CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 148 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 6 février 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 6 février 2019

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Mesdames et messieurs, la séance est ouverte.

Tout d'abord, si vous le permettez, j'aimerais régler une question de régie interne. Le sous-comité a accepté notre proposition d'inviter les ministres le 25 février prochain.

Qui veut proposer l'adoption de cette motion?

Merci, monsieur Motz.

J'aimerais simplement dire à mes collègues et aux témoins que nous risquons d'être interrompus. Toutefois, nous tenterons de fonctionner aussi normalement que possible. Si les lumières se mettent à clignoter et que la sonnerie commence à retentir, il se peut que je demande au Comité de poursuivre ses travaux.

Un des témoins nous arrive de la Californie. Nous devrions tenir compte du long voyage qu'il a dû faire.

De toute manière, nous n'aurons qu'à passer à l'étage supérieur. Je ne veux pas...

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Devrions-nous commencer par lui?

Le président: Est-ce que M. Porter est arrivé lui aussi? Il est parti de...

M. Christopher Porter (chef d'intelligence stratégique, FireEye, Inc.): Oui, j'arrive de Washington.

Le président: Oh, d'accord. Cela ne compte pas vraiment.

M. Christopher Porter: D'une capitale glaciale à une autre.

Le président: Oui, c'est bien vrai.

Je me suis rendu au Pentagone en juin dernier. Je préside la commission mixte de défense. Une année, la réunion se tient à Ottawa, tandis que l'année suivante, elle a lieu à Washington.

Les Capitals de Washington venaient de gagner la coupe Stanley. Mon homologue américain s'est trouvé très drôle en me remettant une rondelle de Washington. Ce à quoi j'ai rétorqué: « Ouais, vos Russes ont très bien joué. »

Sur ce, je donne la parole pendant 10 minutes à M. Porter, qui nous arrive directement de Washington.

M. Christopher Porter: Merci, monsieur le président. Je suis heureux de pouvoir vous faire part du point de vue de FireEye sur les menaces qui planent sur le secteur canadien des services financiers et vous présenter un aperçu de la façon dont notre entreprise et le secteur privé en général travaillent en partenariat avec le gouvernement pour contribuer à la défense de ce secteur.

Comme le président l'a dit, je m'appelle Christopher Porter. J'occupe les fonctions de chef d'intelligence stratégique chez FireEye, une société spécialisée dans la cybersécurité. Nous comptons plus de 4 000 clients répartis dans 67 pays. Aujourd'hui, mon témoignage portera sur les leçons que nous avons tirées de nos interventions à la suite d'incidents partout dans le monde, ainsi que sur le renseignement que nous recueillons sur les menaces qui touchent spécifiquement le Canada.

En plus de mes fonctions chez FireEye, je suis agrégé supérieur de recherches non résident auprès du Conseil de l'Atlantique et, jusqu'en 2016, j'ai servi pendant presque neuf ans au sein de la Central Intelligence Agency des États-Unis. Dans le cadre de ce dernier poste, j'ai été responsable des séances d'information sur le renseignement touchant les cybermenaces destinées au personnel du Conseil de la sécurité nationale de la Maison-Blanche, j'ai été affecté pendant plusieurs années à des opérations antiterroristes et j'ai servi brièvement dans une zone de guerre.

FireEye compte plus de 300 professionnels de la sécurité, qui réagissent à des intrusions informatiques à l'échelle internationale, ainsi que plus de 200 analystes des cybermenaces, qui oeuvrent dans 18 pays. Ensemble, ces gens parlent plus de 30 langues. Ils nous aident à prévoir qui seront nos adversaires et à mieux les comprendre, souvent en tenant compte du contexte politique et culturel des auteurs de menaces. FireEye, qui, à l'origine, était une entreprise technologique, dispose maintenant de ces capacités. Nous avons amassé énormément de renseignements sur les menaces et continuons d'en recueillir tous les jours, alors que ne cessent de se multiplier les attaques contre des organisations partout dans le monde.

Nous entretenons aussi des liens étroits avec le Canada. Les dispositifs de FireEye détendent tous les jours les boîtes de courriel du gouvernement du Canada, et nous travaillons en étroite collaboration avec les institutions canadiennes chargées de la sécurité publique pour assurer la sécurité des Canadiens en défendant leurs réseaux et en soutenant les enquêtes.

Aujourd'hui, je vais me concentrer sur les cybermenaces auxquelles les banques, les sociétés d'investissement et les organismes gouvernementaux de réglementation du secteur financier canadiens doivent faire face à l'heure actuelle, ainsi que sur les cybermenaces auxquelles ils risquent d'être confrontés dans un avenir rapproché. Nous vivons à une époque où la façon dont les cyberopérations sont déployées change rapidement, en particulier dans les États-nations. Les outils qui, autrefois, étaient utilisés de manière soigneuse, discrète et illicite par des espions pour recueillir des renseignements tombent de plus en plus souvent entre les mains d'officiers militaires qui sont prêts à passer à l'offensive et à causer des perturbations et des torts graves.

C'est particulièrement le cas pour le Canada, qui est souvent l'un des premiers pays ciblés par de nouveaux types de cyberopérations. Comme le Canada présente un PIB par habitant élevé, il constitue une cible de choix pour les auteurs d'activités criminelles motivés par l'appât du gain. Le Canada est un chef de file mondial dans la mise au point de technologies de pointe, notamment dans certains créneaux de technologies à double usage, c'est-à-dire celles qui ont des applications tant militaires que civiles. Le Canada est donc constamment ciblé par les services de renseignement étrangers. En tant que pays membre de l'OTAN, largement présent dans le monde entier, tant sur le plan diplomatique qu'au chapitre des investissements, le Canada est une cible naturelle de représailles motivées par des raisons politiques de la part d'acteurs internationaux.

Au Canada, les particuliers et les entreprises sont aussi la cible d'un éventail de menaces, allant des intrusions criminelles délibérées et perfectionnées aux logiciels malveillants qui se propagent dans le monde entier et qui ne touchent les Canadiens que par inadvertance.

Par exemple, en février 2017, plusieurs grandes institutions financières canadiennes ont été exposées à un risque de cybervol parrainé par la Corée du Nord. À l'époque, l'autorité polonaise de surveillance financière a mis ses systèmes hors ligne après s'être rendu compte qu'un code malicieux introduit dans son serveur Web était utilisé pour rediriger certaines cibles vers des liens permettant de télécharger des fichiers malveillants qui prenaient le contrôle des ordinateurs. On sait que ces assaillants ont utilisé une liste blanche d'adresses IP pour déterminer les personnes qui allaient recevoir la charge désignée. De nombreuses institutions financières canadiennes figuraient tout en haut de la liste des entités ciblées. Même si la menace se trouvait en Pologne, elle a tout de même fait son chemin jusqu'au Canada.

Les campagnes qui ont recours notamment à des logiciels rançonneurs, au crypto-détournement et, surtout, à des maliciels servant à voler les justificatifs d'identité représentent une menace grave pour la population canadienne. La fraude liée aux cartes de crédit soulève de grandes inquiétudes. FireEye met régulièrement au jour d'importants forums clandestins qui vendent des milliers de cartes de crédit volées, parfois de grandes institutions financières. Ces forums ciblent aussi très souvent les comptes clients d'institutions bancaires et de coopératives de crédit de taille modeste.

En outre, le Canada est souvent l'une des premières cibles des nouvelles campagnes de maliciel. Une banque canadienne a été l'une des cinq premières institutions financières au monde à être ciblées par le maliciel TrickBot. Depuis, nous avons remarqué que d'autres institutions financières ont été ajoutées dans les fichiers de configuration TrickBot qui sont présents ou basés au Canada. Par exemple, des adresses URL canadiennes sont apparues dans tous les identificateurs de campagne TrickBot. Plusieurs des entités visées étaient des coopératives de crédit ou de petites banques. En août 2017, nous avons aussi découvert un fichier de configuration PandaBot qui a révélé que 15 grandes institutions financières canadiennes avaient été ciblées.

● (1535)

Au moins une demi-douzaine de groupes du crime organisé mènent aussi des opérations criminelles de nature financière en ciblant des entreprises et des citoyens canadiens. Leurs opérations sont maintenant aussi perfectionnées que celles qui, autrefois, étaient l'apanage des États-nations. Un groupe en particulier, que FireEye appelle FIN10, s'en prend spécifiquement au Canada depuis 2013. Il s'adonne souvent à des intrusions contre des organismes spécialisés dans les jeux de hasard et l'exploitation minière, exfiltre des données commerciales et extorque de l'argent à ses victimes.

Compte tenu des intrusions, des activités de menace clandestines, des vastes campagnes de maliciel et de la présence d'auteurs de menaces au pays, le Canada continuera probablement de faire face à des menaces criminelles complexes et exigeantes à court et à moyen terme.

Au Canada, la menace de cyberespionnage est modérée, mais elle pourrait s'aggraver. Au cours des dernières années, nous avons remarqué que 10 groupes de cyberespionnage distincts basés en Chine, en Russie et en Iran avaient pris pour cible le Canada. Des entités oeuvrant notamment dans les secteurs du gouvernement, de la défense, de la haute technologie, des organismes sans but lucratif, du transport, de l'énergie, des télécommunications, de l'éducation et des médias ont été touchées, comme c'est le cas dans bien d'autres pays occidentaux.

Depuis le milieu de l'année 2017, de nombreux groupes chinois auteurs de cybermenaces ont recommencé à s'adonner au vol de technologies ayant des applications militaires et sont susceptibles d'accentuer leurs efforts en ce sens, alors qu'apparaissent des différends commerciaux avec le Canada et ses alliés. Cette situation a pour effet d'augmenter considérablement le risque pour les entreprises commerciales canadiennes, toutes industries confondues, surtout celles qui mettent au point des technologies de pointe ou qui entrent en concurrence directe avec des entreprises chinoises à l'échelle internationale.

En plus de s'adonner au vol de propriété intellectuelle, les opérations émanant de Chine continuent de cibler très activement le renseignement stratégique concurrentiel détenu par des entreprises canadiennes, en particulier celles qui font des investissements directs à l'étranger.

Je suis très préoccupé par la militarisation des cyberopérations. Alors que les membres de l'OTAN continuent de mettre en commun leur capacité de formation, les principales cyberpuissances à l'extérieur de l'alliance sont susceptibles de faire de même. Cette prolifération des cyberpuissances offensives à la fine pointe de la technologie, qui sont de plus en plus prêtes à passer à l'action sans trop subir de contrecoups, est susceptible d'engendrer bientôt une multiplication des cyberincidents perturbateurs et déstabilisants, qui aggraveront rapidement la méfiance au sein de la population.

Autrefois, certains pays auraient réagi aux sanctions occidentales en redoublant les attaques par déni de service sur des sites Web du secteur financier. À l'avenir, ils risquent plutôt de s'adonner simplement à des attaques destructrices, qui visent à paralyser de façon permanente les services financiers ou à modifier les données de manière à miner la confiance envers le système financier mondial. Par exemple, ils pourraient retarder ou entraver le règlement en toute confiance de la dette d'un gouvernement garantie par des créances.

Les pays suffisamment sanctionnés, qui se retrouvent donc de plus en plus à l'écart du système financier, sont peu portés à modifier leur comportement au cours d'une confrontation. Les efforts visant à nuire à des gouvernements étrangers pourraient être de plus en plus contrecarrés par des cybercampagnes perturbatrices, comme celles qui ciblent les infrastructures électorales et les candidats. Le Canada est particulièrement vulnérable aux campagnes de ce genre.

J'exhorte le gouvernement du Canada à collaborer avec ses alliés américains et européens afin de conclure des accords pacifiques et diplomatiques avec des adversaires éventuels dans le cyberespace. Contrairement à ce que bien des gens avaient prédit, l'attribution, bien que difficile, ne s'est pas avérée un obstacle à la mise en application d'accords diplomatiques de ce genre. En outre, de nombreux adversaires potentiels du Canada partagent des inquiétudes semblables au sujet des cybermenaces qui planent sur leur secteur financier et sur la stabilité de leur gouvernement, et ils souhaitent protéger leur population.

Il est possible de conclure des accords diplomatiques qui assurent la souveraineté des pays signataires et la stabilité de leurs opérations, tout en protégeant la dignité humaine. Ces accords peuvent être mis en application et ils seraient avantageux pour tous les signataires. Toutefois, ils pourraient exiger que l'Occident limite certaines de ses cyberactivités. Bien qu'ils soient insuffisants pour assurer totalement la protection des Canadiens, les accords diplomatiques qui restreignent certains types de cyberopérations et qui sont accompagnés de technologies et de services du secteur privé sont nécessaires pour protéger les entreprises et les citoyens canadiens à long terme.

Monsieur le président, je vous remercie de m'avoir donné l'occasion de participer aux discussions aujourd'hui. Je suis prêt à répondre à vos questions.

● (1540)

Le président: Merci, monsieur Porter.

Monsieur Reiber, vous disposez de 10 minutes.

M. Jonathan Reiber (chef, Stratégie de cybersécurité, Illumio): Messieurs le président et le vice-président, je vous remercie de m'avoir invité à témoigner devant votre comité aujourd'hui. C'est un honneur pour moi de représenter mon entreprise, Illumio, et de vous faire part de mes réflexions concernant l'avenir de la cybersécurité et de la planification des politiques relatives à la sécurité nationale.

J'occupe actuellement le poste de chef de la Stratégie de cybersécurité chez Illumio, une entreprise qui fournit des capacités de microsegmentation en matière de cyberrésilience. Je suis l'ancien chef de la cyberstratégie du Pentagone. Dans le cadre de ces fonctions, j'ai rédigé des discours pour le sous-secrétaire à la défense à l'époque de l'administration Obama.

Si vous le permettez, j'aimerais d'abord rendre hommage à un grand chef de file canadien du secteur de la sécurité nationale avec qui j'ai travaillé au sein de l'administration Obama et qui est décédé l'an dernier. Ensemble, nous avons travaillé dans le domaine de la cybersécurité. J'aimerais vous parler de lui brièvement et, ainsi, m'assurer que son nom est consigné au compte rendu canadien.

On a salué la vie de Shawn Brimley partout aux États-Unis, son pays d'adoption. Entre autres hommages, l'ancien président Barack Obama a rédigé une lettre à son sujet, et la presse nationale américaine a publié des éloges funèbres émouvants. Toutefois, pour sa famille et nos deux pays, j'aimerais que soit consignée au compte rendu permanent de la Chambre des communes la déclaration suivante.

Né à Mississauga, en Ontario, Shawn Brimley a servi dans l'Armée canadienne et a fréquenté l'Université Queen's. Plus tard, il s'est installé à Washington avec sa femme, Marjorie Clark Brimley. Au cours de sa carrière échelonnée sur 40 ans, il en fait plus que la plupart des gens pendant toute leur vie. Après avoir travaillé au Pentagone et à la Maison-Blanche, il a dirigé l'un des principaux groupes de réflexion de Washington, le Center for a New American Security. Il a rédigé le document intitulé « 2010 Quadrennial Defense Review », aidé à façonner le pivot entre les États-Unis et l'Asie, a dirigé à partir de la Maison-Blanche des initiatives d'intervention et de planification stratégique en cas de crise et a été l'un des principaux penseurs à l'origine de la troisième stratégie compensatoire en matière d'innovation à long terme de la défense américaine.

En tant que mari et père aimant, grand ami et mentor, Shawn Brimley a contribué à l'amélioration de la sécurité de tout un chacun. La Chambre des communes, le Canada et les États-Unis peuvent être fiers de ses réalisations.

Shawn Brimley a témoigné devant le Congrès américain en 2015, et c'est pour moi un honneur de comparaître aujourd'hui devant ce comité de la Chambre, surtout pour parler d'un dossier sur lequel Shawn et moi avions commencé à travailler il y a neuf ans.

Au fil des années qui ont suivi mon arrivée au Pentagone, les cybermenaces sont devenues un défi de premier plan pour la sécurité internationale. Cette situation est attribuable à trois tendances: la vulnérabilité des réseaux et des données du cyberespace; la vaste transformation numérique de la société; et des investissements insuffisants de la part des organisations dans les personnes, les processus et les technologies nécessaires pour prévenir les cyberattaques, se défendre contre celles-ci et se rétablir à la suite de celles-ci. Les gouvernements et les organisations ont pris des mesures pour améliorer leur dispositif de cybersécurité en créant des équipes, en élaborant des options et en mettant en place des technologies, mais, à cause de leur lenteur, les progrès ne peuvent pas suivre l'évolution de la menace.

Les attaquants étatiques et non étatiques volent, détruisent et manipulent des données dans le cyberespace et au moyen de celui-ci. Les adversaires se multiplient dans ce qu'on pourrait appeler l'« espace gris », qui se trouve sous le niveau d'un conflit direct, et ils ne semblent pas découragés dans la poursuite de leurs objectifs. Pour ne citer que quelques exemples, pensons à la campagne permanente que mène la Chine pour voler la propriété intellectuelle américaine, y compris les données de l'avion de combat interarmées; le vol de 81 millions de dollars aux dépens de la Banque centrale du Bangladesh et de la Réserve fédérale américaine commis par la Corée du Nord en 2015; le vol de 21,5 millions de dollars de dossiers de personnel commis par la Chine aux dépens de l'Office of Personnel Management des États-Unis; et les attaques commises en 2015-2016 par des agents russes pour perturber le réseau électrique ukrainien.

Les acteurs étatiques représentent la plus grande menace parce qu'ils disposent des ressources nécessaires pour payer des pirates informatiques. Ces gens peuvent fréquenter un gymnase; ils peuvent travailler avec diligence au fil du temps pour tenter d'atteindre une cible. Au cours des dernières années, ils sont passés du vol et de la destruction de données à la manipulation de données à des fins politiques et médiatiques.

Le piratage russe de l'élection présidentielle américaine de 2016 en est l'exemple parfait. Comme vous le savez, sous la direction expresse du président russe Vladimir Poutine, les services russes du renseignement militaire ont piraté les réseaux des organisations et des dirigeants politiques américains et ont exploité les vulnérabilités dans les pratiques commerciales des médias sociaux pour faire de la propagande et susciter la méfiance dans la population américaine.

L'opération russe a touché trois parties du « centre de gravité » américain pendant une période de transition politique cruciale: la population américaine, les dirigeants politiques et les principales entreprises technologiques. Depuis cet incident, d'autres États ont posé des gestes semblables. Par exemple, la Chine se serait insinuée dans le système électoral du Cambodge en 2018, lui permettant ainsi de manipuler le résultat de l'élection.

Pourquoi le problème est-il si grave en ce moment? Je dirais que c'est le cas pour trois raisons principales. Premièrement, l'urbanisation ne cesse de s'intensifier. Deuxièmement, on assiste à une prolifération des technologies à double usage. Troisièmement, l'économie mondiale est maintenant interconnectée. Cela signifie que de petits groupes peuvent avoir un impact considérablement disproportionné par rapport à leur taille. Anthony Giddens a qualifié ce phénomène de risque à conséquences graves de la modernité.

Parmi les exemples, citons les attentats terroristes perpétrés par Al-Qaïda le 11 septembre 2001, les actions des prêteurs à risque et leur impact sur le marché hypothécaire et, plus récemment, l'opération russe dans le cyberespace visant à perturber l'élection présidentielle américaine. Tout comme lors des attentats du 11 septembre 2001, lorsque 19 hommes ont échappé au dispositif de sécurité et ont transformé des avions en missiles, un petit groupe d'agents russes a exploité une faille dans le système de sécurité américain pour mener une attaque asymétrique à haut risque.

● (1545)

Internet, qui a été créé il y a plus de 35 ans, compte maintenant un peu moins de 4 milliards d'utilisateurs. L'accès au réseau s'est accru sans qu'on prenne pleinement conscience des risques. Qu'il s'agisse des vulnérabilités du code ou de l'impact des médias sociaux sur la formation de l'identité politique, les réseaux et les environnements infonuagiques sont vulnérables aux failles, et la société est exposée à la manipulation.

Les pays devraient s'employer en premier lieu à dissuader les cyberattaques étatiques. La dissuasion est une question de perception et elle fonctionne lorsqu'on réussit à convaincre un adversaire potentiel que les coûts d'une attaque seront supérieurs aux avantages qu'il en retirera. Pour que la dissuasion soit efficace, il faut être en mesure d'imposer des coûts à l'attaquant au moyen de sanctions ou de moyens militaires; des outils défensifs pour repousser une attaque imminente, comme des pare-feu; et, dans le cas où un pirate enfreint le périmètre, des capacités de résilience visant à limiter son impact, notamment la microsegmentation.

Deux propositions issues de l'histoire récente peuvent éclairer l'étude menée par votre comité. Premièrement, les adversaires se sont multipliés dans le cyberespace, et ce, malgré les efforts de dissuasion déployés par le gouvernement américain. Les États-Unis et d'autres pays doivent donc adopter une position plus énergique pour dissuader l'agression. En 2018, le gouvernement américain a adopté une telle position, notamment au moyen de la théorie du département de la Défense qui consiste à se défendre en amont dans le cyberespace.

Comme mon collègue l'a souligné, au fur et à mesure que les adversaires se sont multipliés, les États-Unis ont choisi de les inculper ou de les sanctionner. Ces mesures punitives, bien que raisonnables, ne semblent pas avoir créé de précédent ni prévenu efficacement l'escalade. Par exemple, même après avoir été sanctionnée pour son ingérence dans l'élection de 2016, la Russie aurait continué d'introduire des maliciels dans le réseau électrique américain jusqu'en 2018.

Qu'entend-on par « se défendre en amont dans le cyberespace »? En présence d'indices et d'avertissements concernant une cyberattaque imminente, les États-Unis doivent être en mesure de repousser l'adversaire. Ils doivent donc pénétrer dans la cyberinfrastructure pour mener une contre-offensive afin d'atténuer l'attaque imminente. Les États-nations ont le droit de se défendre dans le cyberespace, tout comme elles le font dans d'autres domaines. Toutefois, pour maintenir la paix et la stabilité, toute opération doit être menée en conformité avec le droit des conflits armés.

La nécessité de mettre en place un dispositif de dissuasion plus vigoureux est la première chose à retenir des 10 dernières années d'élaboration de politiques en matière de cybersécurité aux États-Unis. La deuxième, c'est la nécessité de supposer qu'il y a eu intrusion et de prévoir que les adversaires vont réussir à s'infiltrer dans les défenses internes et à avoir accès aux données les plus vulnérables.

Qu'entend-on par « supposer qu'il y a eu intrusion »? La plupart des organisations mettent l'accent sur les défenses périmétriques, mais elles ne disposent pas d'un système de sécurité interne, qui empêche les serveurs de communiquer entre eux une fois que l'attaquant a pénétré dans le réseau. Une fois qu'il a infiltré un réseau, un intrus peut passer en moyenne six mois à l'intérieur d'un centre de données ou d'un environnement infonuagique. Il peut alors se déplacer et inoculer des maliciels comme bon lui semble. Les applications les plus précieuses de l'organisation, comme ses principales bases de données, sont alors facilement accessibles.

Par exemple, lors de l'attaque chinoise contre l'Office of Personnel Management des États-Unis, il n'existait aucune règle régissant l'interaction interne des applications et des serveurs. Par conséquent, lorsque l'intrus chinois est entré dans le système, il a pu facilement avoir accès à la base de données contenant 21,5 millions de dossiers.

La microsegmentation empêche la propagation des intrusions. À son niveau le plus élémentaire, elle érige des murs autour des applications cruciales afin de les isoler du reste de l'environnement infonuagique et des centres de données. Un intrus pourrait s'introduire dans trois serveurs, mais pas dans 3 000. Il s'agit donc d'une base solide sur laquelle repose la cyberrésilience et de la dernière ligne de défense. Pour les infrastructures essentielles comme le secteur financier, un tel type de capacité permet de renforcer la résilience non seulement du secteur en question, mais aussi du pays dans son ensemble.

Il ne s'agit pas de savoir si une intrusion se produira, mais plutôt de déterminer à quel moment elle aura lieu. Les pays doivent se défendre de manière proactive contre les agresseurs pour que la dissuasion soit efficace. Ils doivent aussi supposer qu'il y a eu intrusion et mettre en place des stratégies de défense poussées pour résister aux cyberattaques. Le leadership assure le succès de tous les éléments du projet de cybersécurité.

Dans son essai précurseur, intitulé « The Challenge of Change », l'historien Arthur M. Schlesinger a déclaré: « La science et la technologie révolutionnent nos vies, mais la mémoire, la tradition et le mythe encadrent notre réponse. » C'est bien vrai. Notre capacité de gérer le changement technologique dépend en fin de compte du succès du chef de file et de sa capacité de tisser la trame susceptible de changer les choses. Au cours des 10 dernières années, des chefs de file solides en matière de sécurité ont fait leur apparition au Canada et aux 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 représente tout simplement le plus récent chapitre de notre histoire.

En fin de compte, le leadership repose sur l'analyse, et c'est ce qui rend le travail de ce comité aussi important.

Je vous remercie de m'avoir invité. Je suis prêt à répondre à vos questions.

● (1550)

Le président: Merci, monsieur Reiber.

Je vous remercie de votre déclaration au sujet de Shawn Brimley. Nous avons tous apprécié vos paroles aimables et réfléchies à son sujet.

Nous allons maintenant passer à Mme Damoff ou à M. Spengemann.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Monsieur le président, je vais commencer, puis je céderai la parole à mon collègue.

J'ai une très brève question pour vous, monsieur Porter. Vous avez dit que l'infrastructure électorale canadienne est particulièrement vulnérable. Comme vous le savez, le système électoral canadien est différent de celui en place aux États-Unis. Pourquoi le système canadien est-il particulièrement vulnérable?

M. Christopher Porter: Je tiens à préciser que ce n'est pas le Canada en tant que tel qui est particulièrement vulnérable. Je voulais dire qu'il s'agit d'une vulnérabilité particulièrement importante pour le Canada. Évidemment, l'utilisation de bulletins de vote au Canada élimine bien des inquiétudes que nous éprouvons aux États-Unis. Néanmoins, je pense que le système électoral canadien est une cible de choix pour un certain nombre d'agresseurs, qu'il s'agisse de militants politiques internes ou de pirates chinois, russes ou autres, qui pourraient chercher à influencer le processus.

À l'image du secteur financier, le processus électoral doit inspirer une grande confiance au sein de la population. Les sociétés libres et démocratiques dans lesquelles nous vivons nous procurent d'énormes avantages, et nous pouvons faire des affaires et transférer de l'argent dans le monde entier. En revanche, le moindre problème, voire la perception d'un problème — même s'il ne s'agit pas d'une intrusion en tant que telle —, peut causer des torts disproportionnés au processus électoral et au secteur financier.

Mme Pam Damoff: Permettez-moi de vous interrompre, car j'aimerais obtenir des éclaircissements là-dessus. Je vous remercie.

M. Christopher Porter: D'accord.

Mme Pam Damoff: Cette semaine, j'ai rencontré des représentants de l'Association canadienne des compagnies d'assurances mutuelles. Ils sont avec nous aujourd'hui. Nous avons discuté du système bancaire ouvert. Ils m'ont expliqué en quoi cela consiste, car je n'en avais aucune idée. Je sais que les États-Unis cherchent à adopter un système semblable. En avez-vous entendu parler?

Le concept consiste à faire en sorte que les entreprises de technologie financière, comme Wealthsimple au Canada, aient accès à des données bancaires. Au Canada, les banques sont assujetties à une réglementation très sévère. Les données circuleraient dans un portail comme Expedia.ca, et les entreprises pourraient y avoir accès pour s'adapter aux besoins de leurs clients.

À mon avis, un tel système est vulnérable à toutes les formes d'atteintes à la cybersécurité et à la vie privée. Apparemment, un tel système existe déjà en Europe, et les États-Unis s'apprêtent aussi à l'adopter.

● (1555)

M. Christopher Porter: Je ne connais pas assez bien ce système pour en parler. En général, les arrangements de ce genre, dans le cadre desquels un courtier en données agit en tant que fiducie d'intérêt public ou de fiducie pour l'ensemble de l'industrie, permettent d'améliorer la cybersécurité au quotidien, mais ils rendent aussi le système plus fragile. Une compromission peut prendre une ampleur démesurée.

Toutefois, je ne m'y connais pas assez pour parler de cette situation en particulier.

Mme Pam Damoff: Connaissez-vous un peu le système?

M. Jonathan Reiber: Non, pas du tout.

Mme Pam Damoff: D'accord.

Je cède maintenant la parole à M. Spengemann.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Merci beaucoup.

Merci à vous deux d'être ici aujourd'hui.

Je m'intéresse aux petites entreprises et à la cybersécurité, qui sert l'intérêt public national et mondial. Que peut-on faire pour faciliter la tâche aux entrepreneurs axés sur les données et qui, au départ, peuvent avoir de la difficulté à assumer les coûts liés à une cybersécurité efficace? Le gouvernement peut-il prendre des mesures pour corriger la situation? Les entreprises bien établies, qui disposent de vastes bases de données sur leur clientèle et d'importants moyens financiers, s'en tirent plus facilement. Ce n'est pas le cas pour les entreprises en démarrage.

Qu'en pensez-vous?

M. Jonathan Reiber: Bien sûr. Il existe différentes façons de stimuler l'investissement au pays. Au cours des dernières années, le cadre réglementaire a évolué considérablement et peut donc être utilisé à cette fin. La cybersécurité, c'est un peu comme l'assurance-vie. Il faut un déclic pour inciter les gens à agir. Dans le cas de l'assurance-vie, il s'agit habituellement de la naissance d'un enfant. Dans le cas des dépenses, toutefois, je pense que le déclic doit venir de l'extérieur.

Pour ce qui est du Règlement général sur la protection des données, des lois en vigueur au Colorado et en Californie, de la loi que vous avez adoptée... aussi, l'État de New York vient d'adopter une loi touchant le secteur des services financiers, qui insiste sur la nécessité de gérer les atteintes à la vie privée. Les entreprises doivent donc se conformer aux dispositions législatives. En outre, cette loi aura un effet sur le comportement des entreprises sur le marché et sur la façon dont elles dépensent leur argent.

Les services ne sont pas très dispendieux. Ce n'est vraiment pas une question de dépenses. Comme je l'ai dit tout à l'heure, c'est en fait une question de leadership.

En ce qui concerne les investissements dans la cybersécurité, j'aime parler des nouvelles mesures de sécurité par rapport aux anciennes. Par le passé, les mesures de sécurité comprenaient le cryptage, les systèmes de détection des intrusions et les pare-feu. Maintenant, on dispose d'une nouvelle capacité, soit la microsegmentation, qui assure une très grande résilience aux centres de données.

Je recommande aux organisations qui souhaitent investir dans la cybersécurité de songer à adopter ces nouvelles mesures de sécurité, qui permettent de protéger le périmètre et l'intérieur de leur système.

Au cours des dernières années, les dépenses liées aux services ont diminué au fil de l'évolution du marché. Toutefois, je souligne aussi que la réglementation est une bonne étape...

M. Sven Spengemann: ... à un point tel que, dans la plupart des cas, de telles dépenses ne nuiraient même pas à l'accès au marché.

M. Jonathan Reiber: Souvent, le budget affecté à la technologie de l'information équivaut à 10 % des dépenses totales. Dans le cas du Pentagone, environ 10 % de son budget total, qui se chiffre à 40 milliards de dollars, devrait être investi dans la cybersécurité, ce qui équivaut, grosso modo, au montant que les États-Unis dépensent pour leur cybercommandement.

M. Sven Spengemann: D'accord. C'est très utile.

Monsieur Porter, avez-vous des commentaires à ce sujet?

M. Christopher Porter: Oui. Je vous remercie de la question.

Le ciblage des petites entreprises est un enjeu qui me tient beaucoup à coeur sur le plan des politiques. Tout d'abord, même si cette question ne relève pas directement de mon champ de compétences, je pense que l'infonuagique a rendu possible l'accès à d'excellents fournisseurs de services de sécurité, selon une échelle graduelle de prix. Ainsi, les entreprises assument des coûts par bande passante ou par licence, au lieu de devoir payer d'énormes coûts fixes en capital. Comparativement à ce qui se passait il y a à peine quelques années, ces solutions sont beaucoup plus abordables. Cependant, pour mettre en échec un acteur de calibre mondial, il faut plus que de simples moyens technologiques. Il faut disposer d'une infrastructure organisationnelle, qui assure la formation et le maintien en poste des employés, ainsi que de services de recherche des menaces. Or, les petites entreprises ne peuvent y arriver seules.

FireEye offre des services de gestion des mécanismes de défense, qui consistent notamment à gérer les réseaux à la place des entreprises. Il s'agit d'une solution efficace à 95 %. À mon avis, la Chambre pourrait se pencher sur l'échec de la politique... Aux États-Unis, l'échec de la politique, c'est qu'on cherche à défendre les plus grandes sociétés, car, en cas d'atteinte à la sécurité, ce sont elles qui présentent les menaces les plus évidentes pour la sécurité nationale.

M. Sven Spengemann: D'accord.

M. Christopher Porter: Dans l'Ouest, nous ne sommes pas aussi expérimentés dans la mise à mort à petit feu. Ainsi, des acteurs qui détruisent 1 000 petites entreprises n'attireront pas l'attention du président ou du premier ministre. Cependant, un compromis de taille le fera. J'estime que cette situation découle d'une lacune dans les politiques à laquelle il faut remédier. Au Canada, je recommande que les autorités affirment, à tout le moins — même si c'est très difficile — que le gouvernement accorde la priorité à la défense de tous, et pas uniquement à la défense des grandes entreprises et des industries qui fonctionnent en vase clos. La tâche peut sembler herculéenne, mais il serait souhaitable qu'on la considère comme une priorité officielle à laquelle il faut commencer à s'attaquer.

● (1600)

M. Sven Spengemann: Vos observations sont très pertinentes. Merci.

Merci, monsieur le président.

[*Français*]

Le président: Monsieur Paul-Hus, vous avez la parole pour sept minutes.

M. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, PCC): Merci, monsieur le président.

Messieurs les témoins, je vous remercie d'être parmi nous aujourd'hui.

J'ai eu l'occasion de rencontrer M. Reiber dans la Silicon Valley en octobre dernier. C'est là que j'ai eu l'idée d'inviter aussi quelqu'un de FireEye à venir nous rencontrer.

Ma première question concerne la position du Canada sur le plan de la cybersécurité à l'échelle mondiale par rapport à celle des États-Unis.

Il est évident que les États-Unis, en tant que superpuissance, sont une cible de premier choix. Avec la Chine et la Russie, vous êtes en quelque sorte une cible naturelle. Au Canada, nous sommes toujours considérés comme de bons garçons et de bonnes filles, autrement dit des gentils. Si on compare les deux pays du point de vue militaire, les États-Unis ont une grande armée, alors que le Canada en a une qui est plutôt petite. Par contre, nous nous sommes toujours dit qu'en cas de problème, nous travaillerions ensemble pour nous défendre.

Dans le contexte de la cybersécurité, considérant toute l'infrastructure actuelle de défense américaine, des organisations privées ou même des organismes publics — la CIA, le Department of Homeland Security et les autres —, pensez-vous que, dans le cas d'une attaque, la collaboration entre nos deux pays serait possible et que vous pourriez nous aider?

[*Traduction*]

M. Jonathan Reiber: Pour une raison que j'ignore, l'interprétation n'a pas fonctionné et je dois me fier à mes connaissances en français qui se limitent à ce que j'ai appris à l'école secondaire. Je vais tenter de répondre.

Si j'ai bien compris, compte tenu de l'évolution des rapports entre la CIA, le département de la Sécurité intérieure et le secteur militaire vous avez demandé quel est le niveau de collaboration entre ces entités au titre de la défense commune et si elles pourraient aider la Canada? Es-ce bien un élément de la question?

M. Pierre Paul-Hus: Si le Canada est la cible de cyberattaques, les États-Unis pourraient-ils aider le Canada rapidement?

M. Jonathan Reiber: Bien sûr. C'est ce que j'ai pensé. Oui.

M. Pierre Paul-Hus: À votre connaissance, les lois canadiennes constituent-elles un obstacle?

M. Jonathan Reiber: Une résolution prise aux termes de l'article 5 prévoit qu'en cas de cyberattaque d'un certain niveau, toutes les parties au Traité de l'Atlantique Nord peuvent prendre des mesures pour assurer leur défense commune.

Au sujet des cyberattaques, il est intéressant de noter que, à ce jour, elles n'ont jamais dépassé le seuil qui déclenche immédiatement l'annonce sans équivoque d'une intervention militaire. D'un point de vue historique, l'ingérence russe dans les élections présidentielles de 2016 constitue certainement un cas qui aurait justifié une contre-offensive militaire. Je crois que d'autres membres de l'administration Obama ont émis la même opinion. La difficulté dans ce cas en particulier tient au fait que le calcul décisionnel est complexe. Je n'entrerai pas dans cette voie, parce que la question ne portait pas vraiment là-dessus.

M. Pierre Paul-Hus: Merci. Je dispose de seulement sept minutes.

En ce qui concerne les liens entre les secteurs public et privé, je note que vous avez travaillé pour la CIA et le Pentagone et que vous évoluez maintenant dans le secteur privé. Ici au Canada, nous cherchons à trouver comment collaborer avec le secteur privé parce que, comme on le sait, il est plus difficile d'affecter des fonctionnaires à ce genre d'activités.

M. Jonathan Reiber: Certainement.

M. Pierre Paul-Hus: Estimez-vous que le Canada devrait changer sa façon de faire pour adopter le modèle actuellement en place aux États-Unis?

M. Jonathan Reiber: Je pense que cette transition est déjà faite. En réalité, depuis 2014, on observe une tendance importante pour créer une synergie entre le secteur privé et le gouvernement. Il s'agit d'un effort extrêmement pertinent. Nous avons amorcé le processus en lançant des programmes collaboratifs dans le domaine de l'innovation pour la défense — le U.S. Digital Service et le Defense Digital Service — qui ont fait appel à la participation de spécialistes de l'extérieur. Ces initiatives se sont révélées extrêmement utiles.

Il va sans dire que je recommande à tous les pays confrontés à des enjeux de cybersécurité de bâtir des liens étroits entre les secteurs public et privé pour permettre à des entrepreneurs du secteur technologique de collaborer avec le gouvernement et à des représentants du gouvernement national de travailler dans le domaine de la haute technologie.

● (1605)

M. Christopher Porter: C'est intéressant dans le contexte du cybertravail parce que 95 % des attaques ciblent des gens sur les réseaux du secteur privé. Souvent, aux États-Unis et ailleurs, c'est le secteur privé qui est le premier à prendre connaissance du problème. Les gouvernements peuvent faire des interventions plus musclées et des enquêtes plus approfondies. Le secteur privé ne peut remplacer le gouvernement, c'est-à-dire le secteur public, à cet égard. Ces deux secteurs font un travail complémentaire.

Par exemple, il est important de savoir que chez FireEye, certaines des équipes clés qui repèrent des logiciels criminels sont établies à l'extérieur du Canada. FireEye est une fière entreprise créée aux États-Unis, mais elle se considère comme une compagnie internationale pour ce qui est de ses effectifs. Cette structure permet des échanges d'information transfrontaliers rapides, ce que les gouvernements ont parfois du mal à faire.

En réponse à votre question, je pense effectivement que comme le Canada et les États-Unis sont de très proches alliés, en principe, ils s'entraideraient si les circonstances le permettaient. Je m'en remets à mon collègue pour préciser ces circonstances, mais au niveau opérationnel, il est certain qu'au quotidien, les chercheurs canadiens et américains collaborent et échangent de l'information sur les menaces. Je pense que c'est la réalité de tous les jours, pas uniquement en situation de crise.

M. Jonathan Reiber: Oui. De toute évidence, les services du renseignement de sécurité et les services de sécurité travaillent en très étroite collaboration en ce qui concerne les interventions en cas d'urgence. À la commission trilatérale qui réunit les États-Unis, le Mexique et le Canada, on trouve ce genre de collaboration. On la retrouve forcément aussi entre nos deux pays.

M. Pierre Paul-Hus: D'accord. Merci.

Je voulais connaître votre point de vue au sujet de la compagnie chinoise Huawei. Au Canada, les opinions sont partagées à l'égard de cette entreprise: certains affirment qu'il n'y a aucun problème alors que d'autres sont convaincus du contraire. Les États-Unis, l'Australie et la Nouvelle-Zélande ont décidé d'interdire la présence de Huawei sur le territoire. Quelle est votre opinion?

M. Christopher Porter: La société FireEye ne suit pas cette question. Elle s'intéresse aux menaces informatiques non aux risques liés au matériel comme ceux qu'on allègue dans ce dossier.

Je comprends très bien l'origine de ces craintes, particulièrement en ce qui concerne les réseaux gouvernementaux. Les pays ont tout lieu de vouloir que l'ensemble de leur équipement de télécommunications soit fabriqué sur leur territoire ou chez un proche allié. En principe, c'est logique. Cependant, en ce qui concerne le dossier Huawei, je ne sais rien qui n'ait déjà été révélé au public, notamment dans les journaux.

M. Jonathan Reiber: Je ne ferai pas de commentaires sur Huawei en particulier. Je dirai néanmoins que nous sommes confrontés à des risques au niveau de la chaîne d'approvisionnement depuis... Mon Dieu, je ne saurais dire exactement à quand remontent ces problèmes, mais ils sont certainement très présents depuis la création de la plateforme cryptoanalytique dans le domaine du renseignement électromagnétique.

Si, pour se sentir mieux protégé, on décide de réagir à chaque puce dans le cyberespace, cela entraînera une diminution du taux marginal de production. Pour certains éléments, j'estime parfaitement raisonnable que les organismes de sécurité nationale ou de sécurité publique disent qu'ils vont dorénavant fabriquer un certain nombre de puces eux-mêmes. Cependant, comme les coûts sont assez élevés, une telle décision aurait une incidence sur les choix financiers. Je ne pense pas qu'il soit possible d'appliquer cette formule à l'ensemble des secteurs économiques. Néanmoins, il serait probablement possible de l'appliquer dans un certain nombre de sous-secteurs.

Le président: Merci, monsieur Paul-Hus.

Monsieur Dubé, vous disposez de sept minutes, s'il vous plaît.

M. Matthew Dubé (Beloeil—Chambly, NPD): Merci monsieur le président.

Messieurs, je vous remercie d'être parmi nous. Veuillez également pardonner mon retard et le fait que j'ai manqué vos présentations. C'est un problème lorsqu'on est le seul de son parti à un comité; on ne peut être à deux endroits en même temps. J'étais en haut avec des représentants de certains médias.

Je ne vais pas poser de questions sur le rôle du secteur privé. Cet aspect est revenu sur le tapis à maintes reprises. J'estime néanmoins que les rôles respectifs des secteurs public et privé sont en partie à l'origine des tensions sous-jacentes dans ce domaine.

Je me demandais simplement si vous aviez des réserves à l'égard du fait que de nombreux éléments sont offerts à titre de services. En principe, face à une entreprise concurrente, on cherche toujours à protéger ce qu'on fait le mieux et à conserver la clientèle établie. Craint-on que les règles commerciales habituelles et l'industrie nuisent à la capacité d'établir des pratiques normalisées et d'uniformiser les règles du jeu en ce qui concerne nos intérêts ici au Canada ou aux États-Unis, par exemple?

M. Christopher Porter: Vous constaterez probablement, du moins dans le milieu de la sécurité de l'information, qu'une vaste majorité des grandes entreprises collaborent pour l'établissement de normes et l'échange d'information, même les entreprises concurrentes, notamment pour la collecte de renseignements sur les menaces. On collabore souvent en coulisse en échangeant de l'information pour le bien public.

L'établissement de normes est généralement bénéfique pour les entreprises existantes. Je ne partage pas votre préoccupation. Néanmoins, je comprends ce qui la motive en théorie ou en principe, mais je n'ai pas vu de tel cas dans le secteur privé. J'ai de bons amis et collègues dans de nombreuses entreprises qui se livrent concurrence pour l'obtention de contrats mais, dans l'ensemble, la concurrence ne nuit pas à l'établissement de normes.

Je songe par exemple aux entreprises qui ont signé le Cibersecurity Tech Accord sous la direction de Microsoft. Les analystes des politiques publiques examinent le genre de normes applicables au milieu de la haute technologie et les moyens de collaborer pour le bien public. Les entreprises se livrent quand même concurrence pour obtenir des contrats et elles gardent leurs secrets commerciaux — vous avez raison —, mais elles se demandent également comment collaborer pour assurer la prestation des services.

J'aime toujours donner l'exemple des banques qui, au moins dans l'Ouest d'antan, étaient relativement peu à l'abri des menaces physiques. Au fur et à mesure que les gouvernements ont joué un rôle grandissant, que les marchés de la sécurité physique ont évolué et que davantage de normes et de réglementation ont été mises en place, les entreprises qui s'occupent de sécurité physique se sont enrichies. Ce genre de réglementation n'a pas nui à la capacité de ces entreprises de fournir des services ou de réussir sur le plan commercial.

● (1610)

M. Jonathan Reiber: Je partage les propos de mon collègue: le milieu des normes a fait de l'excellent travail et s'est démarqué. La norme de cybersécurité du National Institute of Standards and Technology ou norme NIST, retenue après l'adoption d'une loi sur la cybersécurité en 2011 et 2012, est un résultat très positif des efforts initiaux pour élaborer une norme ou un ensemble de normes. Je vous renvoie à la norme NIST.

Par ailleurs, pour éviter qu'on se concentre sur une technologie ou sur une partie du problème plus que sur une autre, les organisations d'échange et d'analyse d'information qui ont vu le jour dans les différents centres ont facilité l'élaboration d'exigences de cybersécurité propres à chaque secteur en particulier. Aux États-Unis, le secteur des services financiers est à cet égard le plus avancé du groupe. Le Financial Services Information Sharing and Analysis Center, ou FSISAC, constitue une bonne ressource pour comprendre comment le secteur répond à ses propres besoins en matière de cybersécurité.

M. Matthew Dubé: Je vous remercie de vos commentaires.

Je me demande si, lorsqu'on envisage l'avenir, et pour m'exprimer en termes simples .... Je pense qu'il est beaucoup question du coût d'utilisation des services. Ce que votre entreprise offre pour protéger les données que recueillent certaines compagnies, notamment sur les clients... Je pense que ces cas ont fait l'objet d'une abondante couverture médiatique.

J'aimerais savoir comment vous envisagez la situation, dans l'avenir, lorsqu'une partie des risques ne viendra plus de l'accumulation de données par une entreprise donnée dans le cadre d'un programme de récompenses, mais plutôt de ce qu'elle vend. Autrement dit, si une entreprise vend des appareils domestiques, compte tenu entre autres de la prolifération de dispositifs intelligents... Craint-on que les entreprises investissent énormément et dépensent beaucoup, notamment pour des mises à jour nécessaires, afin de protéger leurs propres intérêts, sans nécessairement protéger ceux de l'utilisateur qui achète l'équipement ou les dispositifs?

M. Christopher Porter: Ce qui me préoccupe le plus au sujet de l'Internet des objets, ce qui est ce dont vous parlez, je crois — l'ensemble des appareils physiques connectés à Internet —, c'est que bon nombre de ces appareils ne peuvent pas du tout être mis à jour. Même si une faille est découverte, il est techniquement impossible de la corriger. Pour les fabricants, le fait qu'ils n'aient pas à assumer la pleine responsabilité d'une faille ou d'une défectuosité de leurs produits ne les incite pas à faire autrement.

C'est un vecteur de menace qui me préoccupe. Pour ce qui est des incitatifs du marché à proprement parler, j'ai fait une majeure en administration des affaires, alors je devrais avoir une meilleure réponse, mais ce n'est pas sur quoi je me concentre au quotidien. Je réfléchis aux menaces. Les groupes qui constituent une menace vont se concentrer sur la façon dont ils peuvent causer des perturbations physiques qui minent des collectivités et des sociétés entières. Je suis beaucoup moins préoccupé par les logiciels malveillants de tous les jours qui pourraient s'attaquer à ces appareils que par ceux qui permettraient à des gouvernements étrangers de désactiver des appareils physiques dans les maisons des citoyens. Je dirais que la sécurité publique est d'abord et avant tout une responsabilité gouvernementale.

M. Matthew Dubé: Plus tôt, nous avons parlé des normes. Êtes-vous en faveur de certaines normes, un peu comme celles qui existent en matière de sécurité automobile? Devrait-il en exister pour les vendeurs de téléphones, entre autres, compte tenu de la nouvelle réalité dans laquelle nous vivons?

● (1615)

M. Christopher Porter: Oui, absolument.

M. Jonathan Reiber: En matière de cybersécurité, il est utile d'axer d'abord son attention sur le centre de données et l'environnement nuagique. On a tendance à penser directement au résultat final, comme le vol de propriété intellectuelle et la destruction ou la manipulation de données, des sujets qui pourraient inspirer un film de science-fiction et nous tenir éveillés toute la nuit.

Cependant, en s'intéressant d'abord au centre de données en tant que tel et aux moyens de sécuriser l'interaction interne des serveurs et d'empêcher les intrus de se déplacer latéralement dans les environnements, on prévoit toutes les éventualités. Oui, c'est ce que fait mon entreprise, mais si j'ai joint Illumio, c'est parce que je savais — ayant travaillé au Pentagone et examiné l'éventail des perturbations pouvant survenir sur une plateforme d'armement, dans le secteur financier ou dans l'économie — qu'il fallait vraiment commencer par s'imaginer le pire. Si un intrus pénètre illégalement dans un centre de données et qu'il peut se déplacer sans encombre, alors tout lui est possible. Par conséquent, je suis d'accord qu'il y ait des normes. En fait, le gouvernement français s'est montré très avant-gardiste à cet égard en ce qui concerne les centres de données de sécurité, tout comme d'autres pays. En commençant par là, tout le reste — même une intrusion dans un objet connecté à Internet chez quelqu'un — pourrait être évité, car au bout du compte tout se connecte à un serveur.

M. Matthew Dubé: D'accord, je comprends.

Le président: Merci monsieur Dubé.

[*Français*]

Monsieur Picard, vous avez la parole pour sept minutes.

[*Traduction*]

M. Michel Picard (Montarville, Lib.): Je vous remercie, messieurs.

Lorsqu'un attentat terroriste se produit, nous savons habituellement qui en est l'auteur et ce qui a motivé ce pays à attaquer le nôtre. Par exemple, peut-être que c'est parce que nous nous opposons à ses politiques. Si j'avais ma propre entreprise privée dans le secteur des services financiers, je demanderais: quelle menace mon entreprise représente-t-elle pour des intérêts étrangers? Qu'est-ce qui pourrait les pousser à la cibler dans le cadre d'une cyberattaque? Dans mon exemple, mon entreprise aurait des succursales dans tous les pays, mais n'aurait aucune incidence sur la richesse de quiconque d'un point de vue gouvernemental. Si elle était victime d'une cyberattaque, j'ignorerais qui en est l'auteur. Je ne comprendrais pas pourquoi on l'aurait pris pour cible. Est-ce parce que la cybercriminalité est un sport national dans ce pays ou parce que ce dernier joue au voleur de banque et ne fait que voler mon argent virtuellement? Je ne suis pas certain que les sociétés privées saisissent pleinement ce qu'elles représentent et qu'elles comprennent assez bien le phénomène des cyberattaques pour pouvoir se protéger.

M. Christopher Porter: Je partage vos préoccupations et je suis d'accord avec vous. Souvent, j'ai l'impression que même des entreprises du secteur financier disposant de services de sécurité internes assez sophistiqués se font surprendre par certaines menaces. En général, elles savent qu'elles seront ciblées, mais comme vous l'avez souligné, les raisons pour lesquelles elles sont victimes d'une intrusion n'ont souvent rien à voir avec elles. Peut-être qu'un pays étranger se venge du gouvernement canadien pour des mesures que ce dernier a prises. De nos jours, c'est souvent pour des raisons de compétitivité économique. Ces institutions financières canadiennes ne nuisent peut-être à personne, mais il se peut qu'une autre banque d'un autre pays ou un autre investisseur veuille leur faire concurrence. Si ces autres entités ne peuvent pas le faire équitablement sur le marché libre, il est possible qu'elles obtiennent l'aide d'un groupe de pirates informatiques, par exemple.

En effet, malheureusement, les institutions financières du Canada sont souvent ciblées pour des raisons qui ne leur sont pas directement liées, sauf dans le cas de cybercrimes, car bien sûr c'est là que se trouve l'argent. Mais lorsqu'il s'agit d'une attaque conduite par un État-nation, c'est souvent pour des raisons de compétitivité économique. L'État-nation concerné souhaite soit voler des renseignements aux institutions financières, soit les concurrencer lorsqu'il investit à l'étranger. Il pourrait aussi s'agir de représailles politiques, même pour quelque chose qui se produit dans un autre pays.

C'est le revers de faire partie d'une alliance solide: si un pirate informatique découvre une vulnérabilité dans le réseau d'une institution financière canadienne, il pourrait s'en servir pour diffuser un message politique contre un autre membre de l'OTAN, par exemple. L'attaque pourrait n'avoir aucun lien avec l'institution financière comme telle. Voilà pourquoi il est si important que les services de sécurité du Canada entretiennent des liens étroits qui leur permettront d'avoir une meilleure compréhension du secteur privé et des motivations des attaques.

M. Jonathan Reiber: C'est utile de penser comme le ferait un adversaire, non? Que vous soyez un gouvernement ou une organisation qui se préoccupe des menaces en général, vous devez vous poser certaines questions. Qu'est-ce qu'un adversaire? Que pourrait-il faire pour me mettre en danger? Que peut-il essayer de me faire? Que suis-je prêt à perdre? Une fois que vous avez une idée de ce que sont vos intérêts fondamentaux, de ce que vous êtes prêt à perdre et de ce que vous devez protéger, vous pouvez alors commencer à élaborer une stratégie d'investissement. Cependant, cela ne permet pas de régler tout ce que vous venez de mentionner.

Aux États-Unis, un décret présidentiel sur la cybersécurité a été adopté. Conformément à l'article 9 de ce dernier, une liste d'entreprises a été établie. Le département de la Sécurité intérieure des États-Unis a évalué l'ensemble des entreprises et des organisations du pays afin d'établir lesquelles étaient les plus vulnérables à une attaque informatique, et où une perturbation entraînerait les plus graves conséquences. Cette analyse a mené à ladite liste qui est classifiée. Cette dernière ne contient pas un très grand nombre d'entreprises. Vous pourriez probablement deviner d'emblée un certain nombre d'entre elles. Cette mesure a également permis au gouvernement de se concentrer sur sa collaboration avec ces entreprises clés. De cette façon, on peut dire que nous allons nous assurer le renforcement des cyberdéfenses de ces entreprises.

Cela ne veut pas dire que le gouvernement concentrera ses efforts uniquement sur ces entreprises. L'armée, par exemple, doit étudier les adversaires du pays: la Russie, l'Iran et la Corée du Nord en particulier. Elle doit se poser les questions suivantes: où ces pays investissent-ils? Quels sont leurs intérêts? Que vont-ils essayer de faire? En cas d'attaque assez importante, il faut essayer d'atténuer les conséquences et de repousser les attaquants.

Cela ne règle toutefois pas tout non plus; c'est là que la réglementation entre en jeu. Même si vous vous êtes assurés de renforcer la sécurité des entreprises les plus importantes du pays, même si l'armée surveille les adversaires les plus dangereux, il n'en demeure pas moins qu'on parle d'Internet. C'est immensément vaste. Quelqu'un va toujours essayer de trouver une autre porte d'entrée; il va toujours chercher le point le plus faible, une faille, pour mener une attaque.

Un bon exemple est le cas de l'Iran en 2012. Les États-Unis s'étaient préparés à tout pendant les négociations nucléaires. Comme de raison, l'Iran s'est attaqué à l'infrastructure de l'entreprise Saudi Aramco, située dans le golfe Persique. L'Iran a piraté l'entreprise, comme cela a été rapporté publiquement. C'est dans ce genre de situation où il est essentiel d'avoir une réglementation qui prévoit des exigences en matière de gestion des intrusions. Les entreprises doivent être pénalisées si elles ne respectent pas ces exigences de gestion des brèches. De plus, elles doivent être en mesure de faire certains investissements dans la résilience pour se défendre contre les intrusions.

● (1620)

M. Michel Picard: Quelles sont nos chances de lutter sur un pied d'égalité contre nos ennemis, étant donné que certains d'entre eux agissent dans le cadre d'initiatives financées par des États et disposent d'un budget illimité? Ce qui m'inquiète, au Canada, c'est que le budget est un problème.

M. Jonathan Reiber: En cybersécurité, la bonne nouvelle, c'est que nous pouvons contrôler notre propre terrain. Nous pouvons nous mettre dans la peau d'un adversaire et réfléchir à ce que ce dernier pourrait faire, aux attaques offensives qu'il pourrait lancer à partir de son terrain à lui. Ce n'est pas au secteur privé de s'occuper de cette question; c'est aux gouvernements de le faire. En tant qu'organisation, que vous soyez une organisation gouvernementale ou autre, vous pouvez organiser et configurer votre terrain de manière à renforcer considérablement vos défenses contre une attaque. Par cela, j'entends des dispositifs de cybersécurité à l'intérieur du périmètre de sécurité; des pare-feu; le chiffrement des courriels; l'authentification à facteurs multiples pour les utilisateurs; et des investissements afin d'accroître la microsegmentation. De cette façon, si un intrus franchit vos défenses périmétriques, il sera stoppé dès qu'il entrera dans votre centre de données ou votre nuage.

Si vous avez fait tout cela et que vous avez pris une cyberassurance, vous aurez pris des mesures très rigoureuses. On pourrait penser qu'une banque ou une grande institution aurait fait de même. Lorsque je m'adresse à une communauté de cybersécurité et que je demande à ceux qui utilisent l'authentification multifactorielle de lever la main, c'est presque toujours moins de 20 %. Quand je demande combien d'entre eux chiffrent leurs courriels, là non plus, les mains levées ne sont pas très nombreuses. C'est cette réalité qui fait que nous avons besoin de mesures d'incitation et de réglementation.

Je pense que ces mesures contribueraient grandement à nous protéger contre ceux qui essaieraient de nous attaquer. Elles permettraient de bloquer 95 % des intrusions et d'éviter les dommages connexes. Un partenariat avec le gouvernement est nécessaire afin d'imposer des sanctions ou des mesures punitives dans les cas où l'organisation pourrait ne pas être en mesure de le faire.

M. Michel Picard: Merci.

Le président: Merci, monsieur Picard.

Passons maintenant à M. Motz, qui dispose de cinq minutes.

M. Glen Motz: Monsieur Porter, si nous sommes l'un des premiers pays ciblés par des cyberattaques, ne faudrait-il pas que nous disposions d'une cyberdéfense de pointe? Malgré sa population moins nombreuse et les contraintes budgétaires, comment le Canada peut-il devenir plus avant-gardiste, que ce soit par rapport à ses homologues ou afin de mieux se défendre? Comment pouvons-nous y arriver? Pouvez-vous énumérer quelques pratiques exemplaires ayant cours dans le monde et que nous pourrions envisager d'adopter?

M. Christopher Porter: Bien sûr. Je vous remercie d'avoir posé la question, monsieur le président.

La bonne nouvelle, qui est aussi la mauvaise, c'est que, dans la mesure où les cyberpolitiques en sont encore à leurs balbutiements et que nos alliés cherchent encore le dispositif qui se révélera vraiment efficace, le Canada est bien positionné pour se démarquer en trouvant une solution qui fonctionne. Je crois que c'est tout à fait possible.

J'aimerais réorienter un tant soit peu la question. En général, au sein de l'OTAN, quand les gouvernements apprennent des choses de nature secrète, ils ont tendance à protéger d'abord et avant tout leurs propres réseaux, et peut-être aussi les entreprises et les particuliers. Quelques fois, il leur arrive de déclassifier l'information reçue et de la communiquer aux entreprises. Or, il s'agit d'un processus à long terme qui prend généralement beaucoup de temps. Au privé, si on ne produit pas de données utilisables dans les 48 heures, c'est que nous n'avons pas fait notre travail. Pour les gouvernements, les délais se comptent plutôt en mois. Cela dit, dans certains cas, c'est justifié, je ne dis pas le contraire. Il y a souvent de bonnes raisons d'agir ainsi.

Je vous rappelle qu'à une certaine époque, tout ce que je vous ai dit à propos de la mise en commun du cyberrenseignement valait aussi pour le contreterrorisme, par exemple. Du moins jusqu'au 11 septembre et jusqu'à ce que l'aviation ne devienne une cible. La pression était alors beaucoup plus grande pour que l'information se rende jusqu'aux autorités locales, aux parties intéressées et aux entreprises américaines. Les données étaient plus facilement déclassifiées et partagées.

Selon moi, c'est ainsi que devrait aussi fonctionner le cyberrenseignement. Les alliés devraient se montrer plus tolérants aux risques et transmettre plus rapidement au secteur privé les renseignements nécessaires à la mise en place d'une bonne défense. C'est irréaliste de penser que les petites entreprises — et même les grandes — puissent suivre efficacement l'évolution des menaces. Si l'information circulait plus librement entre les grandes entreprises privées de cybersécurité et les gouvernements, les choses iraient bien mieux. À condition de tolérer un certain niveau de risque, évidemment.

Pour le moment, les gouvernements ont tendance à se considérer comme la banque de données principale, à tout garder pour eux et à dire aux autres ce qu'ils doivent faire. Or, ce n'est pas ainsi que les choses fonctionnent, dans le cyberespace. Les gouvernements ont évidemment le premier rôle, mais ils ne sont pas les seuls en scène.

● (1625)

M. Glen Motz: Très bien, je vous remercie. Je n'ai pas beaucoup de temps.

Monsieur Reiber, selon ce que vous savez du droit canadien, manque-t-il quoi que ce soit, du point de vue législatif, qui permettrait d'améliorer la protection des consommateurs et de leurs renseignements personnels et de mieux protéger nos infrastructures essentielles?

M. Jonathan Reiber: Je vais devoir m'abstenir de répondre, monsieur, parce que je suis loin d'être un expert — même si j'aurais aimé l'être.

J'ai lu la nouvelle cyberstratégie du Canada pour 2018, et je crois qu'il s'agit d'un point de départ intéressant pour le pays en général, mais je ne connais pas très bien le droit canadien.

M. Glen Motz: D'accord.

Et vous, monsieur Porter? Avez-vous quelque chose à ajouter?

M. Christopher Porter: Non.

M. Glen Motz: Monsieur Reiber, vous avez abordé le concept de la microsegmentation. N'est-ce pas un peu cher pour les petites entreprises?

M. Jonathan Reiber: Non, pas du tout.

M. Glen Motz: De quoi s'agit-il précisément? Faut-il des serveurs différents ou faut-il au contraire reconfigurer ceux qu'on a?

M. Jonathan Reiber: Tout dépend du résultat attendu. Pour les prix exacts, il faudrait demander à mes collaborateurs.

Chaque cas est analysé séparément. Je recommande aux organisations de commencer... Nous avons constaté que la plupart des organisations savent instinctivement quelles sont leurs applications vedettes, celles qui ont le plus de valeur dans leur milieu. Pour reprendre un des exemples que j'ai donnés tout à l'heure, pour le service des ressources humaines d'une entreprise, il s'agirait de la base de données où sont stockés tous les renseignements des employés.

À partir du moment où vous avez identifié les applications les plus importantes pour vous, vous devez tracer un plan où figurent votre centre de données, l'ensemble de vos applications et de vos activités qui ne sont pas des applications, mais qui, dans le centre de données, servent de liant entre les applications et les serveurs. Il faut avoir une image claire, un plan de tout ça, mais peu d'organisations le font. En géostratégie, il faut absolument avoir un bon plan du terrain pour en garder le contrôle. Eh bien c'est la même chose, parce que le plan sert à illustrer les interactions entre les différentes applications.

Si Chris travaille au service du marketing et que moi, je suis responsable des serveurs, quelle que soit l'organisation dont nous faisons partie, il n'y a aucune raison pour que son serveur interagisse avec le mien si jamais il se faisait pirater par courriel. Cela ne le regarde pas. Ce n'est pas lui, l'ingénieur, c'est moi. Bref, on doit coucher sur papier la manière dont fonctionnent nos applications et définir les règles qui encadrent les interactions entre elles.

Le degré de rigidité des règles dont une entreprise souhaite se doter pour protéger ses applications vedettes dans l'ensemble de son organisation aura une influence sur le prix, et c'est pour cette raison que je ne veux pas donner de chiffre précis. À partir du moment où une entreprise se dote d'un tel plan et se fixe des règles à l'interne, c'est là qu'elle commence à vraiment protéger ses acquis. Le principal avantage des règles, c'est qu'elles permettent de signaler les problèmes. Si quelqu'un pirate un serveur qui ne devrait pas interagir... J'en reviens à ce que je disais, s'il s'agit du serveur du service du marketing, je sais, moi, en tant qu'ingénieur, que ce serveur ne devrait pas avoir d'interactions avec les autres. Dès que la présence d'un intrus est détectée, une alarme se déclenche afin d'en informer les responsables de la sécurité.

Le président: Vous savez que vous êtes dans le marché des microserveurs.

M. Glen Motz: Oui.

Le président: D'accord. Prenez garde à votre frigo, toutefois.

Madame Dabrusin, vous disposez de cinq minutes.

Mme Julie Dabrusin (Toronto—Danforth, Lib.): Si je ne m'abuse, vous avez commencé à parler des influences extérieures, mais sans entrer dans les détails. J'aimerais donc y revenir.

À notre dernière réunion, nous avons reçu les représentants de HackerOne. Ils nous ont expliqué qu'il est possible d'améliorer la sécurité d'un système en faisant appel à des gens qui ont ce type de connaissances, car on peut alors en connaître les vulnérabilités. Selon eux, nous devrions légiférer pour mieux protéger ceux qu'ils appellent les « pirates éthiques ». Personnellement, je ne raffole pas de ce terme, mais tant qu'on comprend qu'ils sont du côté des bons et non des méchants.

Qu'en dites-vous? Devrait-il y avoir des lois pour protéger ces types de pirates et favoriser ce genre d'activité?

● (1630)

M. Jonathan Reiber: Contrairement aux autres domaines, dans le cyberespace, c'est le cerveau l'arme la plus puissante, ou à peu près. Ce qui compte, c'est la personne qui est là, ce qu'elle sait et ce dont elle est capable. Ses intentions comptent pour beaucoup.

Selon moi, le piratage électronique — personnellement, je préfère l'expression « test de pénétration » — est absolument essentiel à toute bonne stratégie de sécurité. C'est bien beau de se doter des meilleurs appareils du monde, d'avoir le fin du fin en matière de sécurité et de dépenser sans compter, mais vous avez aussi besoin d'une personne qui va sans cesse essayer de pénétrer dans votre réseau, d'en tester la résistance et d'en déceler les vulnérabilités, comme s'il s'agissait d'un adversaire qui essaie de se frayer un chemin jusqu'à vos données.

Je préfère ne pas m'avancer pour ce qui est des lois. C'est très compliqué. Les Accords de Wassenaar prévoient des mesures législatives d'envergure internationale et les choses suivent leur cours, mais...

Mme Julie Dabrusin: Pardon?

M. Jonathan Reiber: Wassenaar? Ma connaissance de l'orthographe allemande et néerlandaise est limitée, mais je peux vérifier pour vous.

Mme Julie Dabrusin: Je vous remercie.

M. Jonathan Reiber: Mondialement, la prolifération des logiciels malveillants et des tests de pénétration est inquiétante, parce qu'on ne sait jamais ce qu'une personne pourrait être tentée de faire une fois qu'elle a acquis ce type de connaissances ni même si elle ne dispose pas d'un logiciel lui permettant de percer vos défenses.

La Pennsylvanie a adopté une loi qui définit qui peut utiliser des logiciels malveillants, et dans quel but. Voilà pourquoi j'imagine que, plus on va avancer, et plus il y aura de lois pour encadrer les tests de pénétration et même la possession de logiciels malveillants. C'est très compliqué de vérifier pourquoi une personne a un logiciel malveillant sur son ordinateur et comment il a pu se trouver là: son appareil a-t-il été infecté ou a-t-elle quelque chose derrière la tête? Pour prouver quoi que ce soit, il faut connaître les intentions de cette personne. C'est compliqué.

Mme Julie Dabrusin: Monsieur Porter, y a-t-il des choses à surveiller selon vous? Y a-t-il des avantages à procéder ainsi?

M. Christopher Porter: J'insiste sur ce que disait mon collègue à propos des risques: il faut une certaine tolérance, surtout au niveau universitaire et avant, car il faut des gens pour tester les limites de la sécurité informatique — y compris des chercheurs professionnels — sans qu'ils soient considérés comme des criminels. Tant que c'est dans une bonne intention et qu'ils ne causent pas délibérément de dégâts. Selon moi, les États qui réglementent ce domaine ou qui légifèrent sont bien intentionnés, car ils veulent améliorer la cybersécurité, mais dans les faits, ils rendent impossible la tenue de recherches inédites.

Je n'ai évidemment pas les compétences requises pour donner mon avis sur les lois canadiennes, mais je vous en prie: résistez à l'envie de criminaliser ce qui, au fond, n'est rien d'autre que des mathématiques et de la logique sous forme électronique. N'en faites pas un acte criminel, parce que ces gens qui emploient leur créativité pour explorer les limites du possible, vous aurez peut-être besoin d'eux un de ces jours pour défendre votre pays. Rien ne pourrait compromettre davantage vos relations avec les membres du milieu de la sécurité que de criminaliser leur travail ou de prêter une intention coupable à ce qui pourrait bien n'être que de la curiosité intellectuelle inoffensive.

Mme Julie Dabrusin: C'est ce qui m'amène à ma prochaine question. Je crois que c'est vous, monsieur Reiber, qui avez dit que le manque d'infrastructures humaines, faute d'un meilleur terme, constituait la troisième partie du problème. On nous a très souvent répété qu'il faut doter l'humain des capacités nécessaires pour comprendre la cybersécurité.

D'après ce qui se fait ailleurs dans le monde, y a-t-il des choses que nous devrions reproduire pour nous doter de ces capacités, ou au contraire éviter?

M. Jonathan Reiber: Je commencerais par vous recommander la carte que vient de publier le National Institute of Standards and Technology. Sauf erreur, aux États-Unis, c'est le National Institute for Cybersecurity Education qui est chargé de mettre en carte la densité de la population et le nombre d'utilisateurs. C'est un bon moyen de savoir si on répond bien aux besoins du marché du travail.

Je crois qu'une maîtrise et des études universitaires adaptées aux normes techniques de l'heure, comme Security Plus ou CISSP... Ces programmes d'études permettent d'apprendre certaines des fonctions au coeur de la cybersécurité. Quant à savoir la mesure dans laquelle les collèges communautaires — je ne sais pas trop comment vous les appelez ici, au Canada, pardonnez-moi... Les établissements qui offrent des programmes de cybersécurité sont très utiles, et nous avons constaté que cela aide beaucoup quand le gouvernement fédéral offre de l'aide aux universités qui souhaitant en offrir un.

Ce qui aide aussi, c'est quand les universités d'État sont regroupées autour des industries qui entament la transition. Chez nous, le secteur manufacturier et des pans entiers de l'économie américaine ont énormément évolué. Je pense par exemple à l'Université d'État du Michigan, qui devrait se doter bientôt d'un programme sur la sécurité dans le secteur de l'automobile, qui a lui-même entamé la transition vers la cybersécurité. C'est très utile de dénicher les synergies à l'intérieur d'une grappe industrielle et d'investir dans un programme universitaire correspondant.

J'aimerais en terminant parler de l'évolution de la Cyber Mission Force, qui relève des forces américaines. Créée en 2012, elle est devenue pleinement opérationnelle en 2018. Les personnes qui en font partie — elles sont 6 200 — sont des sommités, et les investissements consentis par le gouvernement ont un énorme pouvoir dissuasif. Ces pirates sont intégrés à l'armée, et il s'agit bel et bien de pirates. Leur formation a quand même duré cinq ans — en tout cas cinq ans pour l'ensemble du groupe, parce qu'il a fallu changer certaines personnes d'école, ce qui exige du temps et des efforts.

Il faut toujours un peu de patience, et c'est ce qui m'amène à dire: songez d'abord et avant tout à protéger vos applications les plus importantes.

● (1635)

Mme Julie Dabrusin: Je vous remercie.

Le président: Merci.

M. Christopher Porter: Monsieur le président, si vous le permettez, j'aimerais faire quelques observations.

Le président: Mme Dabrusin s'est vu accorder beaucoup de temps par la présidence.

Peut-être, aurez-vous l'occasion de formuler vos observations à un moment ultérieur.

Monsieur Eglinski.

M. Jim Eglinski (Yellowhead, PCC): Merci, Monsieur le président. J'espère que vous vous montrerez aussi généreux avec moi.

Le président: Vous êtes loin d'être aussi charmant que Mme Dabrusin.

M. Jim Eglinski: Allez! Vous avez vu mon visage?

Messieurs, je vous remercie de votre présence aujourd'hui. Vos propos sont à la fois très intéressants et un peu effrayants.

Monsieur Reiber, durant votre présentation, vous avez mentionné qu'au cours des 35 dernières années, environ quatre milliards de personnes se sont jointes aux réseaux électroniques. Je crois vous avoir entendu dire à un moment donné — vous ou quelqu'un d'autre — qu'au cours des cinq prochaines années, 25 % de plus s'y ajouteront, notamment en raison de l'essor que connaissent la Chine et l'Inde.

M. Jonathan Reiber: Oui.

M. Jim Eglinski: Évidemment, la cybermenace grandira avec le nombre de personnes en ligne. La croissance ne sera pas aussi marquée au Canada, bien entendu, mais j'imagine que, toutes proportions gardées, il y en aura une. Le fait que la Chine soit l'un de nos principaux adversaires du cyberespace m'inquiète vivement, et c'est sans doute le cas des membres du Comité ici présents.

Selon vous, quelles sont les quatre principales mesures que devrait prendre le pays pour se protéger à l'avenir?

M. Jonathan Reiber: J'ai préparé deux recommandations. Je vais tenter d'en présenter une troisième et une quatrième. C'est une excellente question.

En premier lieu, il est crucial de protéger les infrastructures essentielles et de déterminer les entreprises et les organismes qui comptent le plus pour le bon état général de l'économie et de la sécurité du pays. Pour faire une analogie, je dirai qu'un pays qui n'a pas ciblé ces sociétés et ces entités serait dans une situation presque comparable à Illumio, si notre entreprise n'avait pas déterminé quelles sont ses applications clés.

Il s'agit d'examiner l'organisation de l'intérieur en se demandant: quelles sont les applications les plus importantes? Voilà le deuxième point. Le premier consiste à cerner les organisations les plus importantes au pays. Ensuite, ces organisations doivent elles-mêmes investir dans un arsenal complet afin d'assurer la sécurité à l'intérieur et au périmètre. Elles doivent aussi déterminer quelles sont leurs principales missions et les données les plus importantes pour exécuter ces missions. Il s'agit d'un processus d'analyse auquel participent les équipes responsables de la sécurité et de l'infrastructure, ainsi que de nombreuses composantes de l'organisation.

Ce sont là quatre points. Le premier consiste à déterminer quelles sont les infrastructures essentielles au pays. Le deuxième consiste à cerner les principaux actifs au sein de l'organisation. Le troisième consiste à réfléchir à la mission de l'organisation et à se préparer à fonctionner sans accès aux données. Cela est très important. Si vos données disparaissaient aujourd'hui, quelles activités seraient impossibles à mener? Quelles activités devez-vous absolument être en mesure de poursuivre?

Le quatrième point revient à ce que j'ai dit concernant la dissuasion. Les pays doivent réfléchir aux moyens de dissuader les États-nations de s'en prendre à eux. Si on présume qu'on s'en prendra à nous, il vaut mieux décourager les gens d'essayer de le faire. En cas d'atteinte à la sécurité en ligne, il faut être prêt et avoir des mesures qui la déjouent. Toutefois, la dissuasion constitue une entreprise titanesque. Ultimement, l'expansion de l'Internet ne représente pas seulement un milliard d'utilisateurs de plus au cours des cinq prochaines années en Chine et en Inde seulement. En effet, il faut aussi penser à tous les appareils connectés dont ces utilisateurs vont se servir. Ainsi, il y aura expansion non seulement par rapport au nombre d'êtres humains, mais aussi par rapport au nombre de technologies que chaque être humain touchera.

● (1640)

M. Christopher Porter: J'ai quelques suggestions à faire, brièvement, si vous le permettez.

M. Jim Eglinski: Oui.

M. Christopher Porter: Ma perspective est quelque peu différente de celle de mon collègue.

Afin d'améliorer la cybersécurité, le Canada pourrait, entre autres, et sans ordre particulier, mettre davantage l'accent sur la diplomatie. La menace de représailles militaires, les sanctions ou les mises en accusation ne sont pas les seules solutions possibles aux conflits dans le cyberespace. Jusqu'à présent, rien ne prouve que ces solutions fonctionnent. On poursuit ces activités année après année en maintenant qu'elles ont un effet dissuasif et, pourtant, la cybermenace demeure? Comment peut-on faire ce lien? Je suis beaucoup plus optimiste que beaucoup d'autres par rapport à la diplomatie. Si vous consultiez une centaine d'experts, je serais peut-être le seul de cet avis. Je suis loin de faire partie d'une majorité.

Pour revenir à votre question, j'ajouterai en deuxième lieu que, pour les services gouvernementaux, il faut recruter parmi un bassin de candidats, non pas homogène, mais diversifié, tant sur le plan de la personnalité que celui des antécédents professionnels. Comme les cyberactivités font partie de la vie de tous les jours, il ne suffit pas de recruter en fonction des compétences techniques. En effet, il faut embaucher des candidats de tous les horizons, comme des économistes, des politicologues, etc.

Enfin, pour revenir à un point que j'ai soulevé antérieurement, je crois qu'un pays fait fausse route en agissant en fonction de la liste de ceux qu'il défendra et ne défendra pas. Selon moi, c'est là un problème de contre-insurrection.

M. Jim Eglinski: Puis-je vous interrompre avec une brève question?

M. Christopher Porter: Bien sûr.

M. Jim Eglinski: Vous représentez tous les deux des organisations offrant des services de sécurité. Les méchants sont-ils tous du même niveau? Je suis en train de dire que vous êtes parmi les bons. Y a-t-il de mauvaises organisations qui offrent des services à la clientèle?

M. Christopher Porter: Oui, certainement. Il est possible d'acheter des services comme on peut acheter n'importe quoi en ligne. Les marchés sont conçus ainsi, particulièrement pour les criminels.

Le président: Merci, monsieur Eglinski.

M. Jim Eglinski: Merci de m'avoir laissé poser la question.

Le président: J'ignorais que Washington accordait toujours de l'importance à la diplomatie.

Des voix: Oh, oh!

M. Jonathan Reiber: Au cas où quelqu'un se poserait la question, je peux vous assurer que je suis pour la diplomatie.

Le président: Madame Sahota, vous avez cinq minutes.

Mme Ruby Sahota (Brampton-Nord, Lib.): Merci.

Comme dans tous les autres pays, notre gouvernement réfléchit à l'interférence et à l'influence, d'autant plus que les élections approchent. La loi exige désormais une transparence accrue de la part des sociétés de médias sociaux concernant les entités qui diffusent des publicités sur leur plateforme. De plus, beaucoup d'argent a été investi pour la cybersécurité, ce qui est nécessaire. Selon moi, il faut même en faire plus.

D'après vous, quelle responsabilité incombe aux médias sociaux? Comment pourraient-ils mieux protéger contre la fraude les utilisateurs de leurs bases de données et empêcher les joueurs étrangers d'envahir l'espace? Que pensez-vous du fait qu'ils ignorent ce qui se passe ou qu'ils choisissent de ne rien faire? J'aimerais entendre les observations de nos deux témoins là-dessus.

M. Christopher Porter: La plupart des grandes sociétés de médias sociaux investissent de manière considérable dans la sécurité — en particulier maintenant. Selon moi, elles font de leur mieux pour s'attaquer au problème. Sans parler en leur nom, je peux dire que beaucoup d'entre elles investissent des montants importants à cette fin. Déjouer les opérations militaires sophistiquées d'un gouvernement étranger représente une tâche énorme, même pour une très grande société du secteur privé. Selon moi, pour n'importe quelle équipe de sécurité, quelle que soit l'organisation dont elle fait partie, c'est beaucoup demander de se débrouiller seul devant un tel problème.

J'insiste sur le fait qu'une bonne partie des vulnérabilités du Canada ne résident pas dans les infrastructures physiques. Les grosses bases de données et les choses physiques sont vulnérables, certes, mais les candidats, les équipes de campagne et les partis constituent aussi des cibles de choix pour les adversaires qui souhaitent s'ingérer dans les élections.

S'ils se trouvaient à être visés dans les médias sociaux ou à faire l'objet d'une campagne de désinformation, je ne sais pas s'ils disposeraient des mêmes ressources et moyens que l'infrastructure de scrutin.

Il faut donc fournir aux candidats, aux équipes de campagnes et aux partis le même soutien en matière de renseignement sur la cybermenace que celui prévu pour les infrastructures et les mécanismes électoraux. C'est très important, selon moi. Assurément, depuis 2016, nous avons constaté que la plus grande partie de la menace est générée par les médias sociaux, mais qu'elle s'attaque à des campagnes individuelles, et non à ce qui est protégé, c'est-à-dire aux infrastructures gérées par le gouvernement.

Cette vulnérabilité est présente non pas seulement au Canada, mais partout en Occident.

● (1645)

Mme Ruby Sahota: Oui.

M. Jonathan Reiber: Assurément, les sociétés de médias sociaux ont investi de manière assez considérable depuis 2016. Dans leurs communications publiques, elles indiquent à quel point elles ont su établir des partenariats avec le gouvernement. En ce qui concerne les infrastructures qui sont susceptibles d'être manipulées au Canada, c'est là un pas très important à franchir pour les sociétés de technologies, selon moi.

Au cas où, avant les élections, il n'existerait pas d'infrastructure pour le partage de renseignements ou de mécanisme de coopération entre les secteurs public et privé, je souligne que nous avons ce qu'on appelle un cadre de sécurité durable aux États-Unis, qui réunit les principales entreprises de technologies de l'information, les propriétaires et les exploitants des infrastructures et les appareils du renseignement et de la sécurité nationale afin qu'ils partagent des renseignements sur la menace et des solutions en matière de conception. Il s'agit là d'une recommandation à plus long terme.

La deuxième chose que je veux aborder concerne l'inscription des électeurs. Chez nous, aux États-Unis, l'inscription en vue des élections est gérée par différents départements dans chaque État. Là où ce n'est pas déjà fait, les organisations doivent sécuriser leurs centres de données afin d'éviter que les gens fraudent les listes d'inscription électorale.

Au Canada, établir qui est responsable de l'inscription des électeurs et où on stocke les données et sur quel serveur pourrait aider quelqu'un qui vise à manipuler les résultats des élections à investir judicieusement.

J'ajouterai qu'une autre mesure consiste à informer abondamment le public de ce qui pourrait arriver. Le département de la Justice aux États-Unis a fait de l'excellent travail à cet égard. L'Université Harvard a un programme sans but lucratif visant à éduquer les secrétariats des États du pays en matière de gestion de crise. Le programme, dont les détails se trouvent sur le site de Harvard, est intitulé « Defending Digital Democracy Projet », ou projet de défense de la démocratie numérique.

Mme Ruby Sahota: Quand cette initiative a-t-elle vu le jour?

M. Jonathan Reiber: Il y a plus de deux ans.

On trouve sur le site de bons documents pour la formation du personnel électoral en matière d'intervention en cas de crise et de gestion de crise.

Mme Ruby Sahota: Le projet a-t-il été lancé en raison de ce qui s'est produit aux élections américaines de 2016?

M. Jonathan Reiber: C'est le résultat direct de ce qui s'est passé pendant les élections de 2016.

Un certain nombre de personnes qui gèrent ce programme, qui n'en est qu'un parmi plusieurs, viennent de cette administration. Ils ont appliqué les leçons qu'ils ont apprises.

Il est évident que les médias sociaux comptent pour beaucoup et que la population canadienne doit être sensibilisée aux risques possibles qui y sont associés. Cela en fait certainement partie.

Vous devriez tenter de travailler avec les entreprises de médias sociaux afin de transmettre à l'avance un message sur leurs plateformes pour informer les utilisateurs canadiens des mesures qui ont été prises pour empêcher l'ingérence électorale. Je crois qu'ils le font déjà, mais ce serait une mesure à prendre.

J'ai une dernière chose à dire. Je sais qu'il ne reste plus de temps... J'aime beaucoup parler.

Le président: Vous avez tout compris.

M. Jonathan Reiber: Ensuite, il faut tenter de savoir qui sera manipulé le prochain. Les élections, c'était une chose, n'est-ce pas?

Ce qui me préoccupe le plus, ce sont les données de recensement. Aux États-Unis, il va prochainement y avoir un recensement, soit en 2022 ou en 2025. Je ne me souviens plus très bien de la date exacte. Imaginez si quelqu'un est capable de s'introduire dans les établissements de recherche et de manipuler des données démographiques pour faire croire qu'un changement démographique accéléré ou un autre s'opère aux États-Unis. Cela changerait la façon dont les gens perçoivent la société dans son ensemble.

Mme Ruby Sahota: Oui.

M. Jonathan Reiber: La prochaine chose à faire serait de se pencher sur les établissements de recherche qui n'ont pas encore fait d'investissement en la matière et qui font un travail de recherche qui influence grandement l'identité générale d'un pays. Si j'étais un adversaire, c'est exactement ce genre d'établissements que je viserais. J'espère qu'ils ne nous écoutent pas.

Mme Ruby Sahota: Oh la la.

Le président: Il est difficile de savoir qui sont les chapeaux blancs et qui sont les chapeaux noirs.

Mme Ruby Sahota: Oui.

Le président: Monsieur Dubé, vous avez un tour généreux de trois minutes.

M. Matthew Dubé: Merci, monsieur le président...

Le président: Excusez-moi.

Je vois que les lumières clignotent. Cela veut dire qu'il nous reste à peu près une demi-heure.

Je passe maintenant à M. Dubé. J'aimerais poser quelques questions.

Je propose, chers collègues, que nous poursuivions jusqu'à 17 h 10. Les deux témoins qui sont présents sont venus de loin pour nous parler, et il se pourrait qu'il y ait des questions de suivi.

Cela convient-il à mes collègues?

Des députés: D'accord.

Le président: M. Dubé a la parole.

M. Matthew Dubé: Merci.

Je vais poser une question rapide étant donné que j'ai un tour généreux de trois minutes...

Vous avez mentionné la protection des centres de données en lien avec la question de l'Internet des objets. Je me sens toujours comme dans un film de *Mary Poppins* quand j'utilise ce terme. Est-ce qu'on remédie également à la menace de la manipulation de données en les protégeant? Vous avez également beaucoup parlé de cette question et je crois, surtout dans le cadre d'une étude sur le système financier, que cela pourrait aussi être un problème.

● (1650)

M. Jonathan Reiber: Oui, cela remédie à la menace de la manipulation des données en ce sens que pour modifier... Imaginez que vous essayez de faire comme les Russes qui, aux dernières nouvelles, auraient récemment piraté un GPS et redirigé des navires en mer Baltique. Prenons le cas des listes électorales dont il est possible de manipuler le contenu. Pour ce faire, il faut se rendre sur un réseau. Les applications n'existent pas simplement dans l'espace et je dis cela sans aucune condescendance.

Les applications et les serveurs, à bien des égards, sont une seule et même chose. Chaque fois que vous vous connectez à une application infonuagique et que vous entrez vos données, vous vous connectez à un serveur qui se trouve quelque part dans le monde. Si un centre de données a été sécurisé de l'intérieur, il est possible d'empêcher un intrus d'y installer un logiciel malveillant, que ce soit pour manipuler, voler ou détruire des données.

M. Matthew Dubé: Veuillez pardonner mes connaissances de non-initié à ce sujet. Cette étude nous fait tous sentir comme des luddites. Je tiens juste à m'assurer de bien comprendre.

Si quelqu'un ne met pas à jour ses micrologiciels, est-ce que le fait que les centres de données soient protégés suffit, même dans les cas où la sécurité de l'appareil n'est vraiment pas bonne. J'ai de la difficulté à résoudre la quadrature du cercle. Je ne sais pas si j'ai bien compris.

M. Christopher Porter: C'est difficile pour moi aussi. Je crois qu'une partie du problème est que beaucoup des groupes les plus sophistiqués utilisent des justificatifs d'identité valides. Si vous êtes le président d'une banque, ils vous piègent pour obtenir vos justificatifs d'identité. Il n'y a aucun comportement malicieux visible. Ils ne font qu'exploiter vos justificatifs d'identité.

Pour ce qui est du secteur financier, la question qui se pose est de savoir à quel point on pourrait retourner en arrière si on découvrait un jour que ce genre de chose avait eu lieu. Est-ce que ce serait un jour, une semaine ou un mois? Pourrait-on régler les problèmes des comptes atteints? À mon avis, la manipulation de données n'est pas tant une question criminelle, mais plutôt une question de vulnérabilité potentielle du secteur financier pouvant poser un risque systémique. Le plus grand risque systémique, c'est que des données soient manipulées dans de grandes banques, et que ce soit annoncé un mois ou un an plus tard à la population que tel groupe avait les justificatifs d'identité de telle personne et qu'il a modifié deux ou trois comptes. Le nombre importe peu. Toute personne qui croit qu'on lui a imposé des frais non justifiés va mettre en doute toutes les activités sur son compte.

Je crois que c'est un risque réel, et que la plupart des organismes, en raison de leur taille, soit ils sont très gros et ont beaucoup de données, soit ils sont très petits et n'ont pas encore fait d'investissements en la matière, ne savent pas exactement en quoi consiste un comportement normal sur leur réseau. Il est très difficile de revenir en arrière après qu'un incident ait lieu si l'on n'a pas les sauvegardes nécessaires et c'est un risque réel pour le secteur financier en particulier.

Le président: M. Dubé a la parole.

M. Jonathan Reiber: Monsieur le président, si je pouvais juste...

Le président: Allez-y.

M. Matthew Dubé: Vous faites preuve de beaucoup d'indulgence.

Le président: Je fais preuve de... Oui.

Allez-y.

M. Jonathan Reiber: Merci, monsieur le président. Je tenterai d'être aussi bref que possible.

Je ne dis pas qu'il ne reste plus rien à faire si les centres de données ont été protégés à l'interne et qu'on peut simplement rentrer à la maison et dormir. Ce n'est pas ce que je dis. Il doit y avoir des couches de sécurité pour protéger les investissements.

Si l'on est face à un adversaire doué, il faut mettre en place des moyens de sécurité pour protéger l'utilisateur, que ce soit le secrétaire de la Défense ou le président ou PDG d'un organisme, soit l'authentification multifactorielle, des pare-feu, et tout le reste.

Ce que je tente de faire valoir, c'est que si l'adversaire est capable de passer l'étape de l'authentification multifactorielle ou de décrypter l'encodage et qu'il arrive à s'introduire dans le système, s'il trouve un serveur, qui a une faible valeur, et que des investissements ont été faits pour protéger le centre de données de l'intérieur, vous allez pouvoir beaucoup plus limiter les dégâts. Si vous n'en avez pas fait, laissez tomber. Ils vont être capables de prendre possession de toutes les applications de votre entreprise. Si vous n'en avez pas fait, vous pourriez perdre *x* ou *y* données ou *x* ou*y* serveurs, mais vous pourrez gérer les coûts associés, sauf si c'est le président ou secrétaire de la Défense, ou quiconque d'autre a eu son compte piraté. Si c'est une personne qui occupe un emploi de niveau inférieur, les dégâts seront moins importants.

Le président: C'était un tour généreux de trois minutes.

Monsieur Reiber, j'ai écouté votre intervention, et je vous ai entendu dire essentiellement qu'il y avait différentes couches de protection et que vous avez un programme de microsegmentation qui fait qu'il y a trois points d'accès au lieu de 3 000.

Compte tenu de l'arrivée du réseau G5, ce modèle de protection de sécurité est-il toujours le plus efficace?

M. Jonathan Reiber: Je n'ai pas encore mûrement réfléchi à l'impact qu'aura le réseau G5 sur notre capacité globale. Je n'en sais pas non plus assez sur le réseau G5 pour vous conseiller en la matière.

Si je devais émettre une hypothèse et dire ce que je pense, je dirais que le réseau G5 va nous permettre d'envoyer plus rapidement des données. Cela ne devrait pas avoir de conséquences sur les propositions que je fais. Je dirais qu'elles seront toujours d'actualité. Si tout ce qui change, c'est la vitesse à laquelle les données sont transmises, les règles et les politiques gérant les applications et les serveurs resteront les mêmes. Ce sont deux éléments qui sont en quelque sorte distincts. Ce sont deux bêtes différentes. Elles ne devraient pas avoir d'incidence négative l'une sur l'autre.

Si une chose peut perturber l'avenir global de l'information, mis à part la micro-segmentation, c'est l'informatique quantique. Elle pourrait changer complètement la nature de la cybersécurité. Même là, je ne crois pas que les couches de sécurité seraient entièrement perturbées.

● (1655)

Le président: Merci.

Monsieur Porter, vous êtes évidemment au courant de l'article 5 du traité de l'OTAN. Ces cyberattaques ont lieu en quelques microsecondes. Vous pourriez être en guerre sans le savoir.

D'après vous, l'architecture décrite dans le traité de l'OTAN, qui a environ 50 ans, est-elle adéquate pour répondre à des cyberattaques? Cela a déjà eu lieu. Il n'y a qu'à penser à l'Estonie. Pensez-vous que ce traité doit être considérablement repensé?

M. Christopher Porter: Monsieur le président, je crois que les mécanismes prévus dans le traité permettent aux membres de l'OTAN de prévoir une réponse politique commune. À mon avis, la grande question est de savoir qui va demander ce genre de réponse et dans quelles circonstances! Selon moi, aux États-Unis du moins, on se prépare à la cyberattaque de type Pearl Harbor, un événement dévastateur majeur. Cela ressemble bien plus à des cyberguerres de tranchées sauf que ce sont les particuliers et les entreprises qui sont dans les tranchées plutôt que les soldats et les intervenants gouvernementaux.

Que fait-on face à cela? Voilà le problème auquel est confrontée l'alliance en ce moment. Ce ne sont pas tant les mécanismes juridiques permettant d'invoquer la défense commune qui pose problème. On y travaille et je crois que dans un réel cas d'urgence, elle serait invoquée correctement de toute façon. Encore une fois, je crois que le plus gros problème est qu'il serait possible de mourir d'une mort par mille coupures et que personne ne penserait au fait qu'il faille le soulever au titre de l'article 5.

Un deuxième problème, qui est beaucoup plus stratégique à considérer, est que les États-Unis et le Canada ont tous les deux d'importantes capacités de renseignement en matière de cybersécurité dans le secteur privé et au sein du gouvernement, mais ce ne sont pas tous les alliées de l'OTAN qui en ont. Si un incident cybernétique majeur avait lieu et qu'on voulait invoquer l'article 5, comment convaincrait-on les autres membres de l'OTAN du fait qu'un incident a eu lieu et que nous avons bien attribué ce fait?

On peut faire hautement confiance aux États-Unis et au Canada à ce chapitre. De nombreux pays n'ont pas assez de gens de l'autre côté de la table pour recevoir l'analyse, l'interpréter et prendre les mesures politiques adéquates.

Ont-ils le même genre d'experts que nous? Je crois que c'est un problème. Comment peut-on partager notre capacité de comprendre et de savoir à quel groupe les attaques cybernétiques sont attribuées? Voilà les deux problèmes pour moi.

Le président: D'accord.

Enfin, la réaction du Congrès américain à l'affaire Huawei consiste essentiellement à accepter l'hypothèse selon laquelle toute cyberattaque perpétrée par la Chine serait si foudroyante et dévastatrice que tout serait, pour ainsi dire, déjà terminé.

Est-ce également votre perspective?

M. Christopher Porter: Monsieur le président, je pense que si on parle exclusivement d'une guerre informatique, effectivement, ce pourrait être une interprétation raisonnable. Cela dit, si les risques demeurent élevés, les réponses aux cyberattaques ne sont pas nécessairement limitées au cyberespace. Je m'en remettrais à mon collègue pour vous décrire ce qui se passerait en termes concrets. Je ne partage donc pas nécessairement cette perspective défaitiste compte tenu des autres options plus conventionnelles qui s'offriraient aux États-Unis dans un tel contexte.

Le président: Monsieur Reiber, souhaitez-vous ajouter quelque chose?

M. Jonathan Reiber: D'accord.

Je ne suis pas non plus d'avis que la Chine gagnerait instantanément une cyberguerre. Cela dit, de nombreux pays sont aujourd'hui capables de livrer des attaques dévastatrices contre les infrastructures essentielles partout dans le monde.

Entre la Russie, la Chine, l'Iran et la Corée du Nord, le pays qui m'inquiète le plus — et de loin — est la Russie. C'est parce qu'elle a implanté des logiciels malveillants à certains endroits du réseau électrique américain, et on ne sait pas exactement pourquoi.

Si un de ces adversaires devait initier un conflit dans le cyberespace, je doute qu'il remporterait une victoire convaincante si rapidement, parce que nous avons investi dans la Cyber Mission Force. Nous avons donc l'avantage d'un effectif de 6 200 informaticiens et opérateurs d'élite qui surveillent ces pays-là de très près.

Quand on se met à grimper l'échelle d'escalade, on comprend rapidement que, dans le cas de la Chine et de la Russie, mais particulièrement la Chine, nos économies sont intimement liées. Ces pays savent bien que toute escalade des conflits au-delà d'un certain point dans le cyberespace commencera à entraîner de graves conséquences économiques, surtout si cela s'accompagne d'un éventuel conflit militaire.

J'ai récemment écrit un article expliquant pourquoi je pense que la Chine constitue la plus grande menace à long terme dans le cyberespace. Tout revient au développement de technologies d'armement perfectionné dans d'autres domaines, comme les canons à rails. C'est pour cette raison que les États-Unis ont investi dans leur troisième stratégie compensatoire dirigée par Shawn Brimley. Si on envisage ce qui pourrait se passer entre ces deux pays au courant des 20 prochaines années, je pense qu'on verrait un certaine égalité en matière de progrès technologiques.

Pour revenir à ce qu'a dit mon collègue, c'est évidemment un situation que l'on veut éviter. Ce serait dans l'intérêt à long terme d'aucun des deux pays. L'intérêt des deux pays — autant les États-Unis que la Chine, et aussi le Canada, je suppose — serait de maintenir des relations productives et paisibles qui mèneront à la prospérité économique de tous les pays du Pacifique et ailleurs. Tout revient donc à une question de diplomatie et aux efforts nécessaires pour leur expliquer ce que signifie l'escalade et ce qu'elle représente.

Cela dit, nous devons malheureusement maintenir des options technologiques en cas d'éventuel conflit.

● (1700)

Le président: D'accord, merci.

Monsieur Spengemann, aviez-vous une question à poser?

M. Sven Spengemann: Oui, monsieur le président. Merci beaucoup. Je serai bref.

Je voulais que ça figure au compte-rendu. C'est bien le Comité de la sécurité publique. Pour revenir à la cybercriminalité commerciale, aux crimes cybernétiques peut-être même perpétrés par de grandes sociétés contre de petites entreprises, pourriez-vous nous décrire en quoi consiste le modèle d'application de la loi?

Veuillez commencer par le manque de signalement. Je pense que vous avez déjà abordé la question lorsque vous avez parlé de la nécessité de dresser les exigences de gestion provisoire de manière à inciter les entreprises, premièrement, à signaler les incidents de cybercriminalité. Seulement par la suite peut-on commencer à recueillir les preuves et, éventuellement, procéder aux poursuites. Y a-t-il des actions judiciaires en cours qui sont restées dans le contexte nord-américain? Je pense que tout se complique énormément lorsqu'interviennent des acteurs étrangers ou des sociétés étrangères.

Que dire du modèle fondamental d'application de la loi et de sa pertinence en matières de cybercriminalité en 2019? Avez-vous des perspectives à ce sujet-là?

M. Jonathan Reiber: Je serai très bref.

Le FBI joue un rôle pivot dans la poursuite des cybercrimes au sein des États-Unis, et sa division de la sécurité nationale s'occupe des acteurs externes qui livrent des attaques contre les États-Unis. À ma connaissance, c'est le seul organisme de sécurité nationale ayant l'autorité nécessaire pour mener des opérations dans le cyberespace et couper l'accès à un serveur situé aux États-Unis.

Nous avons pris l'habitude de recueillir des éléments de preuve au sein du ministère de la Justice. Le FBI et le ministère de la Justice travaillent main dans la main. J'aimerais pouvoir vous citer une affaire précise qui illustrerait bien mon point; je pourrai certainement vous faire parvenir plus d'information. Il s'agit cependant...

M. Sven Spengemann: La capacité existe. L'effectif est suffisant.

M. Jonathan Reiber: Tout à fait, oui.

La Computer Fraud and Abuse Act a été adoptée dans les années 1980, mais je me trompe sûrement là-dessus. Il ne faut jamais faire des calculs en public ou bien citer des dates qu'on ne connaît pas.

Donc, depuis l'adoption de la loi américaine sur la fraude et la malveillance informatique, à l'époque où des pirates informatiques américains livraient des attaques contre des cibles américaines...

La cyberattaque contre Dyn, dont vous avez peut-être entendu parler, est un bon exemple. Elle était d'une envergure telle que des organisations essentielles comme Netflix et Twitter en ont été ralenties. Tout le monde s'arrachait les cheveux. Le directeur du renseignement national a fait une déclaration officielle disant que la menace était grave. Finalement, il s'agissait de trois personnes aux États-Unis qui font aujourd'hui leur service communautaire en aidant le gouvernement à prévenir des cyberattaques.

C'est un agent du FBI particulièrement entreprenant situé à Anchorage, en Alaska, qui a ouvert l'enquête. Le FBI est structuré de manière à permettre à différents bureaux au pays de faire enquête. Ils ont fait toutes leurs activités d'informatique judiciaire et ont fini par trouver les responsables.

M. Sven Spengemann: Monsieur Porter, auriez-vous quelque chose à ajouter rapidement?

M. Christopher Porter: Oui, je dirais que la GRC a d'importantes compétences techniques lui permettant d'enquêter de tels crimes elle-même. FireEye offre un soutien technique dans le cadre de maintes enquêtes au Canada.

J'ignore dans quelle mesure cela s'applique également au Canada, mais aux États-Unis, on tient beaucoup à ce que les entreprises victimes se sentent à l'aise de signaler toute information, à ce qu'elles soient indemnisées et à ce qu'elles ne subissent aucun préjudice en conséquence. Il est absolument essentiel de bien cerner la menace, surtout lorsqu'il y a lieu de penser que l'activité criminelle puisse également présenter un risque pour la sécurité nationale. Il faut clairement préciser dans la loi que les entreprises peuvent signaler une atteinte à la protection des renseignements personnels sans craindre que cela se retourne contre elles.

Le président: Merci, monsieur Spengemann.

Il nous reste environ 15 minutes avant le vote.

Monsieur Paul-Hus, à vous de poser la dernière question.

M. Pierre Paul-Hus: Merci, monsieur le président.

L'étude du Comité porte sur le secteur bancaire en particulier. Lors de notre réunion en Californie, vous avez parlé de la France et des mesures musclées qu'elle prend contre les cybermenaces. Pourriez-vous nous en parler un peu plus longuement?

Et puis ma dernière question porte sur les banques aux États-Unis. Les banques américaines sont-elles bien protégées ou bien ont-elles besoin de protections supplémentaires? Qu'est-ce que le Canada peut faire de mieux?

● (1705)

M. Jonathan Reiber: Je pense qu'un certain nombre de pays ont pris de rigoureux règlements pour protéger les infrastructures essentielles. Je pense que la France, avec l'ANSSI et les directives qu'elle a prises, est un excellent exemple. Mon impression est qu'elle exerce un plus grand contrôle sur ses infrastructures essentielles, du moins sur le plan législatif, que les États-Unis.

Notre exemple relève de la liste d'entités visés par l'article 9, dont j'ai parlé plus tôt. Nous sommes passés à travers, demandant quelles sont les infrastructures essentielles les plus importantes aux États-Unis, autrement dit, celles qu'il faut protéger à tout prix.

Nous n'avons toujours pas de loi nationale sur la protection des données et de la vie privée aux États-Unis. Pour la gestion des atteintes, nous avons les États, et chaque État joue un rôle différent. La Californie et le Colorado ont adopté un règlement plus rigoureux. Le RGPD, lui, est très rigoureux dans cette optique-là. Il exige que toute atteinte à la vie privée soit prise en main dans un délai très court et prévoit une amende en cas de non-respect.

Le RGPD en vigueur en France ainsi que les textes en vigueur en Californie et au Colorado sont parmi les règlements les plus progressifs et aussi les plus musclés. Cela ne veut pas dire qu'il n'y pas de détracteurs. Bon nombre de secteurs ressentent maintenant le besoin d'avoir à l'effectif un agent de vérification de la conformité pour répondre à toutes les exigences, ce qui n'est pas toujours une tâche facile. Étant donné la nature du cyberespace, je pense qu'on s'attend simplement à ce que les sociétés s'adaptent en conséquence.

Le secteur financier est particulier dans la mesure où il est assiégé depuis son arrivée sur Internet. Il y a déjà eu un certain nombre d'infractions majeures qui ont retenu l'attention des responsables de la sécurité nationale et des intervenants du secteur des banques, et ce dernier en est venu à investir des sommes considérables en cybersécurité. C'est pour cette raison qu'il a tellement d'avance.

Peut-être l'ai-je déjà mentionné, mais les banques sont bien plus avancées que bien d'autres secteurs économiques aux États-Unis. On pourrait raisonnablement supposer qu'il en est ainsi parce qu'elles ont les moyens d'attirer les employés les plus compétents. Elles ont les moyens de verser de bons salaires à quiconque est prêt à travailler fort.

Si je puis enfiler mon chapeau d'historien pendant un instant, globalement, si on prend l'ensemble des secteurs, la Cyber Mission Force et l'évolution de la stratégie de cybersécurité... Lorsque j'ai commencé à travailler dans le domaine en 2010 — à l'époque de Shawn Brimley, que j'ai mentionné — on avait un mal fou à recruter du monde pour travailler dans les bureaux de cyberpolitique au Pentagone. C'était une bande de jeunes mordus d'informatique que personne ne prenait au sérieux.

Aujourd'hui, c'est un problème qui nous touche tous. À mon avis, nous pouvons maintenant attirer des gens très compétents dans toutes sortes de secteurs, ce qui me porte à croire que c'est un problème qu'on va pouvoir régler. Je pense vraiment qu'on va pouvoir le faire et qu'on pourra adopter de bonnes technologies. Le secteur bancaire aura ouvert la voie, et un jour quelqu'un racontera son histoire et demandera aux gens qui y étaient comment ça s'est vraiment passé.

M. Pierre Paul-Hus: Merci.

Le président: Merci, monsieur Paul-Hus.

M. Picard a une question d'importance critique à poser.

M. Michel Picard: Effectivement, et techniquement, on peut y répondre par oui ou par non.

Messieurs, avez-vous un gadget Alexa ou Google Home à la maison?

M. Jonathan Reiber: S'il n'en tenait qu'à moi, je n'aurais même pas la télé.

Des voix: Oh, oh!

M. Christopher Porter: J'abonde dans le même sens.

Si possible, j'aimerais également répondre à la question précédente.

Le secteur financier américain est bien défendu, mais il ne s'agit pas seulement d'investissements monétaires et technologiques; c'est aussi une question d'autorité. Si le centre des opérations de sécurité d'une grande institution financière au Canada, par exemple, découvre un problème, a-t-il l'autorité de suspendre les opérations? La suspension des opérations commerciales le temps de remédier au problème peut causer des pertes de millions de dollars. Deux sociétés du même secteur situées d'un côté et de l'autre de la rue peuvent dépenser autant d'argent en sécurité et quand même obtenir des résultats très différents selon l'autorité qu'ont les responsables de suspendre les opérations commerciales.

Soit dit en passant, j'ajouterais qu'au-delà du secteur financier, dont les perturbations représentent une menace systémique pour l'économie canadienne, la plupart des sociétés cotées en bourse à qui j'ai parlé aimeraient investir davantage dans la cybersécurité. Elles n'ont pas l'impression de pouvoir le justifier puisque, sur le court terme, de tels investissements feraient chuter leur chiffre d'affaires. On estime que c'est un centre de coûts. C'est un domaine où il peut être utile de réglementer, car en l'absence de règlements ou de normes industrielles, quiconque prend l'initiative est désavantagé, car tout investissement dans la cybersécurité équivaut à une baisse des profits.

Ce sont deux facteurs qui contribuent aux lacunes en matière de cybersécurité.

Le président: Sur ce, je pense que nous nous arrêterons là.

Au nom du Comité, je tiens à vous remercier, monsieur Porter et monsieur Reiber, d'avoir pris la peine de vous rendre jusqu'ici, de Washington et de la Californie, respectivement. Ce fut très instructif.

Comme M. Dubé, j'ai, moi aussi, l'impression d'être un luddite quand j'entends certains des témoignages, mais j'espère que nous nous améliorerons avec le temps.

Merci encore une fois à vous.

● (1710)

M. Jonathan Reiber: Merci, monsieur le président.

M. Christopher Porter: Merci, monsieur le président.

Le président: La séance est levée.