Introduction

Les cybermenaces sont devenues un défi de premier plan pour la sécurité internationale. Trois tendances l'ont rendu ainsi : la vulnérabilité des réseaux et des données du cyberespace, la transformation numérique de la société mondiale et un manque d'investissement de la part des organisations et des gouvernements dans les personnes, les processus et les technologies nécessaires pour dissuader les cyberattaques et se défendre contre celles-ci. Les gouvernements, les entreprises et les organisations ont pris des mesures pour améliorer leur dispositif de cybersécurité en créant des équipes de cybersécurité, en élaborant des politiques et des mécanismes d'intervention et en mettant en place des technologies de sécurité, mais les progrès ont été insuffisants pour faire face à cette menace.

L'environnement de la menace

Les attaquants étatiques et non étatiques volent, détruisent et manipulent des données dans et à travers le cyberespace. Quoique des hostilités n'aient pas encore été déclarées par le biais d'une cyberattaque, les adversaires s'épanouissent dans « l'espace gris[i] » sous le niveau d'un conflit pur et simple et ne semblent pas découragés dans la poursuite de leurs objectifs. Parmi les attaques récentes importantes contre les intérêts nationaux des États-Unis, notons la campagne menée par la Chine pour voler la propriété intellectuelle américaine, y compris les données de l'avion de combat interarmées (F-35)[ii], le vol de 81 millions de dollars de la Banque centrale du Bangladesh et de la Réserve fédérale américaine par la Corée du Nord en 2015[iii], le vol de 21,5 millions de dossiers personnels fédéraux par la Chine auprès du U.S. Office of Personnel Management (OPM)[iv] et les attaques russes sur le réseau électrique ukrainien en 2015-2016[v]. Ce ne sont là que quelques exemples.

Les acteurs étatiques représentent la plus grande menace dans le cyberespace car ils ont les ressources nécessaires pour payer les pirates informatiques et peuvent travailler avec diligence au fil du temps pour atteindre une cible. Au cours des dernières années, ils sont passés du vol et de la destruction de données à la manipulation des données à des fins politiques et médiatiques, modifiant la façon dont les populations perçoivent les événements politiques et la nature de la société dans son ensemble. Le piratage russe de l'élection présidentielle américaine de 2016 en est l'exemple parfait. Sous la direction du président russe Vladimir Poutine, les services de renseignements militaires russes ont piraté les réseaux des organisations politiques et des dirigeants politiques américains et ont exploité les vulnérabilités des pratiques commerciales des médias sociaux afin de répandre la propagande et susciter la méfiance au sein de la population américaine[vi]. L'opération russe a touché trois parties du « centre de gravité » américain pendant une période de transition politique : la population américaine, les dirigeants politiques et les principales entreprises technologiques. Depuis cet incident, d'autres États ont posé des gestes similaires; la Chine aurait pénétré les réseaux électoraux du Cambodge en 2018, ce qui lui offrirait la possibilité d'une manipulation électorale[vii].

Pourquoi le problème est-il si grave? Le problème découle en partie des tendances socio-économiques mondiales. L'urbanisation accrue, la prolifération de technologies abordables à double usage et la nature interconnectée de l'économie mondiale signifient que de plus petits groupes de personnes peuvent avoir un impact disproportionné par rapport à leur taille. Le sociologue britannique Anthony Giddens qualifie ce phénomène de « risque à conséquences élevées » de la modernité. Parmi les exemples historiques, mentionnons les attaques terroristes d'Al-Qaïda, les actions des prêteurs à risque et leur impact sur le marché hypothécaire et, plus récemment, l'opération du gouvernement russe dans le cyberespace contre l'élection présidentielle américaine. Tout comme lors de l'attaque d'Al-Qaïda du 11 septembre 2001, alors que 19 hommes ont passé inaperçus devant les services de sécurité et ont transformé des avions en missiles, un petit groupe d'agents russes a trouvé une faille dans la sécurité américaine et mené une attaque asymétrique à haut risque.

L'Internet est passé de zéro à 3,8 milliards d'utilisateurs en moins de 35 ans[viii] et l'accès aux données a augmenté sans que l'on ait une compréhension proportionnée ou populaire du risque, qu'il s'agisse de la vulnérabilité du code informatique ou de l'impact des enclaves des médias sociaux sur la formation de l'identité sociopolitique[ix]. Les réseaux, les centres de données et les environnements nuagiques sont vulnérables aux violations – et la société est vulnérable à la manipulation.

Dissuasion et défense

Les pays devraient en premier lieu se concentrer à dissuader les cyberattaques étatiques. La dissuasion est une question de perception et elle fonctionne en convainquant un adversaire potentiel que les coûts d'une attaque seront supérieurs aux avantages que ce dernier en retirera. Une dissuasion efficace exige la capacité d'imposer des coûts à un attaquant (c.-à-d. par des sanctions ou des moyens militaires), des outils défensifs pour repousser une attaque entrante, comme des pare-feu, et, dans le cas où un pirate enfreint le périmètre, des capacités de résilience pour limiter son impact, notamment la micro-segmentation. Les investissements dans chacun de ces outils peuvent aider à modifier l'équilibre coûts-avantages afin de dissuader les attaques. Ce témoignage examinera chacun de ces points.

Pour un pays axé sur la dissuasion, la défense et la résistance à une cyberattaque, la première étape consiste à formuler une stratégie pour les secteurs public et privé[x]. En termes plus simples, une stratégie devrait identifier les intérêts d'un pays ou d'une organisation, évaluer les forces, les faiblesses, les opportunités et les risques, fixer des buts et des objectifs et identifier les investissements nécessaires dans les personnes, les processus et la technologie. Pour mettre en place une stratégie de cybersécurité, les gouvernements doivent aussi harmoniser leurs rôles et leurs missions – un processus qui a pris des années à se développer aux États-Unis et qui continue d'évoluer[xi]. Le Canada a fait des progrès à cet égard et la Stratégie nationale sur la cybersécurité de 2018 offre une plate-forme sur laquelle s'appuyer.

Aux États-Unis, le secteur privé a développé ses capacités de cybersécurité par lui-même et avec l'aide du gouvernement américain. Un certain nombre d'intrusions très médiatisées ont amené le secteur financier à investir considérablement et, aujourd'hui, c'est ce dernier et le secteur des technologies de l'information qui sont les plus matures dans leurs capacités et leur approche réglementaire. D'autres secteurs ont investi, mais ils sont plus en retard.

Parmi les développements positifs survenus à l'échelle mondiale entre les secteurs public et privé, mentionnons l'essor des centres (ISAC) et des organisations (ISAO) d'analyse et de partage de l'information, le développement du cadre de cybersécurité du National Institute of Standards and Technology (NIST), l'évolution du contexte réglementaire, notamment la réglementation européenne de la protection des données générales, les lois des États du Colorado et de la Californie, la *Loi sur la protection des renseignements personnels et les documents électroniques du Canada*[xii] et le Department of Financial Services (DFS) de l'état de New York sur la cybersécurité[xiii]. Les gouvernements doivent maintenant faire respecter la conformité organisationnelle.

« Se défendre en amont »

Deux propositions se dégagent de l'histoire récente visant à éclairer l'enquête du Comité. Premièrement, les adversaires se sont multipliés dans le cyberespace, et ce, malgré les efforts de dissuasion du gouvernement américain. Les États-Unis et d'autres pays doivent donc adopter une position plus agressive pour dissuader l'agression. En 2018, le gouvernement américain a adopté une telle position, notamment par le biais de la théorie du ministère de la Défense de « se défendre en amont » dans le cyberespace[xiv].

Au fil des dernières années et au fur et à mesure que les adversaires se sont multipliés, les États-Unis ont souvent choisi de les inculper ou de les sanctionner. Ces mesures d'intervention, bien que raisonnables, ne semblent pas avoir créé un précédent ni dissuadé efficacement l'escalade. Par exemple, même après avoir sanctionné la Russie pour le piratage de l'élection présidentielle de 2016, la Russie aurait continué à implanter des logiciels malveillants sur le réseau électrique américain jusqu'à la fin de 2018[xv]. Chaque nouveau piratage indique que la dissuasion ne fonctionne pas dans l'espace gris sous le niveau de conflit pur et simple.

Alors, que signifie « se défendre en amont » dans le cyberespace? Depuis des années, le U.S. Cyber Command collabore avec la National Security Agency et la communauté du renseignement pour surveiller les adversaires et leur infrastructure afin de se préparer à atténuer et à perturber les cyberattaques entrantes. Si le U.S. Cyber Command a déjà mené une opération de contre-offensive pour émousser une cyberattaque, cela s'est fait hors de l'œil du public. Les militaires seraient intervenus en octobre 2018 lorsqu'ils ont envoyé des messages directs à des agents russes pour les avertir que s'ils menaient une attaque, les États-Unis prendraient des mesures[xvi]. Cette opération n'a pas perturbé la cyberinfrastructure de l'adversaire, mais elle a prévenu de manière proactive les adversaires qu'ils étaient surveillés.

S'ils disposent d'indices et d'avertissements d'une cyberattaque imminente, les États-Unis doivent riposter contre un adversaire, et ce, s'ils ont la moindre chance d'atteindre la dissuasion; une politique plus agressive est donc la bonne approche. D'autres pays peuvent parvenir à des conclusions similaires à celles des États-Unis; les États-nations ont le droit de se défendre contre l'hostilité, y compris l'hostilité dans le cyberespace. Pour maintenir la paix et la stabilité, toute opération doit être menée dans le cadre du droit des conflits armés et avec le soutien des pays alliés et partenaires. À cette fin, les Nations Unies devraient continuer de promouvoir des normes de comportement pour les opérations du cyberespace afin de contrôler l'escalade et de gérer les conséquences non voulues[xvii].

Supposer qu'il y a eu intrusion

La nécessité d'un dispositif de dissuasion plus vigoureux est l'une des premières mesures prises depuis la dernière décennie concernant la politique de cybersécurité. La seconde est la nécessité de « supposer qu'il y a eu intrusion » et de prévoir que les adversaires pénétreront les défenses périmétriques et auront accès aux applications de l'entreprise.

Qu'est-ce que cela signifie? Bien que les organisations soient au courant de certaines de leurs applications les plus critiques (c.-à-d. une base de données), la plupart d'entre elles ne possèdent pas de diagramme sur la façon dont ces applications interagissent et n'ont pas encore sécurisé leurs centres de données et leurs environnements nuagiques à l'interne. Le manque de sécurité interne rend les organisations vulnérables à la propagation des atteintes à la sécurité. Une fois qu'un pirate informatique a pénétré un réseau, le temps moyen pour un intrus de s'installer dans un centre de données est de six mois; pendant ce temps, il peut se déplacer sans encombre et implanter des logiciels malveillants dans le but qu'il s'est ultimement fixé. Les applications d'une entreprise, comme ses bases de données clés, sont facilement accessibles pour qu'un pirate puisse les voler, les détruire ou les manipuler.

Prenons l'exemple du piratage chinois du U.S. Office of Personnel Management (OPM). L'une des plus petites agences du gouvernement américain; l'OPM est l'agence « principale des ressources humaines » pour le personnel gouvernemental. En 2015, l'OPM a repoussé plus de 10 millions d'attaques par mois. Lorsqu'un intrus franchissait inévitablement les défenses périmétriques de l'OPM, il se déplaçait facilement dans l'environnement. Pendant des mois, l'intrus a sauté d'un serveur à l'autre jusqu'à ce qu'il trouve les applications de l'entreprise : les renseignements personnels identifiables de 21,5 millions d'employés

fédéraux[xviii]. Il n'existait aucune règle régissant l'interaction interne des applications et des serveurs. Les portes ont été laissées grandes ouvertes.

Renforcer la résilience : la micro-segmentation

La micro-segmentation suppose qu'à un moment donné vous serez victime d'une intrusion, ce qui permettra d'établir une défense interne afin d'empêcher les intrusions de se propager. À son niveau le plus élémentaire, il place des murs autour des applications vitales afin de les isoler du reste de l'environnement nuagique, du centre de données et de l'Internet ouvert. Un intrus pourrait s'introduire dans trois serveurs, mais pas 3 000. Comme la micro-segmentation fonctionne avec l'infrastructure existante, elle atténue également les risques liés aux architectures existantes, comme les serveurs ou les applications non corrigés.

Aujourd'hui, au Canada et dans le monde entier, la plupart des organisations investissent dans la défense périmétrique. Mais sécuriser l'extérieur ne suffit pas. La micro-segmentation fournit une base profonde pour la cyberrésilience – la dernière ligne de défense dans la suite d'investissements de sécurité d'une organisation. Pour les infrastructures critiques comme le secteur financier, une telle cybersécurité améliore la santé des États-nations qu'elle dessert.

Conclusion

Il ne s'agit pas de savoir *si*, mais *quand*, une intrusion se produira. Les pays doivent se défendre de manière proactive contre les agresseurs pour parvenir à la dissuasion, mais ils doivent également supposer qu'il y a eu intrusion et mettre en place des stratégies de défense en profondeur pour résister aux cyberattaques.

Le leadership permet de réussir dans toutes les parties du projet de cybersécurité. Dans son premier essai, intitulé « The Challenge of Change », l'historien Arthur M. Schlesinger a déclaré : « La science et la technologie révolutionnent nos vies, mais la mémoire, le mythe et la tradition encadrent notre réponse. » Cela est vrai – et notre capacité à gérer le changement technologique dépend en fin de compte du succès du chef de file et de sa capacité à raconter une histoire qui permettra d'obtenir des résultats, de gérer des équipes et de prendre des décisions stratégiques pour la société.

Après une décennie d'efforts ciblés, nous avons aujourd'hui une poignée de chefs de file en matière de cybersécurité à travers les États-Unis. Le progrès et l'évolution de la technologie ne s'arrêteront peut-être jamais, mais de bons chefs de file ont toujours aidé la société à s'adapter et à gérer le changement, depuis l'essor de l'aviation jusqu'à l'aube de l'ère nucléaire. La cybersécurité n'est que le dernier chapitre de notre histoire. En fin de compte, le leadership repose sur une analyse solide, ce qui rend le travail de ce comité d'autant plus important. Je vous remercie, et je suis prêt à répondre à vos questions.

---

[i] https://www.csis.org/analysis/five-risks-watch-2019 [DISPONIBLE EN ANGLAIS SEULEMENT].
[ii] https://www.popularmechanics.com/military/aviation/g23303922/china-copycat-air-force/ [DISPONIBLE EN ANGLAIS SEULEMENT].
[iii] https://news.abs-cbn.com/business/09/07/18/us-charges-north-korean-in-bangladesh-central-bank-sony-hacks [DISPONIBLE EN ANGLAIS SEULEMENT].
[iv] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [DISPONIBLE EN ANGLAIS SEULEMENT].
[v] https://www.wired.com/story/russian-hackers-attack-ukraine/ [DISPONIBLE EN ANGLAIS SEULEMENT].
[vi] https://www.dni.gov/files/documents/ICA_2017_01.pdf [DISPONIBLE EN ANGLAIS SEULEMENT].
[vii] https://www.apnews.com/0b52e20517a74b678cf5eae5d0e177ab [DISPONIBLE EN ANGLAIS SEULEMENT].
[viii] https://cltc.berkeley.edu/wp-content/uploads/2017/12/asianfutures.pdf [DISPONIBLE EN ANGLAIS SEULEMENT].
[ix] Sur cette question, qui n'est pas notre principal point d'enquête, voir *entre autres* Nathaniel Persily, https://www.journalofdemocracy.org/article/can-democracy-survive-the-internet, et Cass Sunstein, *Republic.com 2.0*, https://www.jstor.org/stable/j.ctt7tbsw [DISPONIBLE EN ANGLAIS SEULEMENT].
[x] Ceci est plus difficile à réaliser qu'il n'y paraît. Aux États-Unis, les principaux organismes responsables de la cybersécurité sont le Department of Homeland Security, le Federal Bureau of Investigation et le Department of Defense, chacun ayant des missions

précises. Le Department of Homeland Security met à contribution le secteur privé aux États-Unis et, dans certains cas, à l'étranger, en matière de préparation, d'atténuation et de redressement en cas d'attaque; il est l'organisme responsable de la sécurité des infrastructures essentielles du pays dans leur ensemble, y compris en matière de cybersécurité. Le Federal Bureau of Investigation mène des opérations d'application de la loi au pays pour empêcher les criminels et les États-nations de mener des cyberattaques; il s'agit du seul organisme autorisé à mener des opérations de contre-offensive sur des réseaux basés aux États-Unis, une autorité importante pour contourner et bloquer un attaquant étranger qui utilise un serveur basé aux États-Unis pour attaquer ses intérêts américains. Le Department of Defense s'emploie à défendre les réseaux militaires, se prépare à défendre les États-Unis contre d'importantes attaques venant de l'étranger et mène des opérations dans le cyberespace pour mettre fin à un conflit dans des conditions favorables aux États-Unis, comme dans le cas des opérations du cyberespace contre Daesh. Au sein de l'armée, la principale organisation responsable des opérations du cyberespace, le U.S. Cyber Command, est dirigée par un général quatre étoiles ou un officier général dans la chaîne de commandement du secrétaire à la Défense et du président. Celle-ci a été lancée en 2010 et est appuyée par la Cyber Mission Force, qui compte 6 200 militaires, et a atteint sa pleine capacité opérationnelle en 2018. En collaboration avec le FBI, le DHS et la CIA, le Department of Defense s'efforce de dissuader les attaques contre les intérêts nationaux américains. La Central Intelligence Agency a également un rôle opérationnel à jouer dans l'analyse et dans les opérations secrètes si elles sont accordées sous l'autorité présidentielle. Compte tenu de leurs pouvoirs uniques, tous ces organismes travaillent en étroite collaboration avec le National Security Council et d'autres mécanismes de coordination dans le cadre d'une planification et d'un partenariat opérationnel étroits.

[xii] https://laws-lois.justice.gc.ca/fra/lois/P-8.6/.
[xiii] https://www.dfs.ny.gov/about/cybersecurity.htm [DISPONIBLE EN ANGLAIS SEULEMENT].
[xiv] https://cdn.defenseone.com/b/defenseone/interstitial.html?v=8.24.1&rf=https%3A%2F%2Fwww.defenseone.com%2Fideas%2F2018%2F11%2Fwhat-happens-when-us-starts-defend-forward-cyberspace%2F152580%2F [DISPONIBLE EN ANGLAIS SEULEMENT].
[xv] https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html [DISPONIBLE EN ANGLAIS SEULEMENT].
[xvi] https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html [DISPONIBLE EN ANGLAIS SEULEMENT].
[xvii] https://www.un.org/disarmament/topics/informationsecurity/ [DISPONIBLE EN ANGLAIS SEULEMENT].
[xviii] https://www.opm.gov/cybersecurity/cybersecurity-incidents/ [DISPONIBLE EN ANGLAIS SEULEMENT].