, grâce aux médias traditionnels. Par contre, même les médias traditionnels manifestent peu d'intérêt à approfondir la situation actuelle des problèmes de cybersécurité, jugeant cet aspect peu attrayant pour leur public et entretenant une perception indirecte et lointaine des dangers. Les médias spécialisés portent une attention particulière aux cibles des cyberattaques, qui sont publiquement accessibles. Ces sites et médias sont toutefois principalement consultés par des experts dans les domaines cyber et des individus spécifiquement intéressés par le sujet. Considérés

INFRASTRUCTURES ESSENTIELLES APRÈS LA COVID-19 : PRÉVOIR ET MITIGER
L' AUGMENTATION DES CYBERMENACES

comme du contenu spécialisé, ces médias sont peu accessibles à la population générale.

Diverses raisons expliquent l'augmentation des cyberattaques contre les IE suivant le début de la pandémie de COVID-19. Comme mentionné, la croissance des inégalités, les mises à pied de masse ainsi que la montée des vulnérabilités des IE suite aux mouvements vers le travail à domicile. Ces vulnérabilités accentuées par la progression rapide de la crise sanitaire sont en partie des aspects qui pourraient être abordés pour approfondir le discours sécuritaire de la part des personnes influentes.

Les principaux acteurs des IE et de la sécurité comprennent davantage les risques et les véritables dangers des cybermenaces. Malgré cela, leur influence sur les décisions et positions des autorités canadiennes, des médias et leur accès à la population générale sont limités. Il est pourtant primordial de mettre l'accent sur la protection de nos infrastructures, sur lesquelles la population canadienne s'appuie énormément.

Par ailleurs, de nombreux obstacles nationaux et internationaux limitent actuellement l'innovation, la réinvention et la mise en œuvre de nouvelles approches de la protection des systèmes essentiels. Malgré ces observations, investir dans la défense des IE aiderait le Canada à devenir un chef de file en termes de résilience et à faire prospérer ses communautés en sûreté. Dans la mesure où les incidents liés à la cybersécurité des IE dans le monde augmentent et où celles-ci ont été particulièrement affectées dans les dernières années, mettre en avant un processus de sécurisation efficace et réfléchi est vital. La protection de ces infrastructures est primordiale pour le bon fonctionnement de la société canadienne.

Bibliographie

AHMED, Kawser. 2021 "Canada's cyber security in a globalized environment: Challenges and opportunities." In *Routledge Companion to Global Cyber-Security Strategy*, edited by Scott N. ROMANIUK and Mary MANJIKIANPP, 451-462. London: Routledge.

AHOLA, Micke. 2019. *The Role of Human Error in Successful Cyber Security Breaches*. Usecure. <https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches>

MARIANNE GRENIER

AIELLO, Rachel. 2020. "Federal deficit on track to exceed \$381B, as spending increases in wake of second COVID-19 wave." *CTV News*, December 1. <https://www.ctvnews.ca/politics/federal-deficit-on-track-to-exceed-381b-as-spending-increases-in-wake-of-second-covid-19-wave-1.5209807>

ALAGAPPAN, Annamalai *et al.* 2020. "Impact of Biological Pandemic in Critical Infrastructure Services – Are we heading for a Cyber pandemic?" *European Journal of Molecular & Clinical Medicine* 7 (3): 5154-5177.

ARADAU, Claudia. 2010. "Security that matters: Critical infrastructure and objects of protection." *Security dialogue* 41 (5): 491-51".

BABAR, Abdul Haseeb Khan and ALI, Yousaf. 2021. "Framework construction for augmentation of resilience in critical infrastructure: Developing countries a case in point." *Technology in Society* 68: 101809. <https://doi.org/10.1016/j.techsoc.2021.101809>

BAGGETT, Ryan K, SIMPKINS, Brian K. 2018, *Homeland Security and Critical Infrastructure Protection*, 2nd Edition. ABC-CLIO, LLC.

BEAUCERON SECURITY. 2020. *New Study Shows that Canadian Cybersecurity Literacy is Only Average.* <https://www.beauchersecurity.com/blog/new-study-shows-that-canadian-cybersecurity-literacy-is-only-average>

BLEEPING COMPUTER. 2021. <https://www.bleepingcomputer.com/>

BREWSTER, Thomas. 2020. "Coronavirus scam alert: Watch out for these risky covid-19 websites and emails". *Forbes*, March 12. <https://www.forbes.com/sites/thomasbrewster/2020/03/12/coronavirus-scam-alert-watch-out-for-these-risky-covid-19-websites-and-emails/?sh=386581b81099>

BROOKS, Chuck, 2021. "Alarming Cybersecurity Stats: What You Need to Know For 2021." *Forbes*, March 2. <https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-----what-you-need-to-know-for-2021/?sh=694c2bef58d3>

BUZAN, Barry. 1991. *People, states, and fear: The national security problem in international relations* (2nd ed.). Boulder: Lynne Rienner.

BUZAN, Barry, WÆVER, Ole and DE WILDE, Jaap. 1998. *Security: A new framework for analysis*. Boulder: Lynne Rienner.

INFRASTRUCTURES ESSENTIELLES APRÈS LA COVID-19 : PRÉVOIR ET MITIGER
L' AUGMENTATION DES CYBERMENACES

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ. 2020. *Évaluation des cybermenaces nationales 2020*. Gouvernement du Canada. <https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020>

CISA (Cybersecurity and Infrastructure Security Agency). 2021. *Critical Infrastructure Sectors*. <https://www.cisa.gov/critical-infrastructure-sectors>

CONSEIL DES ACADÉMIES CANADIENNES. 2021. *La sécurité publique à l'ère du numérique*. <https://www.rapports-cac.ca/reports/la-securite-publique-a-lere-du-numerique/>

DEAN, Benjamin. 2015. "Why companies have little incentive to invest in cybersecurity." *The Conversation*, March 4. <https://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570>

EROUKHMANTOFF, Clara. 2018. "Securitisation Theory: An Introduction." *E-International Relations*. <https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/>

FERREIRA, Francisco H. G. 2021. *Inequality in the time of COVID-19*. International Monetary Fund. <https://www.imf.org/external/pubs/ft/fandd/2021/06/inequality-and-covid-19-ferreira.htm>

FRANKLIN, Michael. 2020. "COVID-19 pandemic has changed the way we work, but it likely won't stay that way." *CTV News*, July 3. <https://calgary.ctvnews.ca/covid-19-pandemic-has-changed-the-way-we-work-but-it-likely-won-t-stay-that-way-1.5010002xs>

FRIIS, Karsten and REICHBORN-KJENNERUD, Erik. 2016. "From cyber threats to cyber risks." In *Conflict in Cyber Space*, edited by Karsten FRIIS and Jens RINGSMOSEPP, 27-44. London: Routledge.

HARE, Forrest. 2010. "The cyber threat to national security: Why can't we agree?" In *Conference on Cyber Conflict Proceedings 2010*, edited by C. Czosseck & K. Podins. Tallinn, Estonia: Cooperative Cyber Defense Centre of Excellence.

HEIMER, Karen. 2019. "Inequalities and crime." *Criminology* 57 (3): 377-394.

MARIANNE GRENIER

HOROWITZ, T., Brian. 2021. "2020 offered a 'perfect storm' for cybercriminals with ransomware attacks costing the industry \$21B." *Fierce Healthcare*, March 26. <https://www.fiercehealthcare.com/tech/ransomware-attacks-cost-healthcare-industry-21b-2020-here-s-how-many-attacks-hit-providers>

LABINE, Jeff. 2021. "Impacts of cyberattack on U.S. pipeline company a 'wake-up call' for everyone, says national pipeline association." *Edmonton Journal*, May 17. <https://edmontonjournal.com/business/energy/alberta-cybersecurity>

MAYNE, Mark. 2020. "Password Security alert as half a million zoom credentials up for sale." *The Cybersecurity Source*, April 14.

MILLER, L., Kevin. 2016. "What we talk about when we talk about "reasonable cybersecurity": A Proactive and Adaptive Approach." *Florida Bar Journal* 90 (8): 22. <https://www.floridabar.org/the-florida-bar-journal/what-we-talk-about-when-we-talk-about-reasonable-cybersecurity-a-proactive-and-adaptive-approach/>

NISSENBAUM, Helen. 2005. "Where computer security meets national security." *Ethics and Information Technology* 7: 61-73.

PASSERI, Pablo. 2021. "2019 Cyber Attacks Statistics." *Hackmageddon*, January 23. <https://www.hackmageddon.com/category/security/cyber-attacks-statistics/>

PROQUEST. 2021. [Journaux canadiens]. 11 décembre.

RADIO-CANADA. 2021. *Cybersécurité*. <https://ici.radio-canada.ca/theme/301/cybersecurite/1>

RICE, Adam and MAUNU, Mark. 2017. "Politics of cyber attribution pose risk for private industry." *TechTarget*, April. <https://searchsecurity.techtarget.com/feature/Politics-of-cyber-attribution-poses-risk-for-private-industry>

ROBINSON, Michael, JONES, Kevin, and JANICKE, Helge. 2015. "Cyber warfare: Issues and challenges." *Computers & Security* 49: 70-94.

RUDNER, Martin, GENDRON, Angela. 2012. *Assessing cyber threats to Canadian infrastructure*. Canadian Security Intelligence Service.

SCROXTON, Alex. 2020. "Coronavirus: Warning over surge in Zoom Security incidents." *ComputerWeekly.com*, October 4.

INFRASTRUCTURES ESSENTIELLES APRÈS LA COVID-19 : PRÉVOIR ET MITIGER
L' AUGMENTATION DES CYBERMENACES

SÉCURITÉ PUBLIQUE CANADA. 2021. *Infrastructures essentielles du Canada*. Gouvernement du Canada. <https://www.securitepublique.gc.ca/cnt/ntnl-scr/crtcl-nfrstrctr/cci-iec-fr.aspx>

SILICONANGLE. 2021. *Security*. <https://siliconangle.com/category/security/>

SLAUGHTER, Graham. 2021. "As Canada awaits vaccine doses, relying on other countries is the wrong approach: U.K. expert." *CTV News*, January 30. <https://www.ctvnews.ca/health/coronavirus/as-canada-awaits-vaccine-doses-relying-on-other-countries-is-the-wrong-approach-u-k-expert-1.5288416>

THIBODEAU, Marc, 2020. « Une menace plus importante à l'ère de la COVID-19 ». *La Presse*, 21 novembre. <https://www.lapresse.ca/actualites/2020-11-21/cyberattaques/une-menace-plus-importante-a-l-ere-de-la-covid-19.php>

YUN, Tom. 2021. "Colonial Pipeline shutdown: How it could affect Canadians." *CTV News*, May 12. <https://www.ctvnews.ca/business/colonial-pipeline-shutdown-how-it-could-affect-canadians-1.5424996>