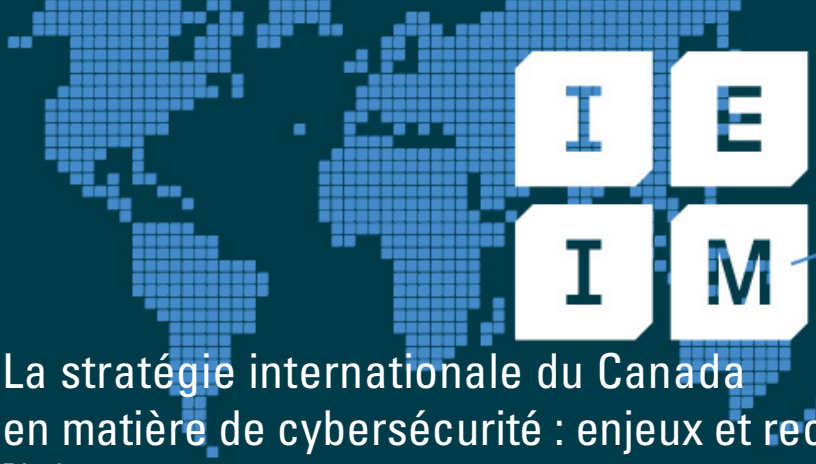

UQÀM

INSTITUT D'ÉTUDES INTERNATIONALES DE MONTRÉAL

WWW.IEIM.UQAM.CA

La stratégie internationale du Canada en matière de cybersécurité : enjeux et recommandations

Février 2020

Résumé exécutif

Il va sans dire que les technologies numériques ont généré des opportunités immenses et presque sans précédent en matière de développement et de croissance sociale et économique aux quatre coins du globe. Or, leur déploiement rapide ne s'est pas fait sans créer de nouvelles menaces envers la sécurité internationale, en matière de droits de la personne ainsi que pour l'économie mondiale. Par ailleurs, les États voient leur influence sur la scène internationale diminuée au profit des acteurs du secteur privé qui développent, opèrent et contrôlent la plupart des technologies de l'information et de communication qui soutiennent les infrastructures essentielles, dont le système de communication mondial, au-delà des frontières étatiques.

Dans ce contexte d'insécurité croissante et de redéfinition de l'ordre mondial, les États, dont le Canada, ont tout de même un important rôle à jouer afin de limiter les risques associés au cyberespace et au développement de nouvelles technologies. Or, bien que plusieurs enjeux et défis associés à la protection et à la stabilité du cyberespace méritent davantage d'attention de la part du gouvernement canadien, celui-ci tarde à adopter une stratégie internationale de cybersécurité. De même, le gouvernement québécois tarde aussi à formuler une stratégie à son niveau. Ce document politique vise à dresser l'état des lieux de la cybersécurité au Canada et à l'international, et à proposer des recommandations aux gouvernements canadien et québécois.

Faits saillants

- → En 2019, la fraude ou le vol de données et les cyberattaques ont été classés dans le top 10 des risques mondiaux, en termes de probabilité et d'impact.
- → Le modèle d'entreprise basé sur la collecte et l'exploitation de données porte atteinte à plusieurs droits fondamentaux, dont le respect de la vie privée, et menace la démocratie.
- → Le Canada reconnait qu'il est susceptible d'être la cible de cybermenaces sophistiquées, provenant d'auteurs parrainés par des États, contre à la fois ses institutions publiques, ses entreprises et ses infrastructures essentielles.
- → Le Canada ne possède toujours pas de stratégie internationale pour la cybersécurité.
- → Le Québec n'a pas encore dévoilé sa politique de cybersécurité.

Contenu

Contexte

Dix ans après avoir lancé la première itération de sa stratégie nationale de cybersécurité[1] (en 2010), le Canada ne possède toujours pas de politique étrangère ou de stratégie internationale orientée vers les enjeux du cyberespace[2]. Si le plan d'action accompagnant la nouvelle mouture de sa stratégie nationale de cybersécurité, dévoilée en 2018, fait bien mention de l'objectif d'élaborer une cyberstratégie internationale, il n'empêche que la date cible de 2019 prévue pour le dévoilement dudit document est maintenant dépassée. Il semble donc que les Canadiennes et Canadiens ne soient pas sur le point de connaître la stratégie que le gouvernement fédéral entend poursuivre à l'international pour assurer leur cybersécurité. La stratégie nationale de 2018 se contente seulement de mentionner que le « gouvernement du Canada travaillera avec ses partenaires internationaux pour faire progresser les intérêts canadiens »[3].

Cette apparente indécision, du moins au niveau fédéral, sur la façon de traiter les enjeux internationaux de cybersécurité s'inscrit pourtant dans un contexte mondial de compétition technologique, de cybermenaces accrues, d'atteintes aux droits de la personne et d'absence d'entente ou de norme internationale sur la sécurité du cyberespace.

> « *L'interconnexion et l'interdépendance qui caractérisent le cyberespace font en sorte que la plupart des risques et défis en matière de sécurité ont* de facto *une portée transnationale* ».

Autrement dit, il serait futile pour le Canada, au même titre que pour le reste des États, d'aborder la cybersécurité uniquement au prisme de la politique interne. Au-delà des gouvernements, la cybersécurité relève principalement du secteur privé qui possède et opère les infrastructures essentielles qui soutiennent le fonctionnement des sociétés développées, y compris en matière de télécommunications et de plateformes numériques. Or, au Canada comme ailleurs, le rôle et surtout les responsabilités du secteur privé en matière de cybersécurité nationale et internationale, et de protection des droits de la personne, restent encore à être clairement déterminés.

La stratégie nationale de 2018 mentionne le potentiel du Canada d'être un leader mondial en matière de cybersécurité. Toutefois, force est de constater qu'en l'absence d'une stratégie internationale claire, il sera difficile pour le Canada d'assumer un tel rôle. Par ailleurs, tous les paliers gouvernementaux doivent établir une stratégie de cybersécurité si le Canada souhaite devenir un leader mondial. Le présent document vise ainsi à soutenir l'objectif du Canada de se démarquer à l'échelle internationale, en matière de cybersécurité, en émettant une série de recommandations pour les gouvernements canadien et québécois.

---

[1] La cybersécurité se définit comme la protection de l'information numérique et de l'infrastructure sur laquelle elle repose. Plus particulièrement, la cybersécurité englobe l'ensemble des technologies, des processus, des pratiques, des mesures d'intervention et d'atténuation dont la raison d'être est d'empêcher que les réseaux, ordinateurs, programmes et données soient attaqués ou endommagés, ou qu'on y accède sans autorisation, afin d'en assurer la confidentialité, l'intégrité et la disponibilité.

[2] Le cyberespace renvoie au monde électronique créé par les réseaux interreliés de la technologie de l'information et de l'information qui circule dans ces réseaux. Le cyberspace est un bien commun reliant plus de trois milliards de personnes qui échangent des idées et des services.

[3] Sécurité Publique Canada (2018), « Stratégie nationale de cybersécurité: Vision du Canada pour la sécurité et la prospérité dans l'ère numérique ».

Enjeux et défis de l'avenir

Interconnexion et interdépendance : un système international de plus en plus complexe

L'infrastructure décentralisée du cyberespace – le système d'information et de communication numérique mondial – a été conçue de manière à favoriser un partage d'information à travers le monde. Il en découle que les cyberattaques[4] ont le potentiel de transcender les frontières et d'affecter plusieurs systèmes et réseaux, tel que démontré par les cyberattaques *NotPetya* et *WannaCry*, en 2017, qui se sont propagées rapidement autour du globe, affectant plusieurs dizaines de pays (plus de 200 000 systèmes informatiques, répartis dans 150 pays, ont été affectés par la cyberattaque *WannaCry*). L'ère numérique fait donc en sorte que les États sont de plus en plus interconnectés et que les risques sont transnationaux. Ainsi, dans son rapport 2019 sur les risques mondiaux, le Forum économique mondial place le vol de données et les cyberattaques au quatrième et cinquième rang respectivement, en raison de leur degré de probabilité et d'impact[5].

Si le cyberespace a permis d'accroître l'interdépendance non seulement en matière de partage de systèmes et de télécommunications, il reflète surtout un phénomène plus large et qui s'étend à d'autres secteurs. Par exemple, la configuration de l'économie mondiale, articulée à la jonction du commerce international et de la finance, repose sur l'interconnexion entre les marchés financiers et les technologies numériques. En raison de son intégration et de sa dépendance à l'égard des réseaux numériques interconnectés, le système financier global est intensément exposé et vulnérable aux cybermenaces[6]. Au Québec, le mouvement financier Desjardins a été victime en juin 2019 d'un vol de données sans précédent, touchant au total 2,7 millions de particuliers et 173 000 entreprises, soit 41 % de sa clientèle[7]. Au Mexique, en avril 2018, une cyberattaque contre le réseau de paiement interbancaire national a entraîné la perte de 15 millions de dollars à travers plusieurs institutions bancaires. Le système mexicain s'apparente au réseau mondial de transfert interbancaire de la Société mondiale de télécommunications financières interbancaires (SWIFT), également victime d'une cyberattaque en 2016[8]. Désormais, le degré d'interconnexion entre les économies du monde est tel qu'une perturbation réussie d'une infrastructure financière pourrait avoir un impact significatif sur l'ensemble du système financier et donc sur l'économie mondiale.

Par conséquent, considérant le contexte international actuel, structuré par un système numérique de plus en plus complexe et intégré entre les pays, la promotion d'une forme d'isolationnisme semble pour le moins contradictoire. La coopération internationale apparaît en effet essentielle pour répondre aux cybermenaces transnationales. Pourtant, dans son plan d'action national en matière de cybersécurité 2019-2024, le gouvernement du Canada reconnaît lui-même que « jusqu'à présent, la dimension

[4] Une cyberattaque suppose l'accès non autorisé à des renseignements électroniques ou à des appareils électroniques, à des systèmes informatiques et à des réseaux utilisés pour traiter, transmettre ou stocker cette information, ou encore leur utilisation, manipulation, interruption ou destruction (par voie électronique).

[5] Joe Myers et Kate Whiting (2019), « These are the biggest risks facing our world in 2019 », *World Economic Forum*, disponible à l'adresse suivante: https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/

[6] Une cybermenace traduit l'existence d'un acteur malveillant qui utilise Internet pour profiter d'une vulnérabilité connue afin d'exploiter un réseau et l'information qu'il contient.

[7] Julien Arsenault (2019), « Faille de sécurité chez Desjardins: 2,9 millions de membres touchés », *Le Soleil*, 21 juin, disponible à l'adresse suivante: https://www.lesoleil.com/affaires/faille-de-securite-chez-desjardins-29-millions-de-membres-touches-video-18ed0e00a0241e08cf3ea871e5d09ce9

[8] Adrian Nish et Saher Naumann (2019), « The Cyber Threat Landscape: Confronting Challenges to the Financial System », *Carnegie Endowment for International Peace*, 25 mars, disponible à l'adresse suivante: https://carnegieendowment.org/2019/03/25/cyber-threat-landscape-confronting-challenges-to-financial-system-pub-78506

internationale de la cybersécurité n'a pas été au centre des préoccupations au Canada, malgré le fait que de nombreuses menaces proviennent de l'étranger et que la cybersécurité soit un enjeu intrinsèquement transnational »[9]. Il importerait qu'un changement s'opère rapidement à cet égard.

Militarisation et sécurisation du cyberespace

Au cours des deux dernières décennies, le cyberespace et les menaces qui y sont associées sont devenus un point central des préoccupations en matière de sécurité nationale dans la plupart des États occidentaux. Une attention croissante a en effet été portée au risque posé par les cyberattaques contre les infrastructures essentielles, aux cybermenaces envers la sécurité nationale et à la transformation des conflits interétatiques par le cyberespace. Le Centre canadien pour la cybersécurité (CCC) affirme notamment dans son rapport de 2018 sur les cybermenaces que le Canada est susceptible d'être visé par des cyberattaques de plus en plus sophistiquées et parrainées par des États, envers ses entreprises, ses institutions et ses infrastructures essentielles[10]. Ces phénomènes de sécurisation et militarisation du cyberespace ces dernières années ont eu pour effet d'inciter les États, focalisés jusqu'à présent sur des stratégies de cyberdéfense, à développer et rendre opérationnelles leurs capacités offensives.

En 2018, le département de la Défense des États-Unis a ainsi affirmé au sein de sa cyberstratégie vouloir mettre l'accent sur la défense « en avant » (*defend forward*) ou, en d'autres mots, sur l'offensive[11]. De même, lors du Sommet de Varsovie en 2016, l'Organisation du traité de l'Atlantique Nord (OTAN) a déclaré que le cyberespace était un domaine d'opérations militaires, au même titre que les domaines de l'air, de la terre et de la mer. Or, les États membres de l'OTAN ne sont pas les seuls à développer des capacités offensives pour des fins militaires, et la militarisation du cyberespace s'opère au niveau global. Par exemple, la République Populaire de Chine de Xi Jinping a réaffirmé dans son 10ème livre blanc de la défense en 2019 que le cyberespace, au même titre que l'espace, est devenu un théâtre essentiel dans lequel se joue la compétition stratégique entre les États[12]. Une telle posture offensive augmente donc les risques d'escalade dans les tensions internationales entre les grandes puissances, contribuant au dilemme de la sécurité[13] associé au développement de nouvelles cybercapacités militaires.

Dans le cas du Canada, la politique de défense, publiée en 2017, fait également état du développement de capacités offensives et défensives dans le domaine du cyberespace. Focalisant sur les risques du cyberespace et les transformations militaires par le cyberespace, le gouvernement canadien ne fait pas exception et choisit également de mettre l'accent sur la dimension offensive.

[9] Sécurité Publique Canada (2019), « Plan d'action national en matière de cybersécurité 2019-2024 », disponible à l'adresse suivante: https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-fr.aspx
[10] Centre canadien pour la cybersécurité intitulé (2018), « Évaluation des cybermenaces 2018 », disponible à l'adresse suivante: https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2018
[11] Department of Defense of The United States of America (2018), « Summary, Department of Defense Cyber Strategy », disponible à l'adresse suivante: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyberstrategysummary.pdf
[12] State Council Information Office of the People's Republic of China (2019), « China's National Defense in the New Era », disponible à l'adresse suivante: http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html
[13] Le dilemme de la sécurité est un concept utilisé en théorie des Relations Internationales qui renvoie au phénomène suivant: lorsqu'un État accroit sa puissance militaire pour garantir sa sécurité, cette attitude peut être perçue comme une menace par un autre État, qui va à son tour renforcer sa puissance militaire, créant ainsi un état d'instabilité et de méfiance dans le système international.

Compétition technologique et économique

Les hostilités entre les grandes puissances, particulièrement la Chine de Xi Jinping et les États-Unis de Donald Trump, sur les plans économique et technologique créent de l'instabilité dans le système international. À l'ère numérique, la technologie se trouve au cœur des tensions entourant les questions de puissance et de gouvernance, puisque la puissance nationale est associée à la compétitivité industrielle et économique, toutes deux soutenues par le développement de la technologie. Ainsi, la montée de la Chine est perçue en Occident, et particulièrement aux États-Unis, comme une menace à la puissance américaine et à l'ordre mondial libéral qu'ils ont établi. En 2018, afin de répondre à la montée de la Chine, le gouvernement américain a justifié, invoquant une atteinte à la sécurité nationale, l'imposition de tarifs commerciaux sur des produits chinois et aussi l'interdiction pour certaines entreprises, dont Huawei et ZTE, de commercer avec les États-Unis[14].

Le Canada semble donc pris entre l'arbre et l'écorce, alors que son principal allié, les États-Unis, et l'un de ses principaux partenaires économiques[15], la Chine, sont en compétition ouverte. Bien que le gouvernement canadien tente de se faire neutre dans le conflit économique opposant la Chine et les États-Unis, il en demeure affecté. La crise diplomatique suivant l'arrestation de Meng Wanzhou, la directrice financière de Huawei, ainsi que l'arrestation de deux ressortissants canadiens en Chine a terni les relations entre les deux pays. Par ailleurs, tandis que le Canada reçoit de la pression de la part des États-Unis d'interdire à Huawei de déployer le réseau 5G au Canada, le gouvernement canadien tarde à offrir une réponse politique claire[16]. Pendant ce temps, le géant chinois continue d'investir des millions de dollars dans les universités canadiennes[17].

Le Canada doit apporter rapidement une réponse claire vis-à-vis de Huawei et du déploiement de la technologie 5G sur le sol canadien. Or, Ottawa se trouve dans une position délicate, puisqu'il s'agit de préserver la confiance avec son allié américain sans pour autant perdre ses liens économiques avec la Chine, un partenaire commercial incontournable pour le développement du Canada dans les décennies à venir. Si l'alliance avec les États-Unis demeure essentielle pour la sécurité et l'économie du Canada, le gouvernement devrait davantage assumer des positions parfois antagonistes à celles américaines afin de protéger et faire valoir les intérêts canadiens. Quant à la Chine, le Canada doit trouver des façons d'entretenir ses relations avec cette puissance fortement impliquée sur la scène internationale et offrant de grandes opportunités de marché.

Enfin, au-delà de l'aspect de la compétition économique, la situation avec Huawei n'est qu'un cas particulier d'un plus grand défi : la dépendance aux technologies et composantes informatiques et électroniques d'origine étrangère au sein des infrastructures nationales essentielles. Une stratégie claire aiderait toutes les parties à mieux gérer ce risque, l'anticiper et favoriser la désescalade.

---

[14] Steve Lohr (2019), « U.S. Moves to Ban Huawei From Government Contracts », *New York Times*, 7 août, disponible à l'adresse suivante: https://www.nytimes.com/2019/08/07/business/huawei-us-ban.html

[15] En 2018, les exportations en Chine ont connu la plus importante croissance parmi les partenaires commerciaux du Canada, en dehors des États-Unis. Le marché chinois représente une opportunité importante pour les entreprises canadiennes, et le Canada veut donc s'assurer d'y avoir accès. Affaires mondiales Canada (2019), « Le point sur le commerce 2019 », disponible à l'adresse suivante: https://www.international.gc.ca/gac-amc/publications/economist-economiste/state_of_trade-commerce_international-2019.aspx?lang=fra

[16] Jim Bronskill (2020), « Pending decision on Huawei 5G puts Trudeau government under pressure », *CBC*, 2 janvier, disponible à l'adresse suivante: https://www.cbc.ca/news/politics/political-pressure-huawei-decision-1.5413058

[17] Ian Young (2020), « Huawei spends millions at Canadian university, but some professors fear US crackdown », *South China Morning Post*, 8 janvier, disponible à l'adresse suivante: https://www.scmp.com/news/china/diplomacy/article/3045090/risky-research-huawei-spends-millions-canadian-university-some

Absence de normes internationales du cyberespace et inefficacité de l'ONU

En raison du développement rapide des technologies numériques, les États tardent à adapter les instruments internationaux existants ainsi qu'à établir de nouvelles ententes pour régir la conduite des États. L'existence de perspectives multiples et divergentes entourant ce qui fait l'objet de la cybersécurité ou ce qui représente une menace dans le cyberespace, notamment en matière de circulation de l'information et de liberté d'expression, explique pourquoi il s'avère difficile d'établir un consensus. Par ailleurs, les États ayant pris de l'avance sur l'implantation de programmes offensifs (dont les États-Unis) ne souhaitent pas mettre place des normes internationales restreignant leur utilisation. Or, ce déficit de gouvernance internationale du cyberespace fait en sorte que les États peuvent agir sans contraintes réelles, créant de l'insécurité et de l'instabilité[18].

Afin d'engager une discussion officielle entre États sur l'élaboration de normes internationales pour le cyberespace, l'Assemblée générale des Nations Unies a créé en 2004 le groupe d'experts gouvernementaux (GEG) sur les développements dans le domaine de l'information et des télécommunications pour la sécurité internationale. Cinq groupes d'experts ont été créés depuis 2004. Or, malgré le consensus entourant le rapport du GEG produit en 2015, celui de 2017 s'est dissous sans accord. L'une des difficultés touchait notamment la manière dont le droit international s'applique au cyberespace.

Pour contrer l'impasse du GEG, l'Assemblée générale des Nations Unies a accepté deux nouvelles initiatives concurrentes en décembre 2018[19]. La première, une résolution parrainée par la Russie, a créé un groupe de travail à composition non limitée ayant pour objectif d'étudier les normes existantes contenues dans les précédents rapports du GEG, d'identifier de nouvelles normes et d'étudier la possibilité d'établir un dialogue institutionnel régulier sous les auspices des Nations Unies. Le groupe de travail est ouvert à tous les États membres de l'Organisation des Nations Unies (ONU) et a également tenu en décembre 2019 une réunion consultative avec des membres du secteur privé, de la société civile et du milieu universitaire. La seconde initiative, soutenue par les États-Unis, a résulté en la création d'un nouveau GEG pour étudier comment le droit international s'applique à l'action des États dans le cyberespace et identifier les moyens de promouvoir le respect des cybernormes existantes. Cependant, plutôt que de favoriser un débat productif entre des points de vue divergents, les deux initiatives semblent plutôt évoluer en parallèle. Il pourrait par ailleurs s'avérer difficile de trouver un terrain d'entente entre les deux groupes.

Ainsi, compte tenu de la difficulté d'obtenir un consensus parmi des grandes puissances (Chine, Russie et États-Unis) dans la recherche d'accords de coopération internationale pour préserver la stabilité et la sécurité du cyberespace, les puissances moyennes, comme le Canada, sont encouragées à prendre le relais. Par exemple, la France, par le biais de son ministère des Armées, a dévoilé en 2019 un document dans lequel elle affirme sa position quant à l'applicabilité du droit international aux opérations menées dans le cyberespace[20].

---

[18] Christian Leuprecht, Joseph Szeman et David B. Skillicorn (2019), « The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity », *Contemporary Security Policy*, 40, (3), pp. 382-407.

[19] Organisation des Nations Unies, « Developments in the field of information and telecommunications in the context of international security », disponible à l'adresse suivante: https://www.un.org/disarmament/ict-security/

[20] Ministère des Armées de la France (2019), « Droit international appliqué aux opérations dans le cyberespace », disponible à l'adresse suivante: https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit%2Binternat%2Bappliqu%C3%A9%2Baux%2Bop%C3%A9rations%2BCyberespace.pdf

L'Australie a quant à elle dévoilé sa stratégie internationale de cyberengagement en 2017[21]. De son côté, le plan d'action canadien prévoit d'améliorer la collaboration du Canada avec les États-Unis en mettant à disposition des fonctionnaires à Washington et en créant un groupe de travail international sur la cybercollaboration au sein d'Affaires mondiales Canada (AMC), afin d'améliorer l'échange d'information et la coordination avec les organismes gouvernementaux. Or, bien que ces initiatives représentent un pas dans la bonne direction, la publication d'une stratégie internationale, qui représente le meilleur moyen pour le Canada de promouvoir son leadership et d'asseoir sa position, se fait toujours attendre.

Rôles et responsabilités du secteur privé en matière de cybersécurité

Alors que la sécurité nationale demeure la responsabilité des États, il se trouve qu'en ce qui concerne les technologies de l'information et le cyberespace, le secteur privé joue un rôle accru. En effet, dans la plupart des pays de l'Occident, dont le Canada, ce sont les entreprises privées qui développent, possèdent et opèrent les technologies de l'information et des communications, de même que la majorité des infrastructures essentielles, et qui sont donc responsables d'assurer la cybersécurité de leurs réseaux et systèmes. En d'autres termes, le secteur privé est de plus en plus responsable de la cybersécurité nationale et internationale. Or, cette privatisation de la sécurité s'opère dans un contexte de partage indéfini des responsabilités.

En effet, alors que la plupart des stratégies nationales et internationales de cybersécurité ou encore des politiques de défense misent sur la collaboration avec le secteur privé, il y a une absence de répartition claire des responsabilités en ce qui a trait à la cybersécurité nationale et internationale[22], de même qu'en termes de responsabilités pour assurer la protection des renseignements privés et confidentiels des citoyens. Par exemple, la stratégie nationale de cybersécurité du Canada se contente de mentionner que les « dirigeants du secteur privé auront un rôle central à jouer, puisque des efforts de collaboration sont requis afin que tous les Canadiens soient outillés pour prévenir et contrer les cybermenaces ». Or, en quoi consiste ce rôle exactement ? Plus particulièrement en ce qui a trait aux cybermenaces sophistiquées provenant d'États étrangers et posant un risque pour la sécurité nationale, quelles sont les attentes précises envers le secteur privé ? À quel moment le gouvernement doit-il intervenir pour assurer la sécurité des Canadiens ? Une clarification du cadre légal pourrait répondre à ces questions.

Dilemme entre sécurité nationale et droits de la personne

La sécurisation du cyberespace crée également un dilemme entre l'importance de la sécurité nationale et le respect du droit à la vie privée. En effet, en mettant l'accent sur les dimensions militaire et sécuritaire, particulièrement en matière de renseignement, les gouvernements tendent du même coup à omettre les impacts négatifs des technologies de surveillance sur le plan des droits de la personne (les révélations d'Edward Snowden en 2013 ont notamment démontré que les États-Unis ont eux-mêmes des pratiques de surveillance critiquables). Récemment, la question du chiffrement (*encryption*) a fait l'objet de débats au Canada comme chez ses alliés du Groupe des cinq[23].

---

[21] Commonwealth of Australia, Department of Foreign Affairs and Trade (2017), « Australia's International Cyber Engagement Strategy», October, disponible à l'adresse suivante: https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf

[22] Madeline Carr (2016), « Public-Private Partnerships in National Cyber-Security Strategies », *International Affairs*, 92, (1), pp. 43-62.

[23] Le Groupe des cinq, *Five Eyes* en anglais, est une alliance entre les services de renseignements des États-Unis, du Canada, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande.

Le ministère de la Sécurité publique du Canada a fait volte-face en 2019 sur son historique de défense du chiffrement en publiant un communiqué conjoint[24] avec ses homologues du Groupe des cinq. Le document demande entre autres aux entreprises technologiques d'inclure des mécanismes dans la conception de leurs produits et services permettant aux gouvernements d'avoir accès aux données récoltées par les entreprises. Or, ce type de « *backdoors* » risque plutôt de nuire à la protection des données confidentielles, essentielles à la cybersécurité. En effet, le CCC reconnaît lui-même dans son évaluation des cybermenaces que ces dernières comportent souvent des implications liées à la vie privée et peuvent avoir d'importantes conséquences, comme le vol de vastes quantités de renseignements personnels.

Par ailleurs, le rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression a publié un rapport en 2019 qui indique que les États (dont le Canada) ont le devoir de défendre les droits de la personne en protégeant les citoyens contre une surveillance ciblée facilitée par les technologies numériques. Le rapport de l'ONU recommande notamment de « réglementer plus strictement l'exportation et l'utilisation des technologies de surveillance et d'appliquer un moratoire immédiat sur la vente et le transfert internationaux des technologies du secteur privé de la surveillance jusqu'à ce que des mesures solides soient adoptées pour garantir que les États et les autres acteurs utilisent ces technologies en toute légitimité et dans le respect des droits de l'homme »[25]. Or, la pratique de certaines entreprises canadiennes a été critiquée, car celles-ci ont exporté des technologies de surveillance dans des pays, dont la Turquie et l'Égypte, où le respect des droits de la personne est remis en cause[26].

Finalement, plusieurs événements récents tels que l'ingérence russe dans les élections américaines de 2016, le Brexit et le scandale entourant l'entreprise britannique Cambridge Analytica ont démontré que les médias sociaux et autres plateformes numériques peuvent être utilisés pour mener des opérations d'influence à grande échelle, propager des discours de haine et favoriser l'instabilité sociale et la polarisation. En 2019, Amnistie internationale a notamment dévoilé un rapport évoquant que le modèle économique des entreprises technologiques, comme Facebook et Google, fondé sur la collection et l'exploitation des données confidentielles de leurs utilisateurs et la surveillance, constitue une menace systémique envers plusieurs droits fondamentaux tels que la liberté d'opinion et d'expression, la liberté de pensée et le droit à l'égalité et à la non-discrimination[27]. Le rapport stipule entre autres que les États doivent adopter de nouvelles réglementations en suivant une approche fondée sur les droits de la personne. Par exemple, la Californie a adopté en 2018 une loi pionnière en matière de protection de la vie privée. En effet, le *California Consumer Privacy Act*, entré en vigueur le 1er janvier 2020, permet aux utilisateurs de différentes plateformes numériques de refuser la vente de leurs données personnelles et de demander aux entreprises de leur divulguer les informations qui ont été collectées à leur sujet[28].

---

[24] United Kingdom's Attorney General's Office and Home Affairs (2019) « Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019 », disponible à l'adresse suivante: https://www.gov.uk/government/publications/five-country-ministerial-communique/joint-meeting-of-five-country-ministerial-and-quintet-of-attorneys-general-communique-london-2019

[25] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Conseil des droits de l'homme, A/HRC/41/35, 28 mai 2019.

[26] Mathieu Braga (2018), « They thought they were downloading Skype. Instead they got spyware », *CBC*, 9 mars, disponible à l'adresse suivante: https://www.cbc.ca/news/technology/citizen-lab-sandvine-report-turkey-egypt-spyware-ads-1.4568717

[27] Amnistie internationale (2019), « Surveillance Giants : How the Business Model of Google and Facebook Threatens Human Rights », disponible à l'adresse suivante: https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/

[28] Kari Paul (2019), « California's groundbreaking privacy law takes effect in January. What does it do? », *The Guardian*, 30 décembre, disponible à l'adresse suivante: https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do

Recommandations

1. Créer une stratégie internationale de cybersécurité.

« Il est nécessaire que le Canada et le Québec favorisent le dialogue multilatéral et multipartite avec des acteurs étatiques et non-étatiques sur les enjeux du cyberespace, y compris en dehors du cadre onusien. »

Le gouvernement canadien, qui promet depuis longtemps une stratégie internationale en matière de cybersécurité, devrait en accélérer la publication et accroître ses efforts d'influence afin d'établir des normes internationales régissant les activités des États dans le cyberespace. Cette stratégie devrait articuler clairement la vision, les valeurs et les objectifs du Canada afin d'assurer un cyberespace sécuritaire et stable. Notamment, le Canada devrait s'engager à prendre des mesures concrètes pour éviter la poursuite d'une course aux cyberarmements et cesser la conduite d'opérations offensives dans le cyberespace contribuant à une montée des tensions internationales. Par ailleurs, compte tenu du rôle important joué par le secteur privé, la société civile et le milieu universitaire en matière de cybersécurité, le document devrait être élaboré en partenariat avec les provinces et des représentants de chacun de ces secteurs.

Quant au Québec, il devrait accélérer la préparation et le dévoilement de sa propre politique de cybersécurité, et ne devrait par ailleurs pas hésiter à y inclure un volet international. Les enjeux de cyberdéfense au Québec sont particulièrement importants puisque les gouvernements provinciaux entretiennent une plus grande proximité avec leurs populations, et peuvent ainsi aider leurs citoyens à agir de façon plus sécuritaire en ligne. Le gouvernement du Québec peut également promouvoir la cybersécurité dans le secteur privé par l'établissement de programmes provinciaux.

2. Promouvoir la coopération internationale en matière de cybersécurité : à l'ère de l'interdépendance numérique, nul pays ne peut affronter les défis seul.

Le Canada et le Québec doivent continuer à promouvoir la coopération en matière de cybersécurité internationale. Les États partagent un intérêt commun et une responsabilité collective d'atténuer et de limiter la prolifération des cybermenaces. Il est donc dans l'intérêt des gouvernements canadien et québécois de favoriser la collaboration avec des acteurs étatiques et non-étatiques afin d'établir des stratégies de gouvernance et de sécurité qui sauront limiter l'impact et la prolifération des cyberattaques. Il existe déjà plusieurs mécanismes de coopération internationale, tels que les deux initiatives de l'ONU – GEG et le Groupe de travail à composition non-limitée – au sein desquelles le Canada continue de s'impliquer. Par ailleurs, d'autres mécanismes tels que le Forum mondial sur la Cyber Expertise (GFCE), dont le Canada est également membre, offrent une voie alternative pour les États et les acteurs non-étatiques afin de discuter des enjeux internationaux du cyberespace. Or, ce dernier n'inclut pas les États aux opinions divergentes (Chine et Russie), ce qui limite sa portée, et ne possède pas le même créneau sur le plan juridique international. Ainsi, le défi pour le Canada dans les prochaines années sera de choisir avec attention son mécanisme de prédilection afin de ne pas gaspiller ses efforts et de s'assurer de bâtir un dialogue constructif en voie de l'adoption et du respect de normes internationales.

Quant au Québec, il pourrait également tenter d'accroître sa représentation sur la scène internationale en participant aux différentes initiatives en matière de coopération pour la cybersécurité internationale. Par exemple, le Québec pourrait emboîter le pas au Canada et signer l'Appel de Paris du 12 novembre

2018 pour la confiance et la sécurité dans le cyberespace[29], déjà soutenu par 76 pays et 26 organismes publiques et administration territoriale, ou encore devenir membre du GFCE.

3. Développer des ententes bilatérales ou des coalitions non seulement avec des États ayant une vision semblable, mais aussi avec des États ayant une vision divergente.

En raison des difficultés de l'ONU de parrainer l'élaboration de normes de cybersécurité internationales et, de fait, de minimiser les tensions entre les grandes puissances, l'adoption d'ententes bilatérales pourrait s'avérer une bonne option pour le Canada dans son effort de se positionner en leader de la gouvernance mondiale du cyberespace. Le Canada devrait tenter d'adopter des ententes avec des pays aux vues similaires afin de façonner les normes internationales qui répondent à ses valeurs et intérêts. Or, aucune stabilité internationale ne peut être atteinte sans l'inclusion des puissances émergentes, et aux vues divergentes, telles que la Chine et l'Inde. Certes, il existe des perspectives distinctes sur la manière dont l'application de la technologie devrait être régie au-delà des frontières. Il apparaît toutefois plus constructif d'identifier et de focaliser sur les quelques points communs que de s'enfoncer dans un dialogue de sourds. Le Canada devrait donc cibler des enjeux sur lesquels il partage une vision semblable afin de bâtir une collaboration durable. Pour ce faire, Affaires Mondiales Canada pourrait travailler avec ses homologues étrangers afin de générer des ententes sur le développement et l'utilisation des technologies numériques.

4. Définir et clarifier le rôle et les responsabilités du secteur privé.

Alors que la plupart des stratégies nationales et internationales de cybersécurité misent sur la collaboration avec les entreprises, il demeure difficile de déterminer clairement quels acteurs engagent leurs responsabilités pour assurer la protection des renseignements privés et confidentiels des individus. Cette problématique concerne également les infrastructures essentielles du cyberespace qui sont opérées par le secteur privé.

Le Canada devrait se faire pionnier et clarifier le rôle et les responsabilités de ses entreprises privées en matière de cybersécurité nationale et internationale, à savoir qui est responsable de protéger le Canada, ses infrastructures essentielles, l'information et les données de ses citoyens, particulièrement contre une menace extérieure. De même, au sein de sa future politique de cybersécurité, le Québec devrait s'assurer de clarifier le partage des responsabilités entre les différents ministères et les entreprises privées.

« Il faut développer une stratégie de gestion des infrastructures essentielles dont le contrôle appartient totalement ou en partie à des entreprises étrangères (particulièrement dans le secteur des réseaux et des télécommunications), par exemple en ce qui concerne le déploiement de nouvelles technologies telles que la 5G. »

De plus, le gouvernement fédéral devrait développer, à l'aide du secteur privé et des gouvernements provinciaux, une structure joignant les secteurs privé et public dont l'un des mandats serait d'établir un processus à suivre en cas de cyberincident menaçant le secteur privé, mais pouvant atteindre des proportions nationales. Une agence publique-privée attribuant des pouvoirs égaux aux deux secteurs en matière décisionnel, et non uniquement sur le plan consultatif, représenterait une solution novatrice. Quant au plan de réponse, il devrait tenir compte des menaces provenant (ou étant parrainées par) d'États étrangers et

[29] République française, Ministère de l'Europe et des Affaires Étrangères (2018), « Appel de Paris pour la confiance et la sécurité dans le cyberespace », disponible à l'adresse suivante: https://pariscall.international/fr/

touchant à la fois à la cybercriminalité, aux opérations d'espionnage et aux risques de destruction et de perturbation des systèmes et réseaux. Le Québec devrait également se doter d'un protocole en cas de cyberattaque, non seulement envers les systèmes gouvernementaux, mais aussi envers le secteur privé.

Finalement, le secteur privé ne peut réduire les problèmes systémiques par lui-même. Le marché actuel ne favorise pas d'investir dans la sécurité parce que l'adoption d'une approche plus sécuritaire engendre d'importants coûts supplémentaires nuisant à la compétitivité. C'est pourquoi le Canada et le Québec devraient adopter des programmes incitatifs de financement, et davantage de réglementation, encourageant les entreprises privées à placer la sécurité au cœur du développement de nouvelles technologies, ainsi qu'à divulguer les vulnérabilités existantes.

5. Adopter une réglementation quant à l'utilisation et la monétisation des données individuelles et confidentielles

Afin d'assurer le maintien et la protection de la sécurité humaine à l'ère numérique, le Canada et le Québec devraient établir une réglementation claire en ce qui concerne la monétisation des données et l'information privée des particuliers. Les individus doivent avoir un plus grand contrôle sur l'exploitation et l'utilisation de leurs données personnelles. Par ailleurs, il s'agit de protéger le climat social et la démocratie en évitant que les données puissent être utilisées, via les plateformes numériques, pour accroître l'instabilité, la polarisation et l'influence.

Ainsi, le Canada et le Québec doivent s'engager à prioriser la sécurité et la dignité humaines ainsi que le respect des droits de la personne, notamment au sein de sa future stratégie internationale de cybersécurité et de ses efforts d'élaboration de cybernormes internationales.

6. Faire preuve de transparence en matière de surveillance et contrôler davantage l'exportation de technologies numériques à l'étranger

Le Canada devrait faire preuve de transparence en ce qui concerne les activités de cybersurveillance de ses organismes de sécurité, tels que le Centre de Sécurité des Télécommunications (CST) et le Service canadien du renseignement de sécurité (SCRS). Il serait ainsi plus facile pour le Canada de promouvoir le respect des droits de la personne à l'international s'il est en mesure de démontrer concrètement sa bonne foi, autant sur le plan de ses activités internes que de ses activités d'espionnage.

Respectant les recommandations du Rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression, le Canada devrait également adopter une politique claire en matière d'exportation de technologies de surveillance. Au sein de sa future stratégie internationale de cybersécurité, le Canada devrait affirmer et promouvoir l'importance du respect de la vie privée et de la liberté d'expression en ligne.

7. Autoriser et promouvoir le chiffrement des plateformes et outils numériques

S'il souhaite se promouvoir de façon crédible en tant que défenseur des droits de la personne, le Canada doit maintenir l'autorisation du chiffrement des plateformes et outils numériques. Le chiffrement est essentiel aux activités des groupes de défense des droits de la personne, des journalistes et de l'exercice par l'ensemble des individus en général de leur droit d'expression et du respect à la vie privé. Par ailleurs, le chiffrement assure la cybersécurité nationale du Canada en protégeant les données confidentielles des gouvernements fédéral et provinciaux contre le cyberespionnage, ainsi que de l'ensemble des citoyens, en plus d'être essentiel pour les communications et opérations militaires et les activités des

forces de l'ordre et des services de renseignement. En adoptant une position claire autorisant et valorisant le chiffrement, le Canada pourrait se démarquer sur la scène internationale à la fois sur le plan de la cybersécurité et sur le plan de la défense du respect de la vie privée. La future stratégie internationale devrait ainsi clairement énoncer la position du Canada et promouvoir le chiffrement sur le plan international.

Conclusion

La cybersécurité est un enjeu transnational qui dépend de la coopération entre une grande variété d'acteurs étatiques et non étatiques. Dans ce contexte émergent d'interconnexion et d'intégration, des interactions purement contradictoires entre les principaux acteurs et une incapacité à collaborer pour la protection et la stabilité du cyberespace pourraient représenter une menace importance pour l'ensemble du système international, y compris l'économie mondiale dont la stabilité dépend désormais des technologies de l'information et de communication. Le Canada est en mesure d'agir en tant qu'entrepreneur dans la gouvernance mondiale. Pour ce faire, il doit se démarquer et avoir sa propre voix pour la promotion à la fois des droits de la personne, du multilatéralisme, du respect des normes internationales et de la stabilité de l'économie mondiale. Quant au Québec, il a également un rôle important à jouer, sur le plan provincial, national et international, afin de renforcer la cybersécurité de l'ensemble des citoyens.

Institut d'études internationales de Montréal
Université du Québec à Montréal
400, rue Sainte-Catherine Est
Bureau A-1540, Pavillon Hubert-Aquin
Montréal (Québec) H2L 3C5

514 987-3667
ieim@uqam.ca
www.ieim.uqam.ca

UQÀM | I E I M Institut d'études internationales de Montréal 15 ans

Auteurs

Karine Pontbriand

Claude-Yves Charron

Luc Dandurand

Citation :

Karine Pontbriand, Claude-Yves Charron et Luc Dandurand, « La stratégie internationale du Canada en matière de cybersécurité : enjeux et recommandations », *Document de recommandations politiques*, N°3, Institut d'études internationales de Montréal, Université du Québec à Montréal, février 2020.