CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 157 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 10 avril 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 10 avril 2019

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Il est 15 h 30, et nous avons le quorum.

Il y a deux témoins dans le premier groupe, M. Ryland et M. Fadden.

Avant de commencer, chers collègues, nous avons deux ou trois écueils à contourner en ce qui concerne notre ordre du jour, et nous devons donner certaines directives aux greffiers et à l'analyste. La réunion du sous-comité devait commencer à 17 h 30. Cependant, la sonnerie se fera peut-être entendre à 17 h 30, faisant ainsi en sorte que nous ne pourrions pas commencer la réunion du sous-comité.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): Commençons à 17 h 29.

Le président: À 17 h 29, c'est un peu serré. Je pensais commencer plutôt à 17 h 20. Nous pourrons mettre fin à la réunion actuelle à 17 h 20 ou peut-être l'étirer un peu jusqu'à 17 h 25.

S'il n'y a pas d'autres considérations, je vais demander à nos témoins de présenter leur exposé. Je n'ai pas prévu d'ordre précis, mais je souligne que M. Fadden a déjà comparu de nombreuses fois devant le Comité, tandis qu'il s'agit, si je ne m'abuse, de la première comparution de M. Ryland.

M. Mark Ryland (directeur, Bureau du dirigeant principal de l'information, Amazon Web Services, Inc.): C'est exact, oui.

Le président: Je devrais peut-être laisser l'expert commencer afin que vous puissiez voir de quelle façon un excellent témoin présente son exposé.

M. Mark Ryland: C'est parfait.

Le président: Monsieur Fadden, s'il vous plaît.

M. Richard Fadden (à titre personnel): Merci, monsieur le président. Je m'attends à ce que votre jugement n'ait pas changé lorsque j'aurai terminé.

Le président: N'exigez pas qu'on passe au vote.

M. Richard Fadden: Encore merci de me donner l'occasion de discuter avec vous.

Pour commencer, je tiens à souligner que, dans le cadre de discussions avec le greffier et le personnel du Comité, j'ai précisé que je n'étais pas un expert du secteur financier, et on m'a suggéré de formuler quelques commentaires généraux sur la sécurité nationale et la cybersécurité, ce que je me propose donc de faire. J'espère que tout ça sera utile au Comité.

Je tiens à formuler des commentaires un peu inhabituels au sujet de votre ordre de renvoi. Vous parlez de sécurité économique nationale. Je suis sûr que ce titre a été choisi après mûre réflexion, mais j'aimerais dire — et je prêche un peu pour ma paroisse, ici — que les enjeux que vous abordez sont des enjeux de sécurité nationale, un point c'est tout. Il ne s'agit pas d'un sous-ensemble du domaine de la sécurité nationale.

Il est ici question de la définition même de sécurité nationale. J'espère et je crois que vous utilisez une définition assez large, mais, selon moi, c'est tout ce qui a une incidence importante sur la souveraineté d'un État. Les choses dont le Comité parle en ce moment sont susceptibles d'avoir une incidence importante sur la souveraineté d'un État, tout comme les activités de blanchiment d'argent réalisées par un État étranger ou un enjeu de sécurité nationale dévastateur. C'était simplement un petit effort de promotion de ma part.

Même si je ne suis pas un expert des systèmes financiers, j'espère et je crois pouvoir vous fournir deux ou trois éléments contextuels utiles. Le premier, c'est que le contexte ou l'environnement dans lesquels les cyberattaques se produisent — qu'elles soient dirigées contre des institutions financières ou autres — sont importants. Ces événements ne se produisent pas de façon isolée. Selon moi, on ne peut pas composer avec les cybermenaces dans le secteur financier sans une compréhension des cybermenaces en général, et on ne peut pas comprendre les cybermenaces sans comprendre les menaces qui pèsent généralement contre le Canada et l'Occident. Nous vivons tous dans un monde planétaire, et c'est assurément une caractéristique qui s'applique aux menaces à la sécurité nationale.

Je le dis pour deux ou trois raisons. Certains d'entre vous sont peut-être assez vieux pour vous rappeler la Guerre froide, lorsque les choses étaient assez simples: ceux qui causaient des problèmes et ceux qui en étaient victimes étaient essentiellement des États. Je simplifie les choses à outrance, mais c'était le Pacte de Varsovie contre l'Occident. Certaines entreprises étaient touchées.

Selon moi, l'un des éléments contextuels qui sont importants, c'est que, de nos jours, nos adversaires ou les instigateurs sont des États, des groupes terroristes, des organisations criminelles — et, ce sur quoi je vais revenir — des sociétés, des groupes de la société civile et des particuliers. Je crois que n'importe lequel de ces acteurs pourrait créer des problèmes au sein des systèmes financiers qui vous préoccupent.

Par ailleurs, avant, les cibles étaient essentiellement des États. Je dirais qu'il s'agit maintenant d'États, de sociétés, d'acteurs de la société civile, de partis politiques, d'organisations sans but lucratif et de particuliers. Le monde est assez complexe, et si les institutions financières en tant que telles ou le gouvernement veulent s'attaquer aux cyberattaques dont ils sont victimes, à mon avis, ils doivent connaître et comprendre le contexte dans lequel tout ça se produit. Ils ne peuvent pas bâtir des murs de façon abstraite.

Selon moi, la question de savoir qui ou quoi pourrait lancer des cyberattaques contre le secteur financier est très pertinente. Je n'essaie pas vraiment de trouver des phrases chocs, mais en voici une: la sécurité nationale n'est pas nationale. Elle n'est pas nationale au sens où un seul État ne peut pas régler ces problèmes — assurément pas une puissance relativement petite ou intermédiaire comme le Canada —, et une coopération internationale est nécessaire.

Ensuite, je ferais valoir qu'aucun État national ou État nation ne peut composer avec ces genres de choses sans l'aide des gouvernements provinciaux ou régionaux, des entreprises et de la société en général. Je vous dirais que c'est une grande erreur pour les institutions financières d'affirmer qu'elles peuvent le faire seules, tout comme c'est une erreur pour le gouvernement d'accepter une telle hypothèse.

J'ai parlé rapidement du contexte et de l'environnement, alors j'aimerais tout simplement décrire rapidement les types de menaces à la sécurité nationale auxquelles le Canada est confronté. Les États révisionnistes, la Russie et la Chine, les extrémistes et l'extrémisme de façon générale, y compris les terroristes, l'enjeu cybernétique, l'Occident dysfonctionnel et les États voyous — comme l'Iran et la Corée du Nord — et les enjeux connexes, me viennent à l'esprit.

Je vous dis tout ça parce que, selon moi, tous ces éléments sont interreliés, et ce, beaucoup plus qu'ils ne l'étaient il y a 15 ou 20 ans. Ils s'appuient les uns sur les autres pour amplifier leurs effets. Par exemple, la Russie et la Chine utilisent des cybersystèmes et bénéficient d'un Occident dysfonctionnel, parce qu'on ne lutte pas contre eux de façon coordonnée. Les groupes terroristes bénéficient de la discorde provoquée par les États révisionnistes, et ils utilisent des cybersystèmes. Tous ces éléments interagissent les uns avec les autres, et je crois que c'est quelque chose que nous devons garder à l'esprit lorsque nous abordons cette question.

● (1535)

Un des autres enjeux que je veux souligner et une des autres choses que je veux vous faire comprendre, c'est que le Canada est très menacé par les cyberattaques de façon générale ainsi que les cyberattaques contre ses institutions financières. Je le dis parce que, lorsque je travaillais, l'une des choses qui me dérangeaient, c'était l'idée qu'avaient bon nombre de Canadiens que le Canada n'était pas menacé parce que nous étions bordés par trois océans et les États-Unis. Cette vision des choses faisait en sorte qu'il était très difficile pour les gouvernements et d'autres intervenants de composer avec bon nombre des menaces à la sécurité nationale. Le Canadien moyen, ne voyant rien se passer, ne croyait pas qu'il y avait là un grave problème.

Je crois que le Canada est très menacé par une diversité d'institutions et d'entités dont je viens de parler, mais pourquoi? Nous avons une économie de pointe, un milieu scientifique et des technologies de pointe, nous faisons partie du Groupe des cinq et de l'OTAN et nous sommes tout juste à côté des États-Unis.

Pour être honnête, nous ne sommes pas considérés à l'échelle internationale comme ayant la meilleure défense cybernétique, et toute institution s'attaquera au maillon le plus faible de la chaîne. Parfois, c'est ainsi qu'on nous voit, même si je ne crois pas que nos résultats sont si mauvais que ça. De plus, nous sommes menacés, parfois, simplement parce que nous sommes victimes d'une attaque aléatoire.

Je crois qu'il est tout particulièrement important pour le Comité de souligner le fait que notre secteur financier est en effet menacé par des cyberattaques, parce que je ne crois pas que beaucoup de personnes le croient.

L'une des autres choses dont j'aimerais parler, c'est l'identité des principaux instigateurs des attaques potentielles. Je crois que ce sont des États nations et des groupes criminels internationaux.

Que vont-ils faire? Ils vont essayer d'empêcher les gens d'avoir accès aux services, s'en tirer avec des vols traditionnels — ce sur quoi je reviendrai —, ils tenteront d'acquérir de l'information et du renseignement, ils voleront de la propriété intellectuelle et des identités, tant afin de s'enrichir qu'à des fins d'espionnage.

Permettez-moi de vous donner deux ou trois exemples d'États qui jouent avec les systèmes financiers d'autres pays.

La Corée du Nord finance beaucoup de ses activités. Elle obtient beaucoup de ses devises fortes en utilisant ses capacités cybernétiques pour avoir accès aux systèmes financiers de pays divers et variés. Par exemple, elle avait un programme il y a un certain temps qui lui permettait de voler de l'argent systématiquement dans les guichets automatiques de partout dans le monde. Elle mise aussi sur un programme qui lui permet d'obtenir des rançons au moyen de rançongiciels. De façon plus générale, on croit que c'est elle qui a gelé le système de santé national du Royaume-Uni il y a quelques années.

Là où je veux en venir, c'est que vous pouvez apprendre tout ça en faisant simplement des recherches sur Google. Les États-Unis ont formellement accusé un certain nombre de personnes de la Corée du Nord qui ont tenté de faire ce genre de choses, et ce n'est là qu'un exemple d'un État qui tente de pénétrer dans les systèmes financiers des pays occidentaux.

L'Iran en est un autre. Vous aurez vu dans les journaux au cours des cinq ou dix dernières années deux ou trois exemples de la façon dont l'Iran a essayé de le faire, particulièrement contre les États-Unis et les banques. Il y a des accusations formelles qui pèsent contre sept ou huit Iraniens.

Je veux dire deux ou trois choses sur la Russie et la Chine et la façon dont, selon moi, vous ne pouvez pas en faire fi lorsque vous abordez ce sujet. Je crois que leur principal objectif est double: le premier, c'est d'empêcher la prestation des services, et l'autre, c'est simplement de réduire la confiance des Occidentaux à l'égard de leurs institutions. C'est quelque chose que ces pays font de façon systématique.

Les groupes criminels sont de plus en plus présents dans le domaine, et c'est quelque chose dont on ne parle pas assez. J'espère que vous avez eu l'occasion de parler à des représentants de la GRC à ce sujet. Si vous regardez les chiffres de la GRC ou de Statistique Canada, la mesure dans laquelle les groupes criminels internationaux s'immiscent dans nos institutions financières a explosé au cours des dernières années.

En résumé, selon moi, les cyberattaques contre notre système financier sont un enjeu de sécurité nationale. Ces attaques doivent être considérées dans un contexte global si vous voulez les éliminer de façon efficace. Il n'y a pas de solution miracle ici. On y arrivera seulement et nous réussirons seulement à réduire le risque si tous les gouvernements, toutes les sociétés et la société civile travaillent en coopération.

Je crois que le gouvernement doit échanger plus de renseignements avec le secteur privé. C'est quelque chose que nous faisons beaucoup moins que le Royaume-Uni et les États-Unis. Vous ne pouvez pas vous attendre à ce que les sociétés privées soient des partenaires efficaces s'ils ne savent pas ce qui se passe.

Le secteur financier doit déclarer de telles attaques et violations de façon beaucoup plus systématique qu'il ne le fait actuellement.

Ces problèmes évoluent constamment, et nous devons en parler beaucoup plus que nous ne le faisons actuellement.

Merci, monsieur le président.

● (1540)

Le président: Merci, monsieur Fadden.

Monsieur Ryland, vous avez 10 minutes, s'il vous plaît.

M. Mark Ryland: Bonjour, monsieur le président, et bonjour aussi aux membres du Comité. Je m'appelle Mark Ryland. Je suis directeur de l'ingénierie de sécurité d'Amazon Web Services. Je travaille directement dans le bureau du DPSI pour le dirigeant principal de la sécurité de l'information. Merci de me donner l'occasion de discuter avec vous aujourd'hui.

J'imagine que, de façon générale, vous en savez tous un peu au sujet d'Amazon.com, mais permettez-moi de fournir quelques renseignements sur notre présence canadienne.

Amazon.ca sert sa clientèle canadienne depuis 2002, et nous maintenons une présence physique au pays depuis 2010. Amazon emploie maintenant plus de 10 000 employés à temps plein au Canada, et, en 2018, nous avons annoncé la création de 6 300 emplois supplémentaires. Nous possédons deux carrefours technologiques, qui sont d'importants centres de développement de logiciels ayant de multiples bureaux à Vancouver et Toronto. Nous employons des centaines de concepteurs de logiciels et d'ingénieurs qui travaillent sur certains des projets les plus avancés pour nos plateformes mondiales. Nous avons aussi des bureaux à Victoria associés à AbeBooks.com ainsi qu'à Vancouver, où se trouve une division appelée Thinkbox.

Nous exploitons aussi sept centres de traitement des commandes au Canada, quatre dans la région du Grand Toronto, deux à Vancouver et un à Calgary. Quatre autres ont été annoncés. Ils ouvriront leurs portes en 2019, à Edmonton et Ottawa.

Mais pourquoi suis-je ici? En quoi consiste l'infonuagique? Vous vous demandez peut-être pourquoi nous sommes ici pour discuter de la cybersécurité du secteur financier. Eh bien, revenons en arrière. Il y a environ 12 ans, nous avons créé une division au sein de notre entreprise: Amazon Web Services, ou AWS par souci de brièveté.

Les AWS ont été créés lorsque l'entreprise s'est rendu compte qu'elle avait acquis une compétence de base en matière d'exploitation de très grandes infrastructures technologiques et de grands centres de données. Grâce à cette compétence, nous nous sommes donné comme mission plus générale d'utiliser cette compréhension technologique afin de servir un tout nouveau segment de clients — des développeurs et des entreprises — en offrant un service de technologie de l'information que nos clients peuvent utiliser pour créer leurs propres applications échelonnables de pointe.

L'expression « infonuagique » renvoie à la prestation sur demande de ressources de TI sur Internet ou par l'intermédiaire de réseaux privés, des services assortis d'une tarification à l'utilisation afin que les gens payent seulement pour ce qu'ils utilisent. Plutôt que d'acheter, de posséder et d'entretenir beaucoup de pièces d'équipement de haute technologie, comme des ordinateurs, des dispositifs de stockage, des réseaux, des bases de données et ainsi de suite, il est possible de seulement appeler une interface de programmation et d'avoir accès à ces services sur demande. C'est ce qu'on appelle parfois une « informatique à la demande ». C'est similaire à la façon dont un client appuie sur un interrupteur et peut avoir de l'électricité chez lui. La société d'électricité prend soin de tout le reste.

Toute cette infrastructure est créée et bâtie. Il y a bien sûr l'équipement physique et l'infrastructure derrière tout ça, mais, du point de vue de l'utilisateur, il faut seulement appeler une interface de programmation. On communique avec une interface de programmation ou on clique sur un bouton à l'aide de la souris pour avoir accès à cette capacité, et on est ensuite facturé à l'utilisation.

Tout ça est totalement contrôlé par logiciel, ce qui signifie que tout est automatisé. C'est un point vraiment important que je vais soulever plusieurs fois, parce que la capacité d'automatiser les choses est un grand avantage lorsqu'il est question de sécurité. Plutôt que de faire des choses manuellement et d'utiliser... Croyez-moi, nous n'avons pas assez d'experts pour consigner toutes les commandes nécessaires pour tout exécuter, alors il faut avoir le bon logiciel pour assurer une automatisation.

En date d'aujourd'hui, nous fournissons des services extrêmement fiables, sécurisés et résilients à plus de 1 million de consommateurs dans 190 pays. En fait, vous pouvez considérer notre plateforme infonuagique comme une fédération de régions infonuagiques distinctes. Il y en a 20 dans le monde et 61 zones d'accessibilité. Chaque région s'appuie sur des emplacements physiques distincts pour accroître la résilience.

Montréal est l'hôte de la région canadienne des AWS, qui compte deux zones d'accessibilité. Chaque zone d'accessibilité se trouve dans une ou plusieurs régions géographiques distinctes et est assortie d'une capacité de redondance du point de vue de l'alimentation, du réseautage, de la connectivité, et ainsi de suite pour réduire au minimum les probabilités de défaillance simultanées. Grâce à cette capacité, grâce à ces emplacements physiques distincts, nos clients peuvent construire des applications extrêmement accessibles et insensibles aux défaillances. Même la défaillance de tout un centre de données n'entraîne pas nécessairement une interruption des applications de nos clients.

Les entreprises qui se tournent vers les AWS vont de grandes entreprises comme Porter Airlines, la Banque Nationale du Canada, la Bourse de Montréal, le Groupe TMX, Capital One et BlackBerry, à beaucoup d'entreprises en démarrage, comme Airbnb et Pinterest, ainsi que des entreprises comme Netflix, dont bon nombre d'entre vous ont entendu parler, et qui utilisent toutes l'infonuagique des AWS.

Nous travaillons aussi auprès de beaucoup d'organisations du secteur public du monde entier, y compris le gouvernement de l'Ontario, le ministère de la justice et le Home Office britannique, Singapour, l'Australie, les États-Unis et de nombreux autres clients du secteur public à l'échelle internationale.

Quels sont les avantages de l'infonuagique? Il y a trois avantages principaux que je veux souligner.

Le premier, c'est l'agilité et la souplesse. L'agilité permet d'acquérir rapidement des ressources, de les utiliser et de les interrompre lorsqu'on n'en a pas besoin. Cela signifie que, pour la première fois, les clients peuvent vraiment traiter les technologies de l'information d'une façon plus expérimentale, parce que les expériences sont peu coûteuses. Les gens peuvent en fait essayer des choses, et si ça ne fonctionne pas, ils ont dépensé très peu d'argent. Plutôt que d'avoir engagé d'importantes dépenses d'immobilisation assorties d'importants coûts pour acquérir des licences, il est possible de le faire selon un modèle beaucoup plus dynamique. L'expérimentation est très utile lorsqu'il est question d'innovation; c'est donc une façon d'accroître l'innovation.

● (1545)

Pour ce qui est de la souplesse, nos clients devaient souvent se doter de systèmes trop gros pour leurs besoins. Ils devaient acquérir une trop grande capacité simplement parce que, une fois par année ou une fois par mois, ils avaient besoin d'une capacité de pointe.

La plupart du temps, leurs systèmes roulaient relativement au ralenti, et il y avait beaucoup de pertes associées à un tel modèle de surapprovisionnement. Grâce à l'infonuagique, il est possible d'obtenir ce dont on a besoin. Les services sont échelonnables, et on peut accroître la capacité ou la réduire de façon dynamique en temps réel.

Un autre avantage est l'économie de coût. Ce que je viens de décrire entraîne aussi des économies de coût. On utilise seulement la capacité nécessaire à un moment donné. Il est aussi possible de transformer les dépenses d'immobilisation en dépenses de fonctionnement, ce que beaucoup de personnes trouvent utile.

En bref, nos clients peuvent maintenir des niveaux d'infrastructure très élevés à un prix qui est très difficile à atteindre lorsqu'il faut acheter et gérer sa propre infrastructure.

La troisième raison, et c'est celle sur laquelle je veux vraiment mettre l'accent dans le cadre de mon témoignage, c'est l'avantage du point de vue de la sécurité. L'infrastructure des AWS met de solides mesures de protection en place pour protéger la sécurité et la confidentialité des consommateurs. Toutes les données sont stockées dans des centres de données extrêmement sécurisés. Nous fournissons très facilement un chiffrement complet: littéralement, il suffit de cocher une case ou d'appeler une interface de programmation. Toutes les données sont chiffrées, ce qui permet de contrôler les sessions, de voir ce qui se passe et de surveiller et contrôler les accès. De plus, notre réseau mondial fournit des capacités inhérentes intégrées permettant de protéger les consommateurs des attaques informatiques par saturation et des autres attaques de type réseau.

Avant l'infonuagique, les organisations devaient passer beaucoup de temps et dépenser beaucoup d'argent pour gérer leurs propres centres de données et s'en faire au sujet de la sécurité de tout ce qui s'y trouvait, et cela signifiait qu'ils consacraient moins de temps à leur mission de base en tant que telle. Grâce à l'infonuagique, les organisations peuvent agir davantage comme des entreprises en démarrage, mettre en oeuvre leurs idées sans coûts initiaux et sans avoir à se protéger contre tous les types de menaces à la sécurité.

Avant, les organisations devaient adopter un important programme d'immobilisations ou conclure des contrats à long terme avec des fournisseurs. Vraiment, la partie la plus difficile tenait au fait que les entreprises et les organisations étaient responsables de tout le système. Les clients étaient responsables de tout, du béton aux serrures sur les portes en passant par les logiciels. Grâce à l'infonuagique, nous assumons un certain nombre de ces responsabilités.

Et qu'en est-il de la sécurité de l'infonuagique? De plus en plus, les organisations se rendent compte qu'il y a un lien entre la modernisation des TI et l'utilisation de l'infonuagique pour améliorer leur posture de sécurité. La sécurité dépend de la capacité à toujours avoir une longueur d'avance sur le contexte des menaces qui évolue rapidement et continuellement en plus d'exiger une agilité opérationnelle et l'accès aux toutes dernières technologies. Tandis qu'une bonne partie des anciennes infrastructures de bon nombre de nos clients arrivent en fin de vie ou doivent être remplacées, les organisations passent à l'infonuagique pour tirer profit de nos capacités de pointe.

Une automatisation accrue est essentielle, comme je l'ai déjà mentionné, et l'infonuagique offre le plus haut niveau d'automatisation. La possibilité d'automatisation est maximisée lorsqu'on utilise une plateforme d'infonuagique. La sécurité dans le nuage est notre priorité. En fait, nous disons que la sécurité est la tâche zéro, elle vient avant même la tâche numéro un, et les organisations de tous les secteurs vous diront de quelle façon l'infonuagique commerciale peut accroître la sécurité de leur infrastructure de TI.

Par conséquent, bon nombre d'organisations, comme des institutions financières, modernisent leur capacité d'utilisation des plateformes infonuagiques. Nous avons été conçus pour assurer la sécurité des organisations, et même pour répondre aux besoins de certaines des organisations pour qui la sécurité est la plus importante considération, comme les services financiers.

Mais il s'agit d'une responsabilité commune. Les clients restent responsables d'assurer la sécurité dans leurs environnements, mais la zone de surface, le nombre de choses dont ils doivent s'inquiéter, est grandement limité, parce que nous prenons soin de beaucoup de ces choses afin qu'ils puissent se concentrer sur le reste. Des grandes banques aux gouvernements fédéraux, nos clients nous ont répété — et nous avons des citations que nous pourrons fournir au Comité — qu'ils se sentent plus en sécurité lorsqu'ils déploient leurs applications dans le nuage que lorsqu'ils le font dans leur propre infrastructure physique, sur place, dans leur propre centre de données.

En résumé, l'infonuagique devrait être considérée non pas comme un obstacle à la sécurité, mais comme une technologie qui favorise la sécurité, et elle est parfois très utile dans le domaine des services financiers en tant que composante de la solution globale pour moderniser et améliorer la sécurité.

Nous avons aussi quelques recommandations de nature stratégique, que nous vous fournirons dans notre mémoire écrit.

L'une des choses que nous voulons mentionner, c'est que, selon nous, on met trop l'accent sur l'emplacement physique des données. Très souvent, les gens se disent: « Il faut que j'aie les données avec moi, physiquement, pour les protéger ». En fait, si on regarde les antécédents en matière de cyberincidents, tout est fait à distance. C'est lorsqu'on est connecté à un réseau assorti d'accès vers l'extérieur que le pire peut se produire.

L'emplacement physique des données, surtout lorsqu'on peut tout chiffrer, comme l'accès physique aux lecteurs de stockage ou peu importe, n'est littéralement pas un vecteur de menace. En fait, il faudrait donner une certaine marge de manoeuvre aux banques et aux autres institutions quant à l'endroit physique où leurs données sont conservées, et ces institutions devraient pouvoir réaliser leur charge de travail dans le monde entier, offrant à leurs clients mondiaux des services à faible latence et en stockant possiblement des données à l'extérieur du Canada.

Il y a deux ou trois autres recommandations, y compris la question de la résidence des données. Nous croyons aussi que la centralisation du travail d'évaluation de sécurité est tout à fait appropriée. Plutôt que de demander à chaque agence ou chaque organisme de réglementation d'évaluer séparément la sécurité de l'infonuagique, il faudrait centraliser ce travail dans une organisation comme le Centre canadien pour la cybersécurité où les responsables peuvent réaliser une évaluation centralisée et déterminer si les plateformes d'infonuagique respectent les exigences. Puis, cette autorisation d'utilisation peut servir à d'autres organisations à l'échelle du gouvernement et au sein des industries réglementées.

● (1550)

Merci beaucoup du temps que vous m'avez accordé.

Le président: Merci, monsieur Ryland.

Les sept premières minutes reviennent à M. Spengemann, s'il vous plaît.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Merci beaucoup, messieurs, d'être là.

Monsieur Fadden, je suis particulièrement heureux que vous soyez là. En ce qui concerne votre ancien rôle de conseiller à la sécurité nationale, je crois que vous avez un point de vue unique sur la façon dont le sujet est lié au ministère de la Défense nationale et aux questions liées à la défense nationale. Je veux commencer par vous poser des questions à ce sujet.

Quelles sont les intersections, les zones grises, entre ce que nous considérons comme des questions liées à la sécurité publique et les questions liées à la défense nationale? Ce sont deux comités qui ont leur propre mandat. De cette façon, il y a des cloisons, et on devrait peut-être réaliser une étude conjointe réunissant les deux comités.

Pouvez-vous formuler des commentaires généraux sur la mesure dans laquelle la composante de défense nationale joue un rôle dans une bonne cybersécurité et quelle part revient à la composante de la sécurité publique?

M. Richard Fadden: Eh bien, je suis assez d'accord avec vous: les distinctions qu'on fait dans le domaine sont un peu artificielles, et une des choses qu'il faut éviter, dans la mesure du possible, c'est de créer de telles cloisons. Nous en avons déjà assez comme c'est là, nous n'en avons pas besoin de plus.

Je crois que la principale contribution de la Défense nationale, c'est par l'intermédiaire du Centre de la sécurité et des télécommunications et, en ce qui concerne le secteur privé, le Centre pour la cybersécurité. Ces intervenants ont tendance à travailler de façon assez coopérative avec d'autres composantes de l'environnement de la sécurité nationale au Canada. Je dirais, et c'est en partie à la lumière de ce que j'ai su lorsque je travaillais, mais c'est aussi en partie parce que je travaille maintenant un peu dans le secteur privé, qu'il s'agissait assurément là de nouveautés qui ont été les bienvenues, mais ces entités n'ont pas réglé tous les problèmes des cyberattaques, ici et ailleurs.

Selon moi, l'un de leurs gros problèmes, et c'est un problème lié à la Défense, dans la mesure où c'est le ministre de la Défense qui est responsable, c'est que nous parlons de ces choses, mais nous en parlons beaucoup moins et nous partageons beaucoup moins d'information avec le secteur privé que ne le font une diversité d'autres pays. Je ne blâme pas un gouvernement ou un fonctionnaire précis. Il y a quelque chose dans l'ADN canadien lié au fait que nous estimons qu'il faut gérer la sécurité nationale, mais pas en parler. Toutefois, je dirais que, dans de nombreux cas, nous nous en tirerions beaucoup mieux si nous en parlions un peu au secteur privé, sans aller dans les détails opérationnels. C'est une façon d'accroître la sensibilisation. Cela permet au gouvernement et aux sociétés de discuter et de communiquer plus d'information qu'on en demande, mais je crois que le principal contributeur, c'est le CST.

● (1555)

M. Sven Spengemann: J'ai eu l'occasion de demander au dernier groupe de témoins quelle était la distinction — s'il y en a une — entre les acteurs étatiques et les acteurs non étatiques, leur différence qualitative en ce qui a trait à leur capacité de mettre à exécution une menace. Pouvez-vous nous en parler? Un acteur étatique a-t-il tout simplement plus de capacités, plus de pirates, plus de personnes? Ou y a-t-il d'autres différences qualitatives faisant en sorte que ces types d'acteurs sont dans des catégories complètement différentes?

M. Richard Fadden: Je crois qu'il y a des distinctions à faire entre les acteurs étatiques. Je crois que la Chine et la Russie sont dans une ligue à part. Ils consacrent des ressources quasiment illimitées à leur capacité cybernétique. Ils sont très, très bons. Selon moi, il est généralement accepté que la Chine utilise l'approche de la balayeuse. Elle prend tout simplement tout ce qu'elle peut. Les Russes, selon moi, comptent sur des technologies un peu meilleures et ils sont un peu plus chirurgicaux quant à ce qu'ils tentent d'acquérir.

Selon moi, les groupes criminels internationaux ne sont pas au même niveau, mais ils deviennent très, très bons. Ce sont des gens très intelligents qui ont découvert qu'il était plus facile de s'enrichir en utilisant des appareils cybernétiques qu'au moyen d'interventions cinétiques d'une forme ou d'une autre. En outre, il n'y a pas de frontière, et dans la mesure où il n'y a pas de frontière, c'est beaucoup plus facile.

Le dernier groupe que je mentionnerais, j'imagine, c'est les groupes terroristes. Ils sont dans une catégorie différente. Certains possèdent une capacité cybernétique limitée. Tout cela n'a pas vraiment une envergure mondiale.

J'imagine que ce que je dirais encore une fois, c'est que les acteurs étatiques en particulier font en sorte qu'il est important pour nous de voir les défenses cybernétiques comme étant en constante évolution. Je ne parle pas en particulier de l'entreprise de M. Ryland, mais, quelle que soit la mesure de protection que nous mettons en place, si on se trouve devant une entité très agressive et qu'on lui donne assez de temps et de technologies, elle trouvera une façon de les contourner. Mon point, c'est que nous devons constamment renouveler nos mesures de défense. Nous devons constamment perfectionner nos technologies, surtout contre les États nations, mais de plus en plus aussi contre les groupes criminels internationaux.

M. Sven Spengemann: Je veux vous poser une question au sujet du contenu dans le domaine numérique, tant du côté civil que du côté militaire. Facebook vient tout juste de décider d'interdire un certain nombre d'entités, des personnes qui ne respectent pas ses normes, y compris Faith Goldy, une nationaliste blanche canadienne. Nous avons aussi eu des discussions au sein du comité de la défense au sujet des campagnes de désinformation russes et du contenu délibérément faux dans la sphère sociale.

Dans quelle mesure le contenu est-il un problème? Où les tendances s'en vont-elles selon vous? Y a-t-il une tendance vers l'interdiction — entre guillemets — de contenu? Dans l'affirmative, qu'est-ce qui arrive? Repoussons-nous ce type de contenu vers le Web invisible ou réglons-nous certains problèmes?

M. Richard Fadden: Selon moi, le contenu est horrifiant, dégoûtant et exagérément terrible. Si vous preniez le temps un samedi après-midi ou un dimanche pluvieux et que vous faisiez preuve d'un peu d'imagination en vous promenant sur le Web, vous pourriez trouver du contenu d'extrême-droite qui est aussi mauvais que ce qu'écrivaient les nazis, et vous trouverez de la littérature djihadiste qui fait la promotion de la mise à mort systématique des gens. Je ne parle pas du Web profond, qui est, encore là, un autre problème. Je crois que le contenu est un réel problème.

Je dirais que ce que Facebook essaie de faire est une bonne première étape, mais je ne veux pas vraiment que Facebook devienne l'entité qui contrôle mes pensées. Par ailleurs, j'ai la même inquiétude au sujet des gouvernements. Je ne veux pas que les gouvernements se mettent à contrôler nos pensées en déterminant ce qu'il faut faire. Je crois que nous avons besoin d'une certaine discussion nationale pour déterminer qui doit s'occuper de tout cela.

L'une des façons dont le Parlement a composé avec ce problème, c'est dans le domaine du blanchiment d'argent. Vous vous rappelez peut-être qu'il y a eu un débat il y a de ça des années sur la façon de composer avec le blanchiment d'argent: fallait-il tout simplement en faire un crime? Essentiellement, ce que le Parlement a fait, c'est d'imposer une obligation aux banques de connaître leurs clients. Cela a amélioré de façon importante la capacité de tout le monde de composer avec le blanchiment d'argent. On n'a pas éliminé le problème, mais les mesures ont été bénéfiques.

Selon moi, il serait possible pour le gouvernement de mettre en place un cadre, législatif ou réglementaire, exigeant que les entreprises qui oeuvrent dans ce large domaine sachent à qui elles donnent accès au Web et les informent de ce qui est permis et de ce qui est interdit.

En raison de mon grand âge et après 40 ans au sein du gouvernement, j'hésite un peu à laisser des gens me dire ce que je dois penser, que ce soit le gouvernement ou le secteur privé; je crois qu'il doit y avoir une mesure de transparence afin que nous sachions à la fois ce qu'on fait et ce qu'on ne fait pas.

Cependant, rien de tout cela ne fonctionnera, selon moi, si le Canadien moyen ne sait pas plus ce qui est accessible et s'il n'a pas des moyens quelconques de faire connaître ce qui le dérange. Actuellement, oui, on peut appeler la Gendarmerie, mais elle s'occupe de tellement de choses que ce n'est vraiment pas l'une de ses priorités.

M. Sven Spengemann: Merci beaucoup. C'est très utile.

Le président: Merci, monsieur Spengemann.

[*Français*]

Monsieur Paul-Hus, vous avez sept minutes, s'il vous plaît.

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

Bonjour, messieurs.

Monsieur Fadden, en 2010, vous avez donné une entrevue à CBC qui a été rapportée dans le *Globe and Mail*. Vous mentionniez qu'il y avait de l'ingérence d'acteurs d'autres États auprès de fonctionnaires et de ministres provinciaux ainsi que dans les milieux politiques canadiens. À ce moment-là, des gens du NPD et du Parti libéral ont demandé votre démission. Heureusement, vous êtes resté en poste.

Ce matin, nous avons appris que le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement, qui vient d'être déposé, confirme ce que vous avez dit et confirme très clairement que la Chine est un acteur dangereux pour la sécurité du Canada.

Dans votre présentation, vous avez parlé des problèmes, mais j'aimerais aussi connaître les pistes de solution. Vous avez parlé de « l'Occident dysfonctionnel ». C'est ce que j'ai entendu à l'interprétation. Pourriez-vous nous éclairer davantage quant à ce que nous pourrions faire? Qu'est-ce que cela veut dire?

● (1600)

[*Traduction*]

M. Richard Fadden: Oui. Lorsque je parle de l'Occident qui est dysfonctionnel, je veux dire que... Je suis sûr que vous ne voulez pas avoir une longue discussion sur l'administration américaine actuelle, mais c'est là un problème important à l'heure actuelle dans la mesure où les points de vue du président américain actuel favorisent une grande instabilité. Les gens ne savent pas exactement ce qui se passe. Le Royaume-Uni n'a pas pris de décision majeure en un an et demi. M. Macron est préoccupé par ce qui se passe avec les gilets jaunes. L'Allemagne est préoccupée par le remplacement de Mme Merkel, et qui sait ce que font les Italiens.

Ce que j'essaie de dire, c'est que, tandis que nous nous inquiétons de ces enjeux majeurs, nous donnons l'occasion à la Russie et à la Chine en particulier de mettre leur nez dans nos affaires d'une façon qu'ils ne pourraient pas le faire si nous étions un peu plus unis. Je ne dis pas que le monde tire à sa fin. Ce n'est vraiment pas ce que je dis, mais je crois que nos adversaires — et je les appelle des adversaires, pas des ennemis — sont très actifs. Ils profitent de chaque occasion. Je crois que nous devons commencer à rétablir les liens étroits qu'il y avait entre certains pays depuis la Deuxième Guerre mondiale.

Selon moi, il faut aussi nous rendre encore plus compte que nous ne le faisons actuellement — et c'est l'un des moyens dont, selon moi, nous devons parler — et mieux comprendre aussi que la Russie et la Chine sont, à leur façon, de grands pays. Ces pays ont beaucoup contribué à la civilisation. Cependant, pour l'heure, ils sont foncièrement mécontents de leur position sur la planète et ils tenteront de changer la donne en utilisant quasiment n'importe quelle méthode. Selon moi, on n'y pense pas assez. Si on n'y pense pas et qu'on n'essaie pas de faire quoi que ce soit à ce sujet, nous sommes vraiment à la traîne.

Selon moi, la première chose à faire, c'est de mieux comprendre ce qui se passe. Quelqu'un m'a demandé l'autre jour dans les médias pourquoi la Russie est allée en Syrie. Elle n'a aucune possibilité d'acquérir des territoires, mais elle tente de causer du tort, et elle réussit très bien. Elle a retardé l'élimination du califat. Elle fait ce genre de choses dans un paquet de domaines. Elle est intervenue dans les élections des États-Unis, de l'Allemagne, de la France et si je ne m'abuse, de l'Italie. Tout ce qu'elle tente de faire, ce n'est pas vraiment de choisir qui gagnera, mais de réduire la confiance du public à l'égard des institutions publiques.

Ce sont toutes des choses dont, selon moi, nous devons parler davantage. Nous devons vraiment bien comprendre, particulièrement au sein des principaux pays occidentaux, la gravité du problème. Certaines parties de l'administration américaine jugent que tout cela est plus important que nous, parfois. Les Britanniques sont à un tout autre niveau. Nous avons besoin d'un consensus au sein de l'Occident quant au fait qu'il y a un problème. Les États-Unis viennent de changer leurs priorités en matière de sécurité nationale pour remettre l'accent sur les conflits entre grandes puissances après s'être intéressés au terrorisme pendant de nombreuses années. Eh bien, si c'est le cas, il faut commencer à réfléchir à ce qu'on fera au sujet de la Russie et de la Chine, sans partir en guerre, ce qui n'est vraiment pas ce que je propose. Il faut en parler, comprendre la nature de la menace et tisser des liens plus étroits à l'échelle internationale. Je crois vraiment que la sécurité nationale n'est pas nationale, pas de la façon dont on l'assure aujourd'hui. Il faut travailler en collaboration avec tout le monde.

[*Français*]

M. Pierre Paul-Hus: Merci.

Revenons à notre sujet de base, qui est le secteur financier, les banques.

Nous avons rencontré plusieurs intervenants, différentes banques et différents autres groupes. Il y a les banques, le système administratif gouvernemental et le côté politique. Lorsqu'il est question de sécurité, d'enjeux, d'ennemis potentiels, le côté politique est toujours frileux. Les banques prennent des mesures de leur côté.

Selon vous, est-ce que l'administration, c'est-à-dire les gens que nous ne voyons pas, ceux qui sont dans l'ombre, est assez efficace actuellement pour pallier le côté politique? Il peut s'agir d'un côté ou de l'autre, je parle de façon générale. Politiquement, parfois, on n'ose pas.

À la suite des années que vous avez passées au sein de l'appareil politique, pensez-vous que nous sommes efficaces ou qu'il y aurait lieu de prendre des mesures très vigoureuses?

[*Traduction*]

M. Richard Fadden: Je dois admettre d'entrée de jeu que je ne suis probablement pas objectif, puisque j'ai travaillé pendant beaucoup d'années dans le domaine, mais je crois qu'il y a eu beaucoup de progrès ces derniers temps et qu'il y a beaucoup plus de coopération et de collaboration.

Cependant, je dirais deux choses. Premièrement, c'est que le monde devient beaucoup, beaucoup plus complexe, et je crois qu'on pourrait dire qu'il faut plus de ressources. Lorsque je travaillais pour le gouvernement, la dernière chose que nous voulions faire, c'était de mettre notre ministre dans l'embarras en disant que nous voulions plus d'argent. Ce n'est pas vraiment ce que je dis maintenant, mais si on pense à la guerre froide, puis au terrorisme, et enfin aux enjeux cybernétiques actuels et aux conflits entre grandes puissances de façon générale, oui, toutes ces institutions ont déjà eu plus de ressources, mais ces niveaux de ressources ne sont peut-être plus suffisants de nos jours, alors c'est quelque chose que je demanderais.

J'imagine que l'autre enjeu que je soulèverais est le suivant: plusieurs politiciens des deux côtés m'ont dit au fil des ans que parler de sécurité nationale ne fait pas gagner beaucoup de votes, et que c'est une des raisons pour lesquelles le gouvernement hésite parfois à prendre les mesures que vous avez soulevées. Cependant, si contrariés que soient les politiciens par les fonctionnaires, ce sont les fonctionnaires qui prennent les devants du point de vue politique des choses, et je crois que nous devons être un peu plus proactifs parfois que nous ne le sommes, parce que la technologie avance, la menace change, et nous semblons toujours essayer de rattraper le retard.

Je ne vise aucun gouvernement ni aucun fonctionnaire. Cela semble tout simplement être la façon dont on fait les choses, en grande partie parce que, si vous êtes le ministre des Finances ou le président du Conseil du Trésor, la dernière chose que vous voulez faire, tous les deux ans, c'est de dire: « voici encore 250 millions de dollars ». Je dis un montant comme ça, mais, vous savez, il y a des changements technologiques, et M. Ryland a parlé de certains d'entre eux, et il y en a un paquet d'autres. C'est très difficile pour un gouvernement de maintenir le rythme sans déployer constamment des efforts, et, en même temps, on s'inquiète au sujet de la Russie, de la Chine, de la Corée du Nord et de l'Iran. On s'inquiète au sujet des groupes criminels internationaux. J'ai l'impression qu'on commence à sous-estimer le problème que posent les terroristes tout simplement parce que nous en avons épinglé quelques-uns.

Par conséquent, et c'est une longue réponse à une question courte: je crois que, de façon générale, les gens font tout ce qu'ils peuvent, mais c'est très difficile de mobiliser tous ceux qui travaillent sur ce dossier — les fonctionnaires et le secteur privé —, sauf s'il y a un consensus quelconque quant à la gravité de la menace.

Je dirais, en toute déférence, que ce genre de consensus brille par son absence au Canada.

● (1605)

Le président: Merci, monsieur Paul-Hus.

Monsieur Dubé, allez-y pour sept minutes, s'il vous plaît.

[*Français*]

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

Messieurs, merci d'être ici aujourd'hui.

Monsieur Ryland, ma première question est pour vous. En ce qui concerne vos services, je ne sais pas si vous êtes en mesure de nous expliquer la séparation des responsabilités entre vous et vos clients.

Quel est le rôle de vos clients pour assurer la sûreté des données qu'ils vont stocker sur vos serveurs en utilisant vos services?

[*Traduction*]

M. Mark Ryland: Cette conversation peut être très longue et nuancée, mais juste pour vous donner un genre de résumé, si vous regardez quelque chose comme ce qu'ont les États-Unis... Il y a un cadre de contrôle de sécurité fondé sur une norme NIST appelée FedRAMP, qui dresse la liste de quelque 250 mesures de contrôle — autrement dit, les caractéristiques de sécurité que vous recherchez dans un système — et si vous prenez tout ce cadre de sécurité, notre plateforme couvre plus du tiers de ces mesures de contrôle. Ce sont simplement des choses dont nous nous occupons littéralement au nom de nos clients. Ils n'ont pas du tout besoin de s'en préoccuper. À peu près le tiers est partagé, de manière à ce que nous puissions nous occuper de certaines des choses, mais le client doit effectuer certaines configurations et faire certains choix qui fonctionnent pour ses besoins. Ces mesures de contrôle sont optionnelles, parce qu'il est raisonnable de choisir une option ou une autre, mais selon les besoins des clients, ils doivent faire un choix. Puis, environ le tiers est essentiellement la responsabilité du client.

Nous avons donc rétréci le champ d'action pour le client. Nous délimitons assez clairement qui est responsable de quoi et détenons littéralement des documents de contrôle à ce sujet, puis nous disposons de beaucoup de matériel — des livres blancs, des documents sur les pratiques exemplaires et ce que nous appelons un « cadre bien conçu » — afin d'aider les gens à assumer cette responsabilité restante. Nous voulons qu'ils y parviennent haut la main et nous déployons donc beaucoup d'efforts pour les aider à concevoir des systèmes sécurisés.

Mais lorsque vous arrivez à ce niveau, tout dépend des besoins de l'application, et il n'y a donc pas de bonne réponse à certaines questions. On vous dira « ça dépend ». Ça dépend de l'application et du besoin.

En général, je crois que c'est un bon résumé du type de modèle que nous utilisons avec nos clients. Nous nous occupons d'un certain nombre de choses qui les préoccuperaient habituellement; nous décrivons quelques domaines dans lesquels nous faisons certaines choses et où ils doivent en faire d'autres, puis nous les aidons avec le reste de la conception d'un système sécurisé en leur fournissant beaucoup d'outils et de caractéristiques qui font en sorte qu'il est plus facile de l'achever.

[*Français*]

M. Matthew Dubé: Merci.

Je veux m'assurer de bien comprendre. Vous avez dit qu'environ un tiers de la responsabilité à bien configurer le tout relevait uniquement du client. Est-ce que cela crée une barrière pour les personnes ou, notamment, les entreprises qui peuvent accéder à vos services, c'est-à-dire que l'expertise doit déjà exister au sein de l'entreprise ou de l'agence gouvernementale?

Je m'explique. Voici l'exemple qui me vient en tête. Je crois que Services partagés Canada a un contrat avec vous. Toutefois, selon ce qu'on voit dans l'actualité depuis un certain temps, cet organisme un bilan assez lamentable en ce qui a trait à la mise en œuvre de système informatique.

Est-ce que les lacunes qui peuvent exister ou le manque d'expertise au sein d'une l'entreprise ou d'une agence gouvernementale pourraient limiter la capacité d'un client de faire affaire avec vous ou avec toute autre entreprise comparable à la vôtre?

● (1610)

[*Traduction*]

M. Mark Ryland: Chaque fois qu'on utilise une technologie, c'est certainement possible de ne pas bien s'en servir. Une bonne partie de notre mission consiste à renseigner et à former nos clients, et c'est ce que nous faisons dans bien des cas. Et une bonne partie de cette formation est en fait gratuite, dans le contexte où on les aide à comprendre ce type de nouveau paradigme qu'est l'infonuagique.

Cela dit, il y a beaucoup de points communs avec des choses qu'ils font déjà depuis un certain temps. Je vais vous donner juste un exemple. Disons que vous dirigez une application Web accessible aux citoyens pour un gouvernement. Vous savez déjà en quelque sorte comment sécuriser un réseau central; vous détenez un système d'authentification, faites une réinitialisation du mot de passe, ces types de caractéristiques qui sont intégrées dans le système. Si vous utilisez ce type de système semblable sur une plateforme infonuagique, les caractéristiques de sécurité s'apparenteraient à celles que vous avez utilisées par le passé.

Ce n'est pas un monde complètement nouveau. Il ne s'agit pas d'un ensemble de compétences entièrement nouvelles qui sont requises pour les professionnels de la sécurité, mais il y a assurément des différences et des changements. Cela fait partie des progrès de l'industrie, tout comme il y a 20 ou 30 ans, quand nous avons beaucoup travaillé sur l'ordinateur central. Ce n'est pas quelque chose sur quoi les gens se concentrent maintenant. Il y a toujours des systèmes centraux qui fonctionnent, et ils doivent être sécurisés, mais l'on a tendance à se concentrer sur les nouvelles choses, les nouveaux systèmes et les nouvelles applications.

Je crois que la transition vers l'infonuagique comporte une caractéristique semblable. Chaque fois qu'il est question de modernisation et d'utilisation de nouvelles technologies, il y a assurément une certaine courbe d'apprentissage, mais vous pouvez aussi en faire beaucoup plus en travaillant moins, avec moins d'êtres humains réels. Parfois, quand on se sert de l'automatisation, d'aucuns jugent que c'est controversé, parce qu'on se dit, eh bien, qu'arrive-t-il si nous retirons des gens? Allons-nous enlever des emplois à des travailleurs? Dans le domaine de la cybersécurité, tout le monde reconnaît que nous avons une énorme pénurie de main-d'oeuvre qualifiée. Tout type de technologie qui peut accroître l'automatisation et permettre à un travailleur qualifié de trouver une solution, puis de la reproduire à grande échelle, représente un gain énorme, et tout le monde peut donc appuyer une plus grande automatisation dans le domaine de la sécurité.

Je crois que c'est une des principales raisons pour lesquelles les gens estiment que les plateformes infonuagiques sont avantageuses. Oui, il y a une courbe d'apprentissage, mais la capacité d'automatiser des choses est vraiment grandement supérieure à l'utilisation de la technologie traditionnelle.

[*Français*]

M. Matthew Dubé: J'ai deux dernières questions à poser rapidement.

Voici la première. Vous n'êtes peut-être pas le mieux placé dans votre organisation pour y répondre. Toutefois, advenant le cas où il y aurait une fuite de données, étant donné qu'il y a une responsabilité partagée, qui serait ultimement responsable des données, légalement? En particulier dans le secteur financier, si un client perdait de l'argent, serait-ce la faute de la banque ou de l'entreprise qui permet l'entreposage de données dans le nuage?

Comment voyez-vous cela?

[*Traduction*]

Le président: Veuillez faire très vite, s'il vous plaît.

M. Mark Ryland: Oui.

La responsabilité partagée suppose aussi qu'on détermine qui assume cette responsabilité. Si un problème devait apparaître dans un de nos systèmes, nous en serions responsables. Si un client configure ou utilise mal un de nos systèmes, il en est responsable.

Encore une fois, nous faisons beaucoup de choses pour soutenir les clients, et il arrive souvent, dans l'équipe de sécurité où je travaille, que des clients soient en proie à un problème et à un certain type d'incident et viennent nous demander de l'aide. Même si, techniquement, ce n'est pas du tout notre faute, nous répondons tout de même avec grand dynamisme pour les aider à résoudre les problèmes qu'ils ont causés.

Je vais prendre un exemple simple et non controversé. Nous détenons des systèmes où des clients ont accidentellement supprimé des données sans faire les sauvegardes appropriées, et ils viennent nous voir en panique. D'un côté, nous pourrions dire: « Eh bien, le système fonctionnait exactement tel qu'il a été conçu. Vous avez fait une erreur. Nous ne pouvons rien faire. » Pourtant, nous nous donnerons beaucoup de mal pour les aider à trouver des solutions à ces types de problèmes, et il en va de même avec les incidents de sécurité.

● (1615)

Le président: Merci, monsieur Dubé. Je suis désolé.

Monsieur Graham, vous avez sept minutes, s'il vous plaît.

M. David de Burgh Graham: Merci.

J'aimerais beaucoup poursuivre sur ce sujet, mais j'y reviendrai dans une seconde.

Monsieur Fadden, je ne crois pas que quiconque désapprouvera votre évaluation selon laquelle notre étude concerne vraiment la sécurité nationale, plutôt que la cybersécurité dans le secteur financier comme question primordiale.

Je dirais que beaucoup de questions sont mises aux voix au chapitre de la sécurité nationale, mais seulement une fois que l'incident s'est produit.

M. Richard Fadden: J'en prends bonne note. Je vous remercie.

M. David de Burgh Graham: Vous avez dit que la sécurité n'est pas nationale; qu'elle est supernationale. Le Canada a-t-il un réseau de base assez fort pour répondre aux besoins des Canadiens? Avons-nous des liens intercontinentaux suffisants pour répondre aux besoins des Canadiens, et est-ce important?

M. Richard Fadden: Je crois que c'est très important.

Avons-nous le réseau de base ou les liens intercontinentaux? Il est difficile de répondre à cette question, car je crois qu'elle suppose une réponse en deux parties: une qui concerne les gouvernements de façon générale, et l'autre, le secteur non gouvernemental.

À mon avis, en ce qui concerne les gouvernements, nous avons des alliances très étroites avec le Groupe des cinq — les États-Unis en particulier — et l'échange de renseignements est énorme. Je dirais que c'est assez efficace, nonobstant le dysfonctionnement dont je parlais.

Quand je travaillais encore, l'approche qui avait été adoptée pour régler certains de ces problèmes... C'est un peu comme parler d'un cancer. Ce n'est pas particulièrement utile. J'ai remarqué que certains d'entre vous portent leur épinglette contre le cancer. Le fait de parler de façon générale au sujet du cancer n'est pas particulièrement utile, parce que le remède contre le cancer concerne les quelque 130 types de cancer. Je trouve que le fait de parler de façon générale de la cybernétique n'est souvent pas très utile. Vous devez la décomposer et vous attacher à ses parties constituantes.

Auparavant, nous divisions l'économie canadienne en secteurs stratégiques, comme les télécommunications, les finances, l'énergie nucléaire... Il y en avait 11 ou 12. Bien honnêtement, je crois que les liens qu'ils entretiennent avec leur établissement principal — l'un avec l'autre au Canada et à l'étranger — varient. Par exemple, notre secteur nucléaire est assez bien organisé, et je crois que le point de vue général, en ce qui concerne les secteurs, c'est que le secteur financier ne se porte pas mal. C'est moins le cas de certains des autres secteurs.

Je n'essaie pas d'éluder votre question, mais je crois qu'il est difficile de juste vous répondre par oui ou non. Je crois qu'il n'y a pas une seule entité — gouvernementale ou non gouvernementale — qui est responsable. C'est juste ainsi que les choses ont évolué.

M. David de Burgh Graham: Je vais demander à M. Ryland de nous fournir plus de précisions.

Vous avez parlé du modèle de surapprovisionnement. Vous parliez des vastes ressources et de la capacité de les répartir entre les systèmes, ce que nous n'aurions pas pu faire auparavant. En guise d'exemple, quelle est la puissance de calcul d'un porte-clé aujourd'hui par rapport à celle d'Apollo?

M. Mark Ryland: La puissance du porte-clé est probablement plus grande. C'est un microcontrôleur de 32 bits.

M. David de Burgh Graham: Lorsque survient ce type de changement massif dans la capacité de calcul, quelle incidence a-t-il sur la sécurité? La technologie change-t-elle à un rythme plus rapide que ce que nous pouvons soutenir?

M. Mark Ryland: Non, je ne le crois pas.

La technologie change rapidement, mais des gens motivent ces changements technologiques. En général, les experts qui conçoivent les systèmes comprennent leur fonctionnement et la façon de les sécuriser. Il peut y avoir un temps mort avant que l'on comprenne de façon élargie ces technologies de pointe, mais souvent, ces experts conçoivent aussi des choses afin de les sécuriser davantage par défaut.

Je crois que l'Internet des objets est un excellent exemple. Nous n'avons pas le temps d'en parler en détail, mais nous avons tous reconnu dans le passé les problèmes avec l'IdO — les appareils domestiques, etc. — qui était déployé de façon très peu sécuritaire. Par le passé, c'était la chose la moins coûteuse et la plus facile à faire. Si vous examinez la technologie récente que nous offrons, ou celle que Microsoft ou d'autres gros fournisseurs vous offrent, par défaut, leurs systèmes sont beaucoup plus sécuritaires. Vous pouvez les mettre à jour par substitution, ce qu'il n'était pas possible de faire auparavant. Ils utilisent des protocoles sécurisés par défaut; ils ne le faisaient pas auparavant. Vous pouvez aller directement au bas de la liste pour savoir comment les intérêts commerciaux de ces gros fournisseurs s'harmonisent avec la conception de systèmes qui sont sécurisés par défaut, tandis que, auparavant, cette fonction revenait à la personne qui concevait le réfrigérateur intelligent, le grille-pain intelligent ou quoi que ce soit d'autre.

Les changements technologiques peuvent en fait relever la barre dans des industries entières au moyen d'investissements et de l'harmonisation des intérêts commerciaux avec une sécurité supérieure.

M. David de Burgh Graham: Je vais revenir à l'infonuagique. Le public ou même les organisations avec qui vous traitez comprennent-ils réellement ce qu'est le nuage?

M. Mark Ryland: Il y a souvent beaucoup de confusion. D'abord, il y a cette idée qui consiste à savoir ce qui existe. Les gens croient qu'il doit y avoir quelque chose qui existe. Il y a aussi la confusion qui apparaît entre les cas d'utilisation des clients. Les gens croient que Facebook et Google sont comme un nuage, mais la prestation de services de TI d'un fournisseur de services d'infonuagique est un modèle tout à fait différent. Tout d'abord, nous ne monétisons pas vos données; nous les verrouillons et ne les examinons jamais. Notre perception est totalement différente.

Une chose qu'ils ont généralement en commun, c'est l'accessibilité aux réseaux. On sera en mesure d'y accéder de n'importe où.

Il y a beaucoup de confusion. Souvent, au début de nos exposés, nous afficherons une mappemonde, où figurent de petits points qui montrent où se trouvent nos choses dans cette ville ou cette région, afin que les gens puissent savoir que de l'équipement physique sous-tend toute cette capacité.

● (1620)

M. David de Burgh Graham: Les AWS consistent-ils essentiellement en des serveurs virtuels ou y a-t-il un autre système à part celui-là? Y a-t-il des machines virtuelles?

M. Mark Ryland: C'est un de nos services principaux. Ça s'appelle EC2, mais nous possédons littéralement une centaine d'autres services. La tendance s'éloigne déjà de l'utilisation de services de machines virtuelles, car c'est là que le client doit assumer la plus grande responsabilité. Les gens préféreraient utiliser les services de niveau supérieur où nous assumons une responsabilité accrue et où ils n'ont qu'à effectuer une configuration très minime.

M. David de Burgh Graham: Si vous utilisez non pas une machine virtuelle, mais plutôt les services fournis, quel contrôle un client peut-il réellement détenir? On doit trouver un juste milieu. En tant que client, serais-je en mesure de choisir le système d'exploitation de ma machine virtuelle? Je pourrais mettre un système Debian, ou quoi que ce soit d'autre, mais que pourriez-vous mettre sur une machine qui n'est pas virtuelle? Quelles sont les autres options?

M. Mark Ryland: Encore une fois, cela dépend du cas d'utilisation. Le modèle informatique associé à un service de stockage vous importe peu, puisque vous ne faites que stocker des données. Les bases de données se trouvent au milieu. Il y a une panoplie de choix et d'options, mais les gens ont tendance à préférer ce qu'on appelle les « services virtuels ». Au fil du temps, vous verrez que les gens adoptent de plus en plus ces services virtuels. Je n'ai qu'à téléverser ma fonction de JavaScript sur cette fonction comme service, et le code s'exécute dès que certains événements surviennent. Je n'ai aucune notion du système d'exploitation ni de quoi que ce soit d'autre; c'est géré pour moi.

M. David de Burgh Graham: Il ne me reste que 40 secondes environ, donc ma dernière question pour vous deux concerne les avantages par rapport aux désavantages en matière de sécurité des logiciels ouverts et des logiciels exclusifs.

M. Mark Ryland: Il y a quelque chose qui s'appelle l'hypothèse des « yeux multiples » pour les logiciels ouverts. Le fait que les gens peuvent voir le code fait en sorte qu'il est plus probable que l'on découvre des défauts de sécurité et d'autres failles. Je ne sais pas s'il y a des données empiriques vraiment solides qui l'appuient, car beaucoup de défauts de sécurité ont été retrouvés dans le code ouvert, mais le grand avantage, c'est que les gens ont plus de contrôle sur leur propre destin, parce que vous pouvez mener votre propre enquête. Vous pouvez trouver vos solutions. Vous ne dépendez pas d'un fournisseur pour découvrir et régler des problèmes de sécurité. Dans l'ensemble, les logiciels ouverts offrent quelques avantages réels, mais ce n'est pas complètement noir ou blanc.

M. David de Burgh Graham: Merci.

Le président: Merci, monsieur Graham.

M. Richard Fadden: Monsieur le président, me permettez-vous de dire deux choses rapidement?

M. Ryland a parlé de ce qu'il fait et de ce que ses clients font. Si nous imaginons une banque pour une minute, je crois qu'il importe que nous ne soyons pas hypnotisés par les choses vraiment efficaces que M. Ryland fait. Si je prenais un dispositif, que je pourrais probablement obtenir si j'essayais fort, et que je le mettais sous le bureau du vice-président exécutif de la Banque de Montréal, ce serait un dispositif d'enregistrement. Lorsqu'il accéderait aux renseignements et entrerait tous ses mots de passe, je serais en mesure d'y accéder à partir du bureau voisin ou d'une autre ville.

Si l'on parle de l'Internet des objets, je ne crois toujours pas que nous soyons à même de comprendre l'établissement d'une relation avec une ampoule électrique. Je crois que les choses sont meilleures qu'elles l'étaient auparavant, mais encore une fois, si vous contrôlez l'ampoule électrique — et je blague par rapport à cela... mais le dispositif que vous souhaitez utiliser, quel qu'il soit, a la capacité d'obtenir des renseignements.

La sécurité des systèmes dont nous parlons comporte deux aspects réels: la partie dont M. Ryland a parlé et l'environnement que les institutions financières utilisent. Ils sont tout aussi importants l'un que l'autre, parce que si vous réussissez à pénétrer efficacement dans l'institution financière, que ce soit au moyen du dispositif dont j'ai parlé ou d'un autre, vous pouvez non seulement causer des dommages à cette institution financière, mais aussi compliquer énormément la vie de M. Ryland.

M. Ryland ne parle pas seulement de dispositifs de sécurité très complexes. C'est toute une série d'autres choses également. Je dirais que la Banque Royale du Canada fait probablement très bien ces choses. Une modeste caisse populaire du Manitoba ne le fait peut-être pas. Excusez-moi s'il y a des gens ici du Manitoba. C'est le maillon le plus faible dans le problème de la chaîne que nous n'avons pas vraiment réussi à comprendre aussi efficacement que nous le pourrions.

Le président: Merci.

À la suite de cette étude, je suis devenu paranoïaque et j'évitais de parler devant mon réfrigérateur ou mon thermostat. Maintenant, je dois m'inquiéter de mon porte-clé et de mes ampoules électriques.

Monsieur Motz, vous avez cinq minutes, s'il vous plaît.

M. Jim Eglinski (Yellowhead, PCC): Vous avez beaucoup de choses à cacher.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Merci, monsieur le président.

Merci, messieurs, d'être ici.

Monsieur Fadden, lorsque nous parlions plus tôt de lutter contre le terrorisme, vous avez fait allusion à notre modèle canadien actuel comme s'il s'agissait d'un jeu de la taupe, où nous éliminons un problème une fois qu'il est apparu. Y a-t-il un mécanisme qui permet une plus grande proactivité pour prévenir les cyberattaques, mis à part la seule éducation ou formation?

M. Richard Fadden: Oui, je crois qu'il y en a un.

Si vous regardez ce que vous pouvez faire — et je ne suis pas ingénieur, donc je limite mes propos à un langage que je peux comprendre —, vous pouvez prévoir des mesures purement défensives. Vous concevez quelque chose dans votre système, quel qu'il soit: vous y mettez des pare-feu et quoi que ce soit d'autre.

Puis, vous avez ce que j'appelle la « défense agressive »: vous pouvez savoir lorsque quelqu'un essaie de sortir ou de pénétrer, et vous vous en occupez.

Enfin, vous avez l'attaque purement offensive: vous êtes en mesure d'aller trouver des problèmes ou d'affaiblir les capacités d'autrui.

Je crois que nous sommes assez bons en ce qui concerne la première option. Nous ne sommes pas si mauvais pour ce qui est de la deuxième. Je ne crois pas que nous soyons vraiment excellents par rapport à la troisième. Je ne crois pas que nous, au Canada, devions le faire seuls. Nous pouvons le faire avec un tas d'autres pays. Toutefois, la capacité de ce que j'appellerai les « cyberadversaires » d'utiliser 37 intermédiaires inconnus fait en sorte qu'il est très difficile pour les gens de savoir d'où ils viennent, et que sais-je encore.

Vous avez vraiment besoin d'un genre de système de surveillance à l'échelle mondiale. Je ne crois pas que nous en ayons un. Je crois que les États-Unis, selon ce que je comprends, essaient de le faire, mais il y a une limite à ce que même eux peuvent faire.

Vous avez probablement entendu parler de l'ancien secrétaire américain à la Défense, Donald Rumsfeld. Il a été couvert de ridicule à un certain moment, mais je crois qu'il a dit une chose qui est vraie, et cela s'applique à ce domaine: vous ne savez pas ce que vous ne savez pas.

Je crois que M. Ryland sera d'accord avec moi pour dire...

● (1625)

M. Mark Ryland: Il y a les inconnus connus et les inconnus inconnus.

M. Richard Fadden: Ce sont ceux-là qui m'inquiètent.

La technologie avance si rapidement que nous trouvons très difficile de garder une longueur d'avance.

C'est une réponse longue à une question courte, mais je ne crois pas que notre situation soit aussi bonne que ce qu'elle pourrait être à l'échelle internationale.

M. Glen Motz: D'accord, pour amener cette idée un peu plus loin, vous avez dit récemment que nous étions en quelque sorte à l'écart lorsqu'il s'agit de notre capacité de surveiller les terroristes de l'État islamique ou les combattants étrangers qui sont revenus ou qui reviennent vers notre territoire. Diriez-vous que nous sommes en meilleure position lorsqu'il s'agit de cybersécurité?

M. Richard Fadden: Eh bien, si vous avez affaire au gouvernement du Canada, je dirais probablement oui. Je crois que, sous l'ancien gouvernement et le gouvernement actuel, l'appareil gouvernemental a fait de réels progrès pour renforcer la capacité de défendre les systèmes du gouvernement du Canada. Il a limité l'accès à Internet aux systèmes du gouvernement du Canada, ce qui a beaucoup facilité le contrôle.

Je revenais sans cesse au maillon le plus faible de la chaîne. Tout ce qu'il vous faut, c'est un maillon faible qui vous permet d'accéder à tout. Cela dit, je crois que, en ce qui concerne la cybersécurité, le gouvernement est mieux placé qu'il le serait par rapport au terrorisme. Je ne crois pas que sa position soit très bonne relativement au terrorisme. J'essayais juste de dire qu'il y a une limite quelque part par rapport à ce que vous pouvez faire.

Si vous étendez cela aux gouvernements provinciaux, par exemple, il y a des liens entre les provinces et le gouvernement fédéral. La protection des provinces varie beaucoup, je crois. Puis, vous continuez d'avancer, et il ne faut pas beaucoup d'imagination.

Je vais vous donner un exemple: j'ai lu il y a quelques années qu'un atelier de soudage familial — je crois que c'était en Arizona — possédait son propre petit serveur et que sais-je encore. Un État étranger s'est servi d'un problème qui est survenu pour accéder à un élément du gouvernement américain en Chine. Ce que j'essaie de dire, c'est qu'il n'est pas nécessaire que la faille soit béante, pour reprendre une manifestation physique, pour y pénétrer.

De façon générale, je crois que nous tirons assez bien notre épingle du jeu. Nous ne faisons vraiment pas mauvaise figure, mais si nous croyons avoir bloqué toutes les cyberattaques possibles contre nous ou notre économie, alors je crois que nous sommes beaucoup trop optimistes.

M. Glen Motz: Nous avons des vases clos dans l'application de la loi lorsqu'il s'agit de mener quelques batailles, parfois, ainsi que d'échanger des renseignements. Vous avez déjà mentionné que le Canada n'a pas de ressources suffisantes appliquées à ce problème.

Voyez-vous le même problème de cloisonnement pour la cybersécurité?

M. Richard Fadden: Il ne s'agit pas tant de cloisonnement. Certains de mes anciens collègues voudront me donner des coups de pied en dessous de la table parce que je le dis, mais je ne crois pas qu'il y ait un cerveau dirigeant central qui s'occupe des questions de cybersécurité au gouvernement du Canada.

Je crois que le Centre de la sécurité des télécommunications a un rôle réel à jouer. Je crois que la Sécurité publique a un rôle à jouer. L'armée voit les choses de manière légèrement différente. Affaires mondiales Canada a un rôle à jouer pour s'occuper de choses à l'échelle internationale. Innovation, Sciences et Développement économique — je crois que c'est ainsi qu'il s'appelle — joue un rôle dans la réglementation d'Internet et la façon dont nous interagissons avec lui.

Je ne crois pas que la pratique américaine qui consiste à mettre en place un tsar soit nécessairement la solution. Je dirais, à tout le moins en me fondant sur mon ancien titre de conseiller à la sécurité nationale, que nous aurions pu bénéficier d'une plus grande coordination, et peut-être, à un certain moment, d'une plus grande orientation. C'est un domaine très complexe, et les ministères se préoccupent d'abord d'eux-mêmes.

L'appareil gouvernemental est la prérogative du premier ministre. Il va organiser les choses comme il l'entend, mais c'est un domaine dont la manifestation a une portée si mondiale et si complexe, que le simple fait de dire à divers ministères et organismes qu'ils doivent coopérer n'est peut-être pas suffisant, à mon avis.

● (1630)

Le président: Merci, monsieur Motz.

Les cinq dernières minutes vont à M. Picard.

M. Michel Picard (Montarville, Lib.): Merci.

Monsieur Ryland, si je comprends bien, le nuage, c'est une structure centralisée pour laquelle les mesures de sécurité et les niveaux de sécurité sont si élevés que les clients pour lesquels vous stockez des données se sentent assez rassurés, estimant qu'ils sont protégés à 99 % contre les attaques extérieures.

M. Mark Ryland: Je crois que c'est un résumé assez juste. Ils ont certainement l'impression d'avoir une longueur d'avance pour ce qui est d'établir des mesures de défense appropriées, car nous nous occupons de beaucoup de choses dont ils devraient autrement s'inquiéter.

M. Michel Picard: Mais vous venez de dire à M. Graham que vous ne saviez rien au sujet du contenu stocké sur votre serveur, car ce n'est pas votre affaire de savoir ce que les clients mettent sur votre serveur, donc quelle serait la sécurité de votre système du point de vue d'un cheval de Troie?

M. Mark Ryland: C'est très sécuritaire, car nous concevons et mettons constamment à l'essai nos systèmes en présumant que nous avons des clients hostiles. Nous présumons que nous sommes attaqués par nos clients, nous en tenons compte et nous nous assurons que les caractéristiques d'isolement du système sont très robustes.

M. Michel Picard: Il y a donc une sécurité de part et d'autre, contre les attaques provenant de l'extérieur ainsi que celles provenant de l'intérieur.

M. Mark Ryland: Oui.

M. Michel Picard: Excellent. Merci beaucoup.

Monsieur Fadden, cette étude nous a fait voyager. Nous n'avions aucune idée de l'endroit où nous allions, parce que c'est tellement vaste, gros, large et diversifié. Nous comprenons tout à fait la pertinence de toute mesure à prendre relativement à cette question, particulièrement de mon côté, avec les institutions financières. Selon vos connaissances au sujet du gouvernement et votre expérience, diriez-vous que nous devrions commencer à établir des politiques, et quelles seraient certaines de vos recommandations?

M. Richard Fadden: Monsieur le président, j'aimerais revenir à un des points soulevés plus tôt. Je crois que, par voie législative, le Parlement doit imposer des obligations aux institutions financières, au même titre que ce qu'il a fait concernant le blanchiment d'argent. Il doit les obliger à faire une diversité de choses. En ce moment, la plupart de ces choses sont faites dans l'intérêt propre des institutions financières. Elles ont tendance à être assez bonnes, mais nous devrions grandement augmenter le nombre de nos signalements d'atteintes et de tentatives d'atteinte. Il y a un règlement, si ma mémoire est bonne, qui en fait une obligation en ce moment. Ce n'est pas aussi complet que ça devrait l'être.

Les Américains et les Britanniques, en particulier, prévoient des sanctions sévères pour les institutions qui ne signalent pas les atteintes. Je ne sais pas comment nous pouvons nous attendre à gérer efficacement les atteintes si nous ne savons pas quand elles se produisent. Je crois que c'est mieux qu'autrefois, mais tout de même... Je dirais donc que l'on doit imposer des obligations claires aux institutions et signaler les atteintes. Encore une fois, certains de mes anciens collègues vont me donner des coups de pied en dessous de la table, mais je ne crois pas que nous transmettions assez de renseignements classifiés au secteur privé. Je crois que nous nous en tirons beaucoup mieux qu'il y a 15 ou 20 ans, mais si vous prenez le représentant du service technologique le plus expérimenté de la Banque Royale — ce qui s'adonne à être ma banque, mais je n'essaie pas de la promouvoir — et que vous lui demandez de collaborer sur des questions de cybersécurité, et que le représentant canadien n'est pas autorisé à communiquer des renseignements classifiés, je ne vois pas comment vous pouvez avoir un dialogue réel. Les États-Unis et le Royaume-Uni autorisent, du point de vue des renseignements classifiés, des gens dans le secteur privé. Je ne veux pas dire que nous ne faisons rien de tout cela, car nous le faisons. Je dis juste que nous ne le faisons pas assez. Je dirais ces trois choses.

M. Michel Picard: Quand vous avez dit que nous pourrions être tentés de faire abstraction de la Russie et de la Chine ou de les oublier parce que notre intérêt est ailleurs, j'ai été surpris. Je croyais que nous étions tellement concentrés sur la Russie et la Chine que nous avions oublié les menaces réelles provenant d'autres pays, de pays satellites travaillant pour ces États principaux. Lorsque nous avons examiné Cambridge Analytica à notre comité, il a semblé évident, au bout du compte, que la menace n'allait peut-être pas être la Russie, mais avec un si grand nombre de bureaux satellites à l'oeuvre dans d'autres pays, où devrions-nous concentrer nos efforts?

M. Richard Fadden: Monsieur le président, je crois que c'est la question à 57 000 $.

Des députés: Ha, ha!

M. Richard Fadden: Une partie du problème tient au fait que vous ne pouvez pas faire abstraction de la Russie et de la Chine. Nous ne pouvons pas fait fi de ces choses que vous venez d'énumérer. Je crois que nous mettons de côté les groupes terroristes internationaux à nos risques et périls. Nous avons tout un tas de groupes de la société civile qui ne prennent pas au sérieux la cybersécurité. Je pourrais probablement en énumérer d'autres, mais la vérité, c'est que nous ne pouvons faire abstraction d'un seul d'entre eux.

C'est pourquoi je crois qu'il doit y avoir une plus grande collaboration, une plus grande communication et plus d'efforts pour nous amener au point suggéré par un des autres députés. Nous voulons essayer de garder une longueur d'avance sur le problème, plus que dans le passé. Je n'ai pas de réponse, sauf pour dire que, même s'il se peut bien que vous ayez raison par rapport à cette période de six mois, peut-être que les choses changeront au cours des prochains six mois. Nous devons être agiles. Encore une fois, après avoir travaillé pour le gouvernement pendant 40 ans, je peux dire que ce n'est pas un de nos points forts. Cela vaut pour les gouvernements de façon générale, mais je crois que nous devons être plus agiles que par le passé pour nous occuper de tous les sujets dont vous parlez.

● (1635)

Le président: Merci, monsieur Picard.

Avant de suspendre, j'aimerais juste remercier nos témoins. Habituellement, les mots « agile » et « gouvernement » ne se retrouvent pas dans la même phrase.

Cela dit, nous allons suspendre les travaux pour une minute ou deux. Merci de vos exposés.

M. Richard Fadden: Tout le plaisir était pour moi.

M. Mark Ryland: Merci.

Le président: Nous suspendons nos travaux.

● (1635)

(Pause)

● (1635)

Le président: Nous allons composer avec le vote par appel nominal, à 17 h 30. Nous arrêterons probablement autour de 17 h 20, plutôt que 17 h 30. Je vais étirer la discussion autant que je le peux.

Cela dit, nous sommes de retour, et je demanderai à M. Drennan de présenter son exposé.

Vous avez 10 minutes. Si vous me regardez, je vous donnerai un signal quand vous approcherez des 10 minutes.

Merci, monsieur Drennan, de comparaître.

M. Steve Drennan (directeur, Cybersécurity, Groupe ADGA): Merci. Je m'appelle Steve Drennan, et je suis heureux d'être ici aujourd'hui pour me représenter et représenter ADGA dans le domaine de la cybersécurité et le secteur financier au Canada. Merci de m'avoir invité à présenter un témoignage au comité de la sécurité publique à la Chambre des communes aujourd'hui, et merci de votre temps.

En guise de contexte, ADGA est une entreprise entièrement canadienne qui fournit des services professionnels stratégiques de consultation et une technologie de pointe dans les services informatiques de défense, de sécurité et d'entreprise depuis plus de 50 ans. Elle offre des solutions ainsi que des services d'ingénierie et de dotation haut de gamme dans des locaux gouvernementaux et commerciaux. ADGA possède donc beaucoup de connaissances et d'expertise dans des domaines comme la cybersécurité. ADGA a aussi des opinions tranchées, tout comme moi, sur les besoins et l'évolution de la sécurité d'un océan à l'autre et sur la connaissance du paysage et des partenaires stratégiques. ADGA possède une solide capacité combinée en matière de sécurité, en plus d'une vaste expérience en conception d'évaluations de cybersécurité et en conformité. Voilà qui vous donne une idée de mes antécédents aujourd'hui.

En examinant les témoignages précédents en ligne, j'ai vu un thème ressortir: que le Comité avait déjà reçu beaucoup de commentaires sur les cyberattaques, les difficultés, les catégories et les défauts dans le domaine. Compte tenu de tout cela, je me suis dit que je miserais aujourd'hui sur les solutions en matière de cybersécurité. Il n'y a pas de solution miracle, mais c'est possible de déployer une forte capacité d'échelle, et beaucoup d'autres éléments peuvent être renforcés de manière à vraiment accroître ce que nous faisons et à stimuler le secteur financier et canadien.

J'aime penser que c'est une infrastructure essentielle. Vous voyez probablement les centrales électriques, les barrages et les systèmes classifiés comme de l'infrastructure essentielle, mais le secteur financier représente certainement de l'infrastructure essentielle. C'est un grand système interdépendant qui englobe beaucoup d'entités différentes, comme la Banque du Canada, Paiements Canada, Interac — qui ont comparu —, le receveur général, les commerçants, les petites et grandes entités commerciales et aussi les clients. Il y a beaucoup de points finaux. Il y a beaucoup de choses qui peuvent mal tourner. Ce sont aussi toutes les données qui sont en transit ou en mémoire. Si vous avez entendu parler d'un réseau, d'un aspect ou d'une solution ou y avez réfléchi, ce n'est pas toute l'histoire.

Un changement se produit dans la cybersécurité. On assiste maintenant à des attaques sociopolitiques et à la manipulation de marques, ainsi qu'à des attaques financières de petit et grand volumes. Étant donné tout ce qui est en jeu et la capacité des cybercriminels de cacher, de dissimuler et de lancer des attaques sans interruption, le Canada doit adopter une approche mise à jour à l'égard de la cyberdéfense dans le secteur financier. Les jours où l'on se cachait derrière des murs, des murs réels ou des pare-feu, sont derrière nous. Tout est très interrelié.

Il importe aussi de comprendre l'adversaire. Je crois qu'on vous a tous bien renseignés à ce sujet, mais les cybercriminels et les États nations possèdent d'énormes ensembles de ressources. Ce serait un très grand pays, sur le plan de son PIB, si tous les cybercriminels combinaient leur richesse. On ne peut souvent pas les atteindre physiquement vu leur lieu de provenance.

Je vais vous donner une statistique, un bref exemple, et je n'entrerai pas trop dans les détails: selon un rapport récent de Mandiant — Mandiant est le cyberarmement de FireEye, un de nos partenaires stratégiques —, la durée médiane mondiale durant laquelle un logiciel malveillant vit dans un réseau jusqu'à ce qu'il soit découvert et arrêté est de 101 jours. Pensez-y une seconde. C'est une durée incroyable pour quelque chose qui exfiltre et saisit des données avant qu'on le découvre. Il faut parfois attendre jusqu'à 2 000 jours avant qu'on le découvre. Bien que le problème cybernétique soit complexe, on peut s'y attaquer de façon simplifiée pour les utilisateurs, les commerçants, les entreprises et les organisations bancaires. C'est ce sur quoi je veux insister aujourd'hui, soit certains des moyens qui nous permettent d'y remédier.

Je vais me concentrer sur les thèmes de solutions cybernétiques qui peuvent permettre de lutter contre des attaques cybernétiques à grande échelle à l'endroit du secteur financier canadien. Le premier thème que j'aimerais parcourir est ce que j'appelle la « convergence des données cybernétiques et la capacité de protection ». Voyez cela comme des solutions de prochaine génération qui pourraient être déployées à l'échelle pour que tout le monde puisse les utiliser et en profiter. Le concept, c'est qu'une organisation pourrait en fait diriger cet effort et mettre cette capacité dans un lieu central pour que cela soit activé par toutes les entités dont je parlais. Tout ce à quoi nous avons réfléchi.

● (1640)

Il y a de nouvelles technologies vraiment fantastiques. L'une d'entre elles associe des idées sur l'intelligence artificielle centralisée, l'apprentissage machine, l'analytique avancée, la recherche de menaces — si vous n'avez pas entendu parler de ces concepts, vous pouvez me poser des questions plus tard — et l'orchestration de la sécurité. Vous pouvez en fait créer des mesures de détection et d'intervention cybernétiques semi-automatiques. Il est possible de le faire de façon assez automatisée. Parfois, vous voulez qu'une personne soit en mesure de prendre des décisions sur des aspects essentiels et d'intervenir lorsque vous ressentez une cybermenace, particulièrement si vous fermez une partie d'un réseau.

Les immeubles et les réseaux intelligents peuvent aussi jouer un rôle. Ce n'est pas juste nouveau. Ce qui est nouveau est bon, mais lorsque vous introduisez toutes sortes de détecteurs de l'Internet des objets, vous présentez tout un tas de données, et celles-ci peuvent ensuite être compromises. Si vous avez la capacité d'ordonner l'ensemble des données physiques — des données opérationnelles, qu'on appelle parfois données de technologie opérationnelle, et des données de l'IdO —, nous pouvons trouver des solutions qui nous permettent de mieux détecter quand il y a un problème. Par exemple, en cas de problème environnemental ou d'attaque contre un immeuble ou un centre de données, vous voudriez probablement être mis au courant dans le monde cybernétique et être en mesure d'y réagir. Aujourd'hui, ce n'est pas bien fusionné, mais ça pourrait l'être.

Il y a l'idée d'aller de l'avant au chapitre de la défense cyberactive ou même des cyberattaques, et c'est lié à la législation et aux règles existantes. Lorsque vous savez que vous êtes sondé et attaqué, la capacité d'intervenir et de déterminer où se trouve l'attaque et de l'interrompre, ou du moins de vous protéger, est très importante.

La sécurité du service de noms de domaine, qui est au coeur d'Internet, est assortie de règles appelées DNSSEC et d'autres éléments. C'est très important, parce que si vous ne pouvez pas faire confiance à votre résolution d'adresse et à l'endroit où vous allez rechercher vos données, cela se révèle très important.

Les renseignements sur la cybermenace, que nous avons abordés plus tôt, sont vraiment intéressants, parce qu'on peut procéder de façon verticale. Vous pourriez ne disposer que de données et de renseignements bancaires canadiens, et vous verriez donc les tendances dans les attaques sur le marché canadien, et ce, avant qu'elles frappent la plupart de vos points finaux, puis vous seriez en mesure d'y réagir à l'avance. Vous pourriez prendre des décisions et faire des mises à jour avant que l'attaque ne soit généralisée. Il pourrait y avoir des attaques du jour zéro ou des attaques par des menaces sophistiquées et persistantes, mais la capacité de voir les attaques et d'y réagir avant qu'elles deviennent un problème est capitale.

● (1645)

Le président: Excusez-moi, monsieur Drennan. Le système archaïque que nous possédons ici empiète sur un exposé très impressionnant sur la cybersécurité. On me dit que nous avons... Est-ce que ce n'est pas 15 minutes?

M. David de Burgh Graham: N'utilisez pas ParlVu.

Le président: Au début, je croyais qu'il s'agissait d'une vérification du quorum, alors je n'ai rien dit, mais ensuite, le temps file... mais ce n'est pas le cas. Nous allons considérer qu'il s'agit d'une vérification du quorum.

M. David de Burgh Graham: Vous pourriez gagner 45 secondes si vous regardiez le site noscommunes.ca plutôt que ParlVu. Vous recevez donc le fil direct de cette façon.

Le président: Je vois ce qu'il regarde.

M. David de Burgh Graham: Vous ne regardez pas la bonne chose. Allez-y plus rapidement.

Le greffier du comité (M. Naaman Sugrue): Je vérifie les deux.

Le président: Bon, nous venons de perdre 45 secondes. Je suis désolé.

Merci, monsieur Drennan, de votre patience et de votre compréhension. Allez-y.

M. Steve Drennan: Merci.

Pour revenir à mon dernier point sur les capacités, vous pourriez mettre en oeuvre à l'échelle une initiative de gestion de la chaîne d'approvisionnement et du cycle de vie, pour rester dans le même thème. Le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications, le CST, exécutait dans le passé un programme appelé la « liste des produits évalués ».

Lorsque nous parlons de Huawei, les gens ont des préoccupations, et nous en discutons; il faut prendre en considération tout ce qui est utilisé: tous les logiciels qui sont programmés — qui sont souvent numérisés et sauvegardés dans le nuage — ainsi que le matériel et les puces. Où les puces sont-elles fabriquées? D'où viennent-elles? Il faudrait un programme intégral qui évalue l'équipement et les logiciels du berceau à la tombe pour que nous puissions être sûrs qu'ils sont sans risque, mais le gouvernement est la bonne organisation pour exécuter ce genre de programme.

Le second thème que j'aimerais aborder concerne les avantages que l'on peut tirer d'un nuage public sécurisé. Je crois que le témoin précédent représentait Amazon Web Services, alors je suis sûr qu'il vous en a parlé de long en large. Je vais dire, à mon tour, que c'est une bonne idée. La meilleure façon de réunir une foule de groupes différents est d'utiliser un nuage public canadien sécurisé. Je crois que c'est une solution que nous devons envisager plus sérieusement. Je sais qu'un certain nombre d'institutions bancaires songent également à utiliser cette technologie.

Lorsque vous avez des réseaux à l'intérieur d'une organisation, c'est un nuage privé ou un nuage hybride, à mesure que vous retirez du contenu du nuage public. Cependant, l'utilisation d'un nuage public sécurisé à grande échelle est capitale, car ce serait une façon géniale de réunir tout le monde et tous les consommateurs afin qu'ils puissent communiquer entre eux. Pourvu que vous preniez des mesures adéquates en matière de sécurité, de politiques et de filtres, tout le monde aura accès au même niveau de sécurité. Certains exploitants se sont dotés de véritables systèmes auxiliaires au Canada, alors s'il y a une panne du système — quelque chose d'inévitable —, la reprise après catastrophe se fait au Canada, ce qui est très important à l'égard de l'hébergement et de la propriété des données.

Dans ce contexte, la flexibilité informatique est capitale, car elle permet de réagir et de lancer de nouvelles applications.

Le président: Il vous reste une minute.

M. Steve Drennan: D'accord. Je vais me dépêcher. Comme troisième thème, je vais parler du besoin de veiller à ce que les données de nature délicate soient beaucoup plus fiables. À dire vrai, les banques et les institutions bancaires clés pourraient devenir une ressource unique et fiable en ce qui a trait aux données d'inscription, d'authentification et d'identification.

Le quatrième thème concerne la sensibilisation des utilisateurs. Une chose que nous ne devons pas oublier est que les utilisateurs sont toujours le maillon faible de la chaîne. On pourrait donner à certaines personnes des mandats spécifiques et offrir davantage de formation afin que les gens soient sensibilisés à ce sur quoi ils cliquent sur Internet et afin qu'ils sachent comment se comporter correctement et sainement.

En conclusion, il y a des solutions informatiques de prochaine génération que nous pouvons mettre en oeuvre à grande échelle afin de stabiliser et de renforcer le milieu financier, mais cela suppose d'injecter les fonds nécessaires et de motiver les gens.

● (1650)

Le président: Merci, monsieur Drennan.

Chers collègues, il nous reste environ une demi-heure. Nous allons utiliser à peu près tout le temps qu'il nous reste si je vous laisse sept minutes chacun. Si vous acceptez d'avoir chacun six minutes, nous aurons le temps pour une question supplémentaire. Êtes-vous d'accord?

Des députés: D'accord.

Le président: Parfait, vous aurez six minutes chacun. La parole va à Mme Dabrusin. Allez-y.

Mme Julie Dabrusin (Toronto—Danforth, Lib.): Merci.

Je voulais d'abord discuter de votre quatrième thème. Un témoin a donné une image qui m'est vraiment restée en tête depuis le début de nos séances. C'était à propos d'un système très sécuritaire qui communiquait de l'information entre deux boîtes en carton. Dans cette métaphore, les deux boîtes en carton représentent les gens qui utilisent le système. Vous n'avez pas eu le temps de terminer ce que vous aviez à dire à propos de la sensibilisation des utilisateurs, mais peut-être pourriez-vous le faire maintenant. Quelles mesures le gouvernement pourrait-il prendre, précisément, afin de s'améliorer de ce côté-là, afin de sensibiliser le public et de renforcer la cybersécurité, l'hygiène informatique ou peu importe comment vous voulez l'appeler.

M. Steve Drennan: Parfait. Je suis content de pouvoir en parler davantage. Je crois qu'il n'y a pas beaucoup de normes. J'ai consulté les lignes directrices du Conseil du Trésor et les exigences relatives à la Gestion de la sécurité des technologies de l'information, et tout cela n'est pas très clair. On ne définit pas vraiment ce qu'il faut faire pour former les utilisateurs ou pour fournir une orientation suffisante en matière d'informatique. Tout ce qu'on fait est un peu passif. Nous avons des sites Web sur la cybersécurité que les gens peuvent consulter pour en apprendre davantage, mais que faisons-nous pour diffuser activement l'information? Peut-être faudrait-il davantage de campagnes. Peut-être devrait-on organiser des activités d'apprentissage par le jeu, des réunions mensuelles et des activités thématiques pour sensibiliser les gens. Je vais vous donner un exemple de harponnage. A-t-on déjà abordé le sujet ici?

Mme Julie Dabrusin: Je ne crois pas.

M. Steve Drennan: Vous a-t-on parlé de hameçonnage?

Mme Julie Dabrusin: Oui.

M. Steve Drennan: Le harponnage est une forme de hameçonnage plus ciblé. Disons que vous recevez tous un message qui semble provenir de l'honorable John McKay. En objet, il vous dit que c'est urgent et que vous devez cliquer dessus. Vous allez probablement vouloir cliquer dessus, puisque le message semble venir de John McKay.

Le président: Ce n'est pas un bon exemple.

Des voix: Ha, ha!

M. Steve Drennan: Eh bien, c'est tout de même un exemple. Si vous recevez un message qui semble venir d'une personne en position d'autorité et que le style d'écriture et les choses qui y sont mentionnées ressemblent à ce qui se trouve habituellement dans les messages que vous échangez, alors vous êtes plus susceptible de cliquer dessus. Vous ressentez la pression. Même si vous remarquez des problèmes avec la mise en page ou des fautes d'orthographe, vous allez tout de même cliquer dessus. J'imagine qu'il vous arrive souvent de sortir vos appareils et de faire défiler vos messages très rapidement.

Une façon de lutter contre le harponnage serait d'offrir une courte formation et de sensibiliser les gens, mais ce n'est pas quelque chose qu'on peut faire seulement une fois. Il faut des interventions répétées. Une façon de procéder serait d'organiser une campagne anonyme pendant laquelle on analyserait du harponnage. Vous pourriez envoyer à tous les membres d'une organisation ce genre de courriel. Vous êtes des gens éthiques, alors cela ne pose pas de problème. Il y a un lien dans le courriel, et si le destinataire clique dessus, cela ne fera qu'enregistrer anonymement que quelqu'un a cliqué sur le lien. Au bout du compte, vous avez une statistique sur le nombre de personnes qui ont cliqué sur le lien. Les résultats ne seront pas reluisants la première fois, mais après, vous pouvez informer les gens que vous avez « organisé une campagne de harponnage. Venez nous voir demain pendant l'heure du dîner et nous vous expliquerons pourquoi vous n'auriez pas dû cliquer sur le lien », parce que beaucoup de personnes l'ont fait. Puis, lorsque vous recommencez — parce que vous allez devoir organiser ce genre de campagne deux ou trois fois afin de sensibiliser les gens —, les utilisateurs vont être beaucoup plus prudents. Vous n'allez jamais atteindre un taux de réussite de 100 %, mais c'est toujours une bonne chose de faire baisser le nombre de personnes prêtes à cliquer sur un tel lien.

Mme Julie Dabrusin: Intéressant. Ce serait une initiative que les organisations pourraient mettre en oeuvre. Mais ce que j'aimerais savoir — parce que nous allons devoir formuler des recommandations — c'est ce que nous pouvons faire pour renforcer notre rôle dans tout cela.

J'ai pris en note qu'un témoin a parlé du problème des mots de passe. Il y a déjà des exigences lorsque vous choisissez un mot de passe: il y a un nombre minimal de caractères, de lettres majuscules et de chiffres, etc., qu'il faut entrer. Cependant, il n'est pas interdit d'utiliser le même mot de passe plus d'une fois. Il semble qu'une grande faiblesse des mots de passe tient au fait que les gens utilisent le même encore et encore. C'est très commun. Peut-être pourrait-on afficher un petit message rappelant aux gens qu'il ne faut pas utiliser le même mot de passe. Ce serait simple, parce que même si un mot de passe satisfait à toutes les autres exigences, il ne serait pas sécuritaire. Dans l'industrie de la finance, les gens s'inscrivent aux services bancaires en ligne et à toutes sortes d'autres choses du même genre, alors peut-être que l'on pourrait proposer ce genre de pratiques comme normes.

M. Steve Drennan: Oui. Vous touchez à deux questions. Il y a d'un côté la sensibilisation à la cybersécurité, et, de l'autre, les mots de passe. Je vais parler des deux.

En ce qui concerne les mots de passe, il devrait effectivement y avoir davantage de normes. Ce serait facile d'établir cela dans les politiques, et vous devriez le faire. Cela pourrait même être visé par une loi. Ce serait plus clair. Si je reviens à la norme de GSTI ou aux exigences connexes, les lignes directrices pour le choix d'un mot de passe ne sont pas toujours claires. Il faudrait une approche plus normative.

Bien sûr, ce que vous dites est un exemple parmi d'autres. Vous voulez probablement éviter les mots de passe répandus que les gens choisissent souvent. Vous devez faire en sorte que les gens savent qu'il ne faut pas choisir des dates qui ont une signification personnelle qu'une personne mal intentionnée connaît déjà.

Il y aurait des façons d'inscrire ce genre d'exigences dans la loi et de les appliquer. Un excellent exemple...

● (1655)

Mme Julie Dabrusin: Puis-je vous interrompre rapidement? Je n'ai plus beaucoup de temps.

M. Steve Drennan: Oui.

Mme Julie Dabrusin: Y a-t-il des pays qui ont pris ce genre de mesures? Pouvez-vous nous donner des exemples que nous pourrions examiner?

M. Steve Drennan: Pas à ma connaissance, mais l'Allemagne et l'Europe ont adopté beaucoup de dispositions législatives sur le sujet. Peut-être devriez-vous consulter le règlement général sur la protection des données et d'autres normes connexes, mais je ne suis pas sûr à 100 %.

Mme Julie Dabrusin: Vous pouvez continuer. Je voulais seulement poser la question.

M. Steve Drennan: Je voulais dire également qu'il y a trop de mots de passe, trop de mots de passe différents. Vous ici présents, à combien de systèmes devez-vous vous connecter juste pour le travail?

Une solution serait d'harmoniser les mots de passe, mais d'adopter l'authentification à deux étapes ou l'authentification biométrique. Cela donnerait des mots de passe très forts et harmonisés. Ce serait beaucoup plus efficace, en vérité. Si en plus vous mettez en oeuvre la capacité de contrôler les utilisateurs afin de cerner des comportements problématiques sur le réseau, cela donnerait un modèle beaucoup plus solide que de demander à tout le monde de se rappeler 15 mots de passe qu'ils vont réutiliser constamment.

Le président: Merci, madame Dabrusin.

Monsieur Motz, vous avez six minutes. Allez-y.

M. Glen Motz: Merci, monsieur le président, et merci, monsieur Drennan d'être ici.

Comme vous l'avez déjà dit, votre groupe travaille auprès du gouvernement, de l'industrie et des organismes d'application de la loi sur des questions de sécurité, y compris la sécurité nationale. L'année dernière, un expert s'est exprimé dans le cadre de notre étude sur la sécurité et avait dit qu'il n'avait aucune confiance dans l'état de préparation du Canada à l'égard des menaces technologiques émergentes comme l'intelligence artificielle ou l'informatique quantique.

Vous avez travaillé avec le Canada, et d'après votre expérience, comment évalueriez-vous l'état de préparation de notre pays dans ce contexte?

M. Steve Drennan: Nous ne sommes pas aussi prêts que nous devrions l'être, mais nous avons au moins commencé. Je dirais, malheureusement, que cela varie beaucoup en fonction du groupe concerné. Par exemple, le Centre canadien pour la cybersécurité met l'accent sur l'analyse et la communication des indicateurs de compromission et d'autres choses du genre, alors qu'il pourrait jouer un rôle beaucoup plus important — et ce sera sans doute le cas dans l'avenir — dans la façon dont ses capacités peuvent être utilisées.

Il y a d'autres organisations dont les capacités varient en fonction des technologies qu'elles utilisent. Par exemple, certaines utilisent le pare-feu de Fortinet, alors que d'autres utilisent celui de Check Point ou de Cisco. Le niveau d'efficacité varie selon les pare-feu; certains appartiennent à la prochaine génération, tandis que d'autres, non.

Malheureusement, les interventions que nous pourrions effectuer visent toutes sortes de choses différentes. Vous avez parlé de l'intelligence artificielle, de l'apprentissage machine et de l'informatique quantique. À mesure que les attaques deviennent plus perfectionnées, nous aurons besoin de mesures de protection plus perfectionnées à grande échelle, et c'est justement pourquoi j'ai proposé l'utilisation d'un nuage public. Si le secteur financier était géré à partir d'un espace commun, les capacités avancées seraient à la portée de tous ceux qui sont connectés à la source. Ce serait une façon de faire en sorte que tout le monde soit sur le même pied.

M. Glen Motz: On dit qu'il manque énormément de spécialistes en cybersécurité au Canada, et dans le reste du monde aussi, j'imagine. Que fait votre groupe afin de former un bassin de personnes compétentes? De quelle façon et à quels égards investissez-vous pour que les gens et certains groupes cibles puissent acquérir des compétences dans ce domaine émergent?

M. Steve Drennan: Ce dont vous parlez est effectivement au centre des priorités du Groupe ADGA.

Nous sommes très fiers du fait que le Groupe ADGA est dirigé par une directrice générale, tout comme nous sommes fiers de notre histoire au Canada et de notre diversité. Nous avons investi massivement dans des programmes d'alternance travail-études pour encourager les gens ayant des compétences émergentes à s'intéresser à la cybersécurité. Il y a d'autres domaines également, mais il est question de cybersécurité aujourd'hui.

Nous jouons de nombreux rôles... Nous pouvons faire du recrutement dans les établissements d'enseignement universitaires et collégiaux, et nous pouvons aider les étudiants qui sont inscrits à des programmes pertinents. Par exemple, le Collège algonquin offre un excellent programme sur la cybersécurité. Les universités sont également en train d'élaborer certaines choses relatives à la cybersécurité, et tout cela se passe ici à Ottawa. Nous jouons donc un rôle actif et nous travaillons aussi avec d'autres collèges.

Il est important de recruter intentionnellement des personnes ayant divers talents et compétences et d'avoir beaucoup de diversité parmi les personnes dans le groupe. Nous allons faire en sorte qu'il y ait constamment un bassin de personnes compétentes au Canada. C'est notre responsabilité à tous de veiller à ce que les gens soient motivés et enthousiastes par rapport au domaine. S'il y a énormément de travail en informatique cette année, mais aucun l'année suivante, les personnes compétentes vont aller voir ailleurs.

● (1700)

M. Glen Motz: La semaine dernière — je crois —, un représentant de l'Université Ryerson est venu témoigner. Il a été question d'un programme universitaire, mais il se pourrait que ce qu'on veut mettre en place soit lacunaire à certains égards. Je voulais savoir si les établissements d'enseignement consultaient votre groupe ou des groupes comme le vôtre dans l'industrie afin de recevoir de l'aide pour l'élaboration des programmes servant à former des diplômés qui ont les compétences nécessaires pour travailler dans votre entreprise.

M. Steve Drennan: Oui, c'est effectivement quelque chose que nous faisons. J'ai déjà aidé à formuler une rétroaction concernant le programme du Collège algonquin. Nous avons aussi eu des discussions avec le Collège Willis. Il a un programme de cybersécurité, et j'ai fourni une rétroaction sur son contenu, sur ce qui manque et sur les autorisations de sécurité du gouvernement du Canada qui seront nécessaires pour les étudiants pendant leurs études et qui leur permettront de trouver de bonnes carrières et de rester au Canada. Nous collaborons avec les universités et proposons une orientation pour leurs programmes, par exemple les programmes dispensés à l'ensemble des étudiants en génie. Nous discutons régulièrement avec ces groupes et nous travaillons directement avec eux. Donc, oui, nous pouvons travailler avec les facultés universitaires pour fixer les objectifs.

M. Glen Motz: Pouvez-vous nous expliquer la différence, s'il y en a une, entre la cybersécurité en matière de défense et la cybersécurité dans le secteur des technologies de l'information? Y a-t-il bien une différence?

M. Steve Drennan: Quelques différences clés me viennent à l'esprit. On pourrait comparer l'un des deux à un barrage sur le point d'éclater. La cybersécurité en matière de défense comprend une succession d'étapes: d'abord, ce qu'on appelle la « défense », puis la « défense active », et enfin la « cyberattaque ». À ce chapitre, les lois habilitantes sont d'une importance capitale. De nos jours, l'informatique est considérée comme un tout nouveau théâtre d'opérations à part entière, au même titre que les théâtres d'opérations de la Marine ou de la Force aérienne. Voilà pourquoi il faut absolument adopter des dispositions législatives qui donneront à la Défense nationale une plus grande marge de manoeuvre dans le cyberespace. Lorsque les troupes sont déployées dans les théâtres d'opérations, l'informatique peut faire la différence entre la victoire et la défaite. C'est une différence entre les deux. Il y a aussi un peu plus de restrictions imposées à la cybersécurité en matière de défense. Il y a une foule de réseaux classifiés et toutes sortes d'autres questions qu'il faut régler, notamment le financement et les vastes modifications qui sont présentement à l'étude.

Il n'y a pas autant de règles dans le secteur privé. Nous avons parlé plus tôt des renseignements sur les cybermenaces. Nous savons que les grands fournisseurs peuvent recueillir des données du monde entier grâce à leurs noeuds dans divers pays. Il y a moins de restrictions imposées à leurs activités de cette façon. À dire vrai, c'est une très bonne chose, parce que les fournisseurs peuvent ensuite communiquer les données au gouvernement et à l'industrie.

Le président: Merci, monsieur Motz.

Monsieur Dubé, vous avez six minutes. Allez-y.

M. Matthew Dubé: Merci beaucoup d'être parmi nous.

J'aimerais revenir sur la question de la main-d'oeuvre que mon collègue a abordée. Je veux l'étudier d'un angle différent. Pouvez-vous me dire si ce qui paralyse l'industrie, c'est le fait que les autorisations de sécurité sont accordées en fonction de l'origine des personnes et d'autres choses du genre? Vous connaissez le processus d'approvisionnement pour les services informatiques, mais pour ce qui est du processus traditionnel d'approvisionnement — je ne sais pas si j'utilise le bon terme —, par exemple lorsqu'il s'agit de construire des avions de combat à réaction, des hélicoptères, du matériel militaire, etc., il y a déjà eu des problèmes parce que des entreprises étaient disqualifiées ou n'obtenaient pas des contrats en fonction de nos alliés ou de notre position dans un contexte particulier. Il y a des entreprises avec des gens très compétents qui auraient peut-être pu fournir du matériel idéal pour les Forces armées canadiennes, disons, mais on les refuse parce que les États-Unis ont des réserves par rapport à un pays ou quelque chose du genre. Ce genre de choses arrive-t-il également dans le secteur informatique, et si oui, quelles mesures pouvons-nous prendre en conséquence?

M. Steve Drennan: Oui, nous avons observé la même chose. Les clients privés sont beaucoup plus souples. Pourvu que votre entreprise ait une bonne réputation et embauche des personnes qui ont les bonnes compétences, le contrat pour la fourniture de services informatiques est à vous. En ce qui nous concerne, nos activités touchent beaucoup l'évaluation de la sécurité, la conception de systèmes de sécurité et la sécurité infonuagique. Au Canada, le secteur privé est très vaste, et il exprime bien plus clairement ce que vous pouvez faire.

Une difficulté tient au grand nombre de contrôles de sécurité qu'il faut subir. De mon côté, cela a été plutôt simple, mais pour d'autres, par exemple les gens qui ne résident pas au Canada depuis assez longtemps, il est impossible d'obtenir une autorisation de sécurité. En général, la plupart des contrats exigent une autorisation de sécurité « secret ». Pour certains, il faut une autorisation de sécurité « très secret », mais c'est plutôt rare qu'on demande une simple cote de fiabilité. Je crois que pour réussir un contrôle de sécurité, vous avez besoin de 5 à 10 années de résidence au Canada, et souvent de la citoyenneté canadienne. Ce serait peut-être une bonne idée d'élaborer des contrôles de sécurité supplémentaires pour que les gens puissent obtenir l'autorisation de sécurité « secret » et d'envisager d'uniformiser le processus. Je ne vois vraiment pas pourquoi chaque ministère doit avoir son propre processus de contrôle de sécurité et ses propres règles. Si vous êtes digne de confiance, vous devriez l'être partout. C'est la même chose pour une entreprise.

Il y a probablement des modifications que l'on pourrait apporter au fil du temps. Il faudrait probablement envisager d'autres façons d'accorder une autorisation de sécurité aux gens. Il y a un certain exode des cerveaux au Canada, alors nous devrions chercher à recruter des gens talentueux à l'étranger. Nous devons faire en sorte que les gens qui viennent au Canada puissent travailler à des projets importants, tout en assurant au gouvernement et aux institutions bancaires que ces personnes ont réussi les contrôles de sécurité appropriés et qu'il n'y a pas de problème avec leurs antécédents.

● (1705)

M. Matthew Dubé: Je comprends. Toujours dans le même ordre d'idées, cela poserait-il un problème particulier dans le secteur informatique? Disons que vous êtes une entreprise qui construit des hélicoptères, vous vendez vos hélicoptères non pas au ministère des Finances, mais au ministère de la Défense nationale. Cependant, si vous êtes une entreprise de cybersécurité, le ministère des Finances a besoin de vos services tout autant que la Défense nationale. On peut refuser rapidement d'accorder une autorisation de sécurité à certaines personnes dans le cadre du processus traditionnel d'approvisionnement en matière de défense à cause de nos alliances militaires traditionnelles. Donc, cela peut-il poser un problème?... Va t-il y avoir un problème si vous fournissez des services de cybersécurité au ministère des Finances et que votre entreprise embauche des spécialistes qui ne réussiraient peut-être pas le contrôle de sécurité de la Défense nationale? Voyez-vous ce que je veux dire?

Vous avez dit qu'il y avait différents processus de contrôle de sécurité. Est-ce que le Canada s'empêche, donc, de protéger correctement le ministère des Finances parce que nous avons choisi d'appliquer les mêmes règles que pour le ministère de la Défense nationale, à des fins d'harmonisation, même si les alliances qui entrent en ligne de compte ne sont pas les mêmes... Je veux dire, les Américains n'ont pas à nous dire comment nous devons protéger le ministère des Finances, alors que nous sommes alliés en ce qui concerne la défense.

M. Steve Drennan: Je ne crois pas que le manque d'uniformité soit un problème. Le véritable problème, c'est le temps. De nos jours, on peut perdre un an ou deux à attendre que les personnes clés puissent participer aux projets. Vous avez parfois besoin de connaissances informatiques précises, alors vous prenez un groupe de personnes... Je crois qu'il a déjà été question d'un processus accéléré; un témoin a déjà parlé de la possibilité de démarrer rapidement des carrières en cybersécurité et d'offrir aux gens des postes de débutant, entre autres choses. Si vous pouvez obtenir une autorisation de sécurité pour un groupe clé en choisissant des employés dignes de confiance provenant d'entreprises... parce que parfois, vous avez besoin d'experts en la matière venant des États-Unis, par exemple. Cela veut dire qu'il est essentiel que les autorisations de sécurité soient similaires et que le processus de contrôle soit rapide. Parfois, le problème est que nous perdons énormément de temps avec tous les différents contrôles de sécurité, et cela a des conséquences directes sur la défense nationale et sur d'autres groupes qui doivent attendre un an ou deux avant que leurs équipes puissent vraiment commencer leur travail. Le ministère des Finances n'a pas nécessairement besoin d'effectuer autant de contrôles de sécurité que le ministère de la Défense nationale, qui lui exige de remplir une demande de permis de visite pour chacune de ses installations, ce qui n'est pas le cas des autres organisations. Il faut cependant que les mêmes normes s'appliquent à tout le monde. Si les données dont il est question sont de nature très délicate, il faudrait tout de même que le processus de contrôle de sécurité soit le même pour tout le monde.

M. Matthew Dubé: Il me reste 20 secondes, et j'aimerais savoir si, selon vous, le Canada s'impose des restrictions excessives en se tournant uniquement vers nos alliés additionnels. Il y a des pays similaires au Canada qui ont peut-être les spécialistes dont nous avons besoin, mais parce qu'ils ne font pas partie du paradigme traditionnel, nous ratons une occasion d'en tirer parti.

M. Steve Drennan: Oui et non. Je crois qu'il y a beaucoup de spécialistes qui ont des autorisations de sécurité comparables dans le Groupe des cinq, mais, effectivement, nous devrions également prendre d'autres pays en considération. Nous devons penser à un processus de contrôle de sécurité rapide pour les autres pays afin de savoir que nous pouvons avoir confiance en ces gens et en leur information. Nous devons trouver une façon d'accélérer les choses.

Le président: Merci, monsieur Dubé. J'ai trouvé votre analyse très intéressante. Notre analyste m'a dit à l'oreille: « Un problème majeur est justement de réussir les contrôles de sécurité. »

Monsieur Picard, vous avez six minutes.

M. Michel Picard: C'est bon de vous revoir. Vous fournissez des services aux institutions financières, n'est-ce pas?

M. Steve Drennan: Oui.

M. Michel Picard: Pouvez-vous répéter votre commentaire à propos du fait que les institutions financières pourraient agir à titre d'entreprise de confiance pour conserver les renseignements critiques? Pouvez-vous préciser?

● (1710)

M. Steve Drennan: C'était l'un de mes points clés. Je n'ai pas eu le temps d'entrer dans le détail, alors je vous remercie de m'en donner l'occasion.

Quand nous allons à la banque, disons à la Banque du Canada, nous sommes tous sûrs qu'il s'agit d'une institution qui mérite la confiance, comme le ministère des Finances. On pourrait donc tirer parti de cela. Il a été question des mots de passe; quand vous entrez vos renseignements d'identification en ligne, vous devez avoir confiance dans le processus. Je crois qu'il faudrait tirer parti davantage de cet espace, de ces personnes et de ces organisations. Il serait possible de renforcer les mesures de sécurité relatives aux renseignements d'identification en ligne afin que ces organismes puissent jouer un rôle plus grand. L'uniformité pourrait être renforcée également. C'est une proposition clé: nous pouvons renforcer et uniformiser le processus d'identification afin de pouvoir l'utiliser à des fins de cybersécurité précises.

M. Michel Picard: Je ne sais pas si les gens seraient à l'aise de savoir qu'une banque conserve leurs renseignements de nature très délicate, au lieu que la banque ait simplement accès à une tierce partie qui, elle, serait responsable de conserver ces renseignements. Le client est en position de vulnérabilité, parce que même si la banque protège correctement ses renseignements, son objectif est non pas de protéger les renseignements, mais de faire de l'argent. Dans cette optique, le client n'est pas sur le même pied que la banque.

M. Steve Drennan: Principalement, l'institution financière jouerait le rôle d'une « autorité d'enregistrement ». La banque ne conserve pas nécessairement les données.

Je crois qu'on vous a déjà parlé de la tokenisation. Les données ne seront pas nécessairement conservées par la banque; plutôt, la banque agira comme instrument d'habilitation. Elle dira: « Vous êtes bien qui vous dites être. Nous le savons. Vous êtes venu à la banque. Nous vous faisons confiance, et vous avez confiance en nous. Nous avons vérifié vos données d'enregistrement. » Son rôle serait de soutenir le processus d'établissement de l'identité en ligne, et non de conserver les données.

M. Michel Picard: Plus tôt, vous avez approuvé très vivement les commentaires d'Amazon Web Services à propos d'une structure centralisée, un système du type iCloud, où tout serait au même endroit.

J'ai deux questions: premièrement, êtes-vous en faveur d'un système bancaire ouvert où toutes les données seraient conservées au même endroit?

Deuxièmement, j'ai l'impression que nous faisons tellement confiance à la sécurité des systèmes centralisés que nous ne pensons même pas à évoquer la possibilité d'un délit interne ou d'une erreur humaine. C'est comme si ce genre de choses n'existait plus.

M. Steve Drennan: Oui, je suis en faveur de l'utilisation d'un nuage public sécurisé. Non seulement cela nous donnerait énormément d'espace pour stocker les données, mais nous aurions aussi la possibilité de détecter correctement les attaques lorsqu'elles se produisent et de protéger les données très efficacement.

À propos de la protection des données, il y a énormément de mécanismes que l'on pourrait utiliser. Par exemple, il y a de bons produits en infonuagique qui vous permettent, à l'échelle locale, de crypter les données lorsque c'est nécessaire. Même en cas de menace interne et d'atteinte à la sécurité, les données volées seraient cryptées. Donc, les données sont protégées, parce que vous avez pris des mesures adéquates lorsque vous les avez stockées.

Trop souvent, les systèmes de sécurité ne sont pas conçus adéquatement, et les données ne sont pas protégées correctement lorsqu'il y a une atteinte à la sécurité. Nous ne sommes pas en mesure de détecter les menaces assez rapidement, et nous ne savons pas comment réagir. Pour répondre à votre question, s'il y a une menace interne, mais que nous nous sommes préparés en conséquence, les données seront protégées, nous pourrons détecter la menace rapidement et réagir.

Un exemple bien connu que je peux donner est le cas de M. Snowden. Il avait un accès très grand au système, et il a été en mesure d'accroître davantage son accès au système. Ce n'est pas le genre de modèle que vous voulez dans ce genre de contexte. Il y a de meilleurs modèles qui pourraient être mis en oeuvre.

M. Michel Picard: Je cède le reste de mon temps à M. Graham.

Le président: Monsieur Graham.

M. David de Burgh Graham: Merci.

Monsieur Drennan, pendant les trois minutes où M. Picard a posé des questions, je me suis connecté à un serveur et, grâce à un simple protocole SMTP, je me suis envoyé un courriel de la part de dieu@paradis.org. Cela me rappelle beaucoup ce dont nous avons discuté à propos du harponnage. Je me demande pourquoi nous utilisons encore des protocoles qui peuvent être aussi facilement piratés.

Le protocole SMTP ne demande absolument aucune authentification. Je peux utiliser n'importe quelle adresse courriel usurpée. Le protocole SSL du SMTP n'est pas universel; il n'empêche pas ce genre d'usurpation de courriel. Serait-il souhaitable, donc, d'imposer une norme PGP pour la signature des courriels? Y a-t-il des mesures que l'on pourrait prendre relativement au traitement cryptographique des signatures? Est-ce une approche que l'on devrait examiner?

Même si cela existe depuis 25 ans, pour une raison ou pour une autre, nous n'y avons pas adhéré massivement.

M. Steve Drennan: D'après mon expérience, c'est probablement parce que le système d'infrastructure à clés publiques est parfois trop complexe pour ce qui est de la délivrance des certificats. Nous ne pouvons pas être sûrs que les certificats délivrés sont corrects ou exclusifs.

La norme S/MIME a déjà été excellente, mais aujourd'hui, il y a de meilleures façons qui peuvent être mises en place pour vérifier les renseignements d'identification et pour délivrer des certificats numériques ou pour vérifier que l'expéditeur du message est bien qui il prétend être ou pour être sûr que le message n'a pas été modifié.

Ces technologies existent bel et bien. Ce serait une bonne idée d'en choisir une comme norme. Je ne sais pas si nous avons besoin de tous les éléments de l'infrastructure à clés publiques. Nous devons bien réfléchir au modèle de certificat numérique que nous voulons utiliser, parce qu'il y a énormément d'acteurs qui font partie du secteur financier.

● (1715)

M. David de Burgh Graham: Quel système d'authentification recommanderiez-vous? Les systèmes de messagerie électronique sont probablement les plus vulnérables, compte tenu du hameçonnage et de tout le reste. Que devrions-nous utiliser?

Vous-même, qu'utilisez-vous?

M. Steve Drennan: À dire vrai, nous utilisons de moins en moins les courriels, pour des raisons de productivité. Les courriels ne sont plus nécessairement utilisés pour les bonnes raisons. Il y a d'autres outils, comme Slack, qui sont plus efficaces pour mener des discussions.

Plus tôt, nous avons parlé de la sensibilisation des utilisateurs. Les gens doivent savoir comment utiliser les courriels et sur quoi cliquer. Simplement parce que tout est crypté, cela ne veut pas dire qu'une personne mal intentionnée ne peut pas vous envoyer un courriel crypté, alors on retourne à la case départ.

Il y a d'autres possibilités. Une option serait de créer un portail unique duquel on pourrait télécharger des courriels sécurisés. Le cryptage qui limite la durée de vie: lorsque vous envoyez un message crypté, le message disparaît au bout d'un certain temps s'il n'est pas ouvert.

Il y a des options intéressantes.

M. David de Burgh Graham: Comme une signature numérique utilisant une clé.

Le président: Merci, monsieur Graham.

Il nous reste quatre minutes. Y a-t-il des questions de la part du Parti conservateur?

Monsieur Eglinski, prenez-vous les quatre minutes?

M. Jim Eglinski: Vous parliez de sécurité avec M. Dubé. Votre entreprise travaille avec de nombreux organismes gouvernementaux, et j'aimerais savoir quelle autorisation de sécurité est exigée pour vos employés? Doivent-ils avoir une autorisation de sécurité secret » ou « très secret »?

M. Steve Drennan: Les membres de notre équipe de cybersécurité ont dû obtenir énormément d'autorisations de sécurité. Nous pouvons détenir et traiter des renseignements classés très secret. Nous travaillons dans des environnements classifiés. Nous avons tous une autorisation de sécurité très secret ainsi que les autorisations de sécurité supplémentaires dont nous venons de parler. C'est nécessaire, si nous voulons décrocher les contrats dont nous avons parlé plus tôt. Nous savons que c'est obligatoire. Cela a aussi une incidence sur les personnes que nous pouvons embaucher, car même si nous cherchons à avoir le maximum de diversité au sein de notre personnel, cela entraîne parfois des difficultés. Une chose est certaine, cependant, c'est que nous avons tous une autorisation de sécurité très secret. Il y a également...

M. Jim Eglinski: Vous ne semblez pas être tout à fait d'accord. Je crois qu'il y a beaucoup de... J'ai déjà mené des enquêtes classées très secret pour des contrôles de sécurité, et il y a énormément de choses à vérifier. Croyez-vous que nous devrions abaisser notre niveau d'exigence ou nos normes?

M. Steve Drennan: Non, mais il faudrait que ce soit plus uniforme.

M. Jim Eglinski: Plus uniforme?

M. Steve Drennan: Il faudrait que tous les ministères fédéraux utilisent le même processus de contrôle de sécurité. Si une entité ou une personne est autorisée à accéder à une certaine classe d'information, jusqu'à une certaine limite, l'autorisation devrait être valide à grande échelle. Ce n'est pas nécessaire d'avoir des autorisations de sécurité différentes pour chaque organisme au Canada.

M. Jim Eglinski: Je crois qu'il n'y a aucune norme qui impose des critères nationaux à respecter pour pouvoir accéder à une certaine classe d'information.

M. Steve Drennan: Vous avez raison.

M. Jim Eglinski: D'accord.

Rapidement, j'ai une dernière question. Il doit me rester environ deux minutes, n'est-ce pas?

Le président: Oui.

M. Jim Eglinski: Vous avez brièvement parlé d'intelligence artificielle. Je me suis penché sur le sujet pendant les études de deux ou trois autres comités. Croyez-vous que l'intelligence artificielle, à un moment donné, arrivera à obtenir de meilleurs résultats en matière de cybersécurité que nous en sommes capables présentement?

M. Steve Drennan: Je crois que ce qui est intéressant avec l'intelligence artificielle — si nous avons la chance, les choses ne finiront pas comme dans les films, les navets que nous connaissons —, c'est qu'elle peut fournir du soutien aux spécialistes. C'est de cette façon qu'elle est utilisée présentement. Disons que vous avez un centre des opérations de sécurité, et que vous avez énormément de difficulté à recruter et à former des spécialistes, puis à les maintenir en poste. Même si vous en avez très peu, le travail peut être beaucoup plus facile si on réduit les ensembles de données à traiter et qu'on prend des décisions à l'avance. Il suffit donc d'entrer ce genre de données, et ce sera beaucoup plus facile pour vous ensuite de prendre des décisions clés. L'intelligence artificielle doit être considérée comme un assistant numérique qui est là pour vous aider à traiter les téraoctets de données et ainsi de rendre votre travail plus facile et plus ciblé. Je crois que c'est la meilleure façon de voir l'apprentissage machine en informatique.

M. Jim Eglinski: Vous ne pouvez quand même pas trop lui en donner.

M. Steve Drennan: Vous pouvez tout lui donner; évitez simplement de lui laisser toutes les décisions.

Le président: Au nom du Comité, je veux remercier M. Drennan. Nous avons eu une séance tout à fait fascinante. Nous avons aussi discuté de choses que M. Graham est probablement le seul à avoir compris.

M. Steve Drennan: Merci.

Le président: Merci encore.

Chers collègues, les travaux du Sous-comité débuteront dans deux minutes.

La séance est levée.