CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 151 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 27 février 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 27 février 2019

● (1550)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Mesdames et messieurs, je vous prie d'excuser mon retard. Je présentais les 31e et 32e rapports du comité des prévisions budgétaires.

Je présente également mes excuses à nos témoins pour le changement d'emplacement. Il semble qu'il se passe quelque chose aujourd'hui sur la Colline. Ceux qui ne suivent pas cela sont en train de regarder CNN. Je m'attends donc à ce que notre séance d'aujourd'hui soit éclipsée par tout cela.

Chers collègues, je propose que nous repoussions la fin de notre séance. Nos témoins sont venus de loin pour comparaître aujourd'hui. Un témoin s'est décommandé, alors nous avons fusionné les deux heures...

Avons-nous fusionné les deux heures? Je ne vois pas l'autre témoin.

Le greffier du comité (M. Naaman Sugrue): Nous pourrions simplement les faire intervenir...

Le président: Lorsqu'ils arriveront, d'accord...

Nous allons donc respecter le déroulement habituel, mais la forme de notre présentation d'aujourd'hui pourra prendre une forme plus souple.

Je vois que M. O'Higgins et Michele Mosca de Quantam-Safe Canada sont présents, tout comme M. Parsons de Citizen Lab. Bienvenue.

Nous allons commencer par les exposés de 10 minutes de chaque équipe. Ensuite, nous passerons à la période habituelle de questions et réponses.

Les témoins de Quantam-Safe ont la parole pour les 10 prochaines minutes.

M. Michele Mosca (directeur, Quantum-Safe Canada): Merci.

Monsieur le président, chers membres du Comité, bonjour. Je m'appelle Michele Mosca, et je suis professeur de mathématiques et de cryptographie à l'Institut d'informatique quantique de l'université de Waterloo.

[*Français*]

C'est pour moi un honneur de vous adresser la parole aujourd'hui.

[*Traduction*]

Lorsque j'ai commencé ma carrière de chercheur à Waterloo et à Oxford, je me disais que, dans quelques dizaines d'années, mes domaines de recherche allaient avoir beaucoup d'importance dans le monde et offrir au Canada des possibilités économiques considérables. Vingt-cinq ans plus tard, place au spectacle.

Il va sans dire que le Canada devrait être proactif de manière à saisir les possibilités de prospérité économique considérables qui découlent des dizaines d'années de travail et des milliards de dollars que nous avons investis pour faire du pays un chef de file mondial des technologies quantiques. Toutefois, avant de déployer les incroyables puissances des technologies quantiques, nous avons la responsabilité d'assurer notre sécurité dans un monde animé par ces technologies. Pour l'heure, nous sommes extrêmement vulnérables. Je vais vous expliquer rapidement ce que j'entends par là.

Premièrement, notre économie est tributaire des technologies numériques, technologies dont la sécurité repose sur la cryptographie. On sait que la cryptographie permet d'assurer la confidentialité des transactions financières et la protection de la propriété intellectuelle. C'est aussi grâce à la cryptographie que nos appareils déterminent à qui l'on peut — ou à qui l'on ne peut pas — faire confiance lors de nos transactions sur Internet. Par exemple, il s'agit de s'assurer que l'on télécharge des mises à jour légitimes pour nos logiciels et non pas des logiciels malveillants. Lorsque vous transférez de l'argent à votre banque, vous voulez être certain qu'il s'agit bel et bien de votre banque et non pas d'une imitation. Le bon fonctionnement de notre économie numérique, laquelle est presque devenue synonyme d'économie tout court, est impossible sans une cryptographie robuste.

Dans un instant, je vous expliquerai en quoi l'informatique quantique menace tout cela, mais auparavant, j'aimerais mettre en lumière l'une des plus grandes difficultés qui se présentent à nous. Étant donné que le problème risque d'apparaître dans 10 ans ou plus, l'être humain a naturellement tendance à ne pas en tenir compte dans le moment présent. Cependant, si l'on continue à rester inactif jusqu'à ce que la situation devienne une crise, cela aura des conséquences dévastatrices sur notre sécurité et notre économie.

Tout d'abord, il nous faudra plus de 10 ans pour préparer notre économie et nos systèmes essentiels contre les attaques quantiques. Il s'agit de modifier nos outils de façon fondamentale. Il ne s'agit pas de s'occuper de simples correctifs et de mauvais mots de passe. Il n'existe pas de solution rapide. On parle ici d'un effondrement systémique contre lequel aucune mesure corrective n'a été instaurée.

Ensuite, il est possible qu'une perte de confiance à l'égard de notre cyberrésilience, ainsi que de la résistance de notre économie à de tels effets, se produise beaucoup plus tôt, possiblement au cours des deux à cinq prochaines années, à mesure que l'informatique quantique franchit les étapes importantes de son développement. En soi, la menace quantique est simple. On n'a pas besoin de connaître l'équation de Schrödinger pour la comprendre. L'ordinateur quantique est un nouveau type d'ordinateur puissant qui sera à même d'effectuer des calculs jusque-là impossibles. Cependant, cet ordinateur va aussi anéantir la cryptographie actuellement en usage. Il faudra s'occuper de ce problème si l'on veut que l'avènement de l'ordinateur quantique représente un événement positif dans l'histoire du Canada et, plus généralement, dans l'histoire de l'humanité.

On peut énumérer quatre conséquences sur notre secteur financier et sur notre économie. Primo, le secteur des services financiers subira une attaque directe: vol d'argent, entraves aux activités légitimes, perte de confiance dans le secteur financier canadien. Secundo, il y aura des cyberattaques contre d'autres secteurs de notre économie, secteurs dans lesquels nous investissons beaucoup d'argent: on pense surtout aux infrastructures essentielles comme les services gouvernementaux, l'électricité et d'autres services publics, les systèmes de transport et les villes intelligentes. Tertio, on assistera au vol de la propriété intellectuelle stratégique protégée par une cryptographie vulnérable à l'informatique quantique. Quarto, les emplois canadiens actuels et à venir subiront des perturbations dans les secteurs qui produisent ou utilisent des technologies vulnérables aux attaques quantiques et n'ont pas de plan pour assurer la sécurité quantique.

Ce sont là quatre risques distincts et très sérieux qui planent sur le secteur des services financiers et sur notre économie dans son ensemble.

Nous connaissons la nature de la menace. Nous avons une bonne idée des outils dont nous aurons besoin et de l'usage que nous devrons en faire pour nous protéger contre ces quatre risques qu'encourt notre économie. Ce n'est pas un exercice théorique. L'espèce humaine ne fait pas toujours preuve des qualités que la situation actuelle réclame. Nous devons travailler ensemble dans plusieurs ministères et dans plusieurs secteurs; personne ne peut faire cela tout seul. Nous devons travailler de façon proactive, en nous y mettant le plus tôt possible.

C'est très difficile. Cela dit, il y a éventuellement un aspect positif pour les citoyens, à savoir que le Canada est un chef de file mondial en science quantique, en cryptographie, en cryptographie résistante aux attaques quantiques — c'est-à-dire en cryptographie conçue pour se protéger contre les attaques quantiques dans la cybersécurité et les services financiers. Si nous ne saisissons pas l'occasion qui se présente, nous n'aurons que nous-mêmes à blâmer.

Compte tenu de notre envergure et de nos ressources, nous devrions être en mesure d'agir assez rapidement pour déployer de nouveaux outils résistants aux attaques quantiques et pour former la main-d'oeuvre nécessaire.

● (1555)

Si nous nous en occupons de façon proactive, la menace quantique peut être transformée en une situation positive offrant de belles possibilités économiques pour le Canada. Nous savons comment faire pour assurer notre sécurité quantique. Nous pouvons passer à l'action, puis exporter nos outils et notre savoir-faire quantiques.

Si, au contraire, suivant notre nature humaine, nous agissons de façon réactive, nous serons vulnérables aux attaques quantiques. Nous serons également vulnérables aux attaques banales qui ont cours actuellement et qui exploitent les failles qui proviennent de notre gestion de crise précipitée. Nous importerons, possiblement par le biais d'une porte dérobée, la mise en oeuvre de nos propres innovations. Voilà ce qui va se produire si nous gérons la situation de façon réactive. Si nous ne sommes pas proactifs, les nouvelles possibilités dans lesquelles nous avons investi pendant des dizaines d'années nous échapperont et une grande portion de notre économie, dans sa forme actuelle, sera en danger.

Voici, pour finir, nos recommandations à l'intention du Comité.

Premièrement, je vous prie d'exhorter le gouvernement à agir rapidement pour mettre en place les éléments nécessaires pour que le Canada devienne un pays résistant aux attaques quantiques sur le double plan de la technologie et des ressources humaines. Pour ce faire, il s'agit notamment d'appuyer la recherche ciblée sur la cryptographie résistante aux attaques quantiques, le déploiement d'un réseau canadien de distribution quantique de clés cryptographiques — une invention canadienne, soit dit en passant —, les systèmes de fibre optique et de réseaux satellitaires et la création d'un bassin d'experts dans le domaine de la cybersécurité axée sur les attaques quantiques.

Deuxièmement, je vous demande d'exhorter le gouvernement à utiliser les leviers stratégiques qui sont à sa disposition, y compris les pouvoirs d'approbation, de planification, d'approvisionnement et de financement, pour faire en sorte que la nouvelle infrastructure numérique soit conçue et construite de façon à être résistante aux attaques quantiques; il faut éviter d'attendre que cette infrastructure soit détruite par les nouveaux ordinateurs quantiques. En résumé, il faut stimuler la technologie et la main-d'oeuvre nécessaires pour que le Canada et la planète puissent résister aux attaques quantiques.

Pour que tout cela fonctionne, un effort proactif et multisectoriel est nécessaire — comme je l'ai dit, aucun groupe ne saurait faire cavalier seul. Ainsi, troisièmement, je vous prie d'exhorter le gouvernement à fournir un financement approprié à une entité sans but lucratif comme la nôtre, Quantum-Safe Canada, pour aider à coordonner les multiples aspects du travail qui doit être accompli pour que le Canada puisse mettre en oeuvre une stratégie efficace dans le domaine de la sécurité quantique.

[*Français*]

Je vous remercie de votre attention.

[*Traduction*]

J'inviterais mon collègue Brian O'Higgins à utiliser le temps qu'il me reste pour vous dire quelques mots. Il est le président de Quantum-Safe Canada. C'est aussi un cryptographe et un entrepreneur en sécurité de renommée internationale.

Le président: Vous avez environ deux minutes et demie.

M. Brian O'Higgins (président, Quantum-Safe Canada): Merci.

Je travaille dans le domaine de la cybersécurité depuis plus de 30 ans, je crois. La guerre entre les bons et les méchants n'a pas de fin. Il semble que les méchants soient en train de gagner et, avec la menace quantique qui plane au-dessus de nos têtes, le secret de l'un des outils les plus importants dont disposent les bons, c'est-à-dire le chiffrement, est sur le point d'être percé.

C'est vraiment un gros problème. C'est une question de sécurité. Nous savons que lorsque nous laissons le champ libre au secteur privé et aux forces du marché, la gestion n'est pas toujours aussi bonne qu'elle pourrait l'être.

Si le gouvernement encourageait l'industrie à aller dans la bonne direction, ce pourrait être très utile. Dans ce cas-ci, certaines des solutions aux problèmes dont nous parlons résident dans des expertises canadiennes de classe mondiale. Si nous agissons d'abord à l'échelle nationale, nous serons en bonne posture dans le marché d'exportation mondial.

Le président: Merci beaucoup.

Monsieur Parsons, vous avez sept minutes.

M. Christopher Parsons (associé en recherche, Munk School of Global Affairs and Public Policy, University of Toronto, Citizen Lab): Bonjour.

Je m'appelle Christopher Parsons. Je suis associé en recherche au Citizen Lab de la Munk School of Global Affairs and Public Policy de l'université de Toronto. Je comparais devant le Comité à titre professionnel afin d'exprimer mes opinions et celles du Citizen Lab.

Mon exposé d'aujourd'hui porte sur un éventail de pratiques de sécurisation qui, si elles étaient adoptées, atténueraient certains des risques auxquels sont confrontés actuellement les acteurs du secteur financier.

Les organismes gouvernementaux canadiens, les entreprises privées, les institutions financières et les particuliers comptent sur des infrastructures informatiques courantes. Nous utilisons les mêmes systèmes d'exploitation iPhone et Android, les mêmes interfaces de service à la clientèle et les mêmes plateformes de commerce électronique, les mêmes bases de codes sous-jacentes et les mêmes infrastructures d'informatique en nuage provenant de tiers.

Cette mise en commun des plateformes peut accroître la productivité et l'efficacité, mais ces avantages sont tributaires de la sécurité globale de ces produits mis en commun. Pour être franc, l'état d'insécurité informatique est grave. Un grand nombre de vulnérabilités dans ces produits mis en commun, dans l'ensemble, menacent le secteur financier au détriment des intérêts du Canada en matière de sécurité nationale.

J'aimerais utiliser le temps qu'il me reste pour attirer votre attention sur quatre enjeux en particulier, enjeux auxquels nous devons nous attaquer pour que les intérêts nationaux du Canada soient mieux protégés à l'avenir. Ces enjeux comprennent la nécessité pour le Canada d'établir officiellement une politique nationale de chiffrement responsable, de mettre à jour les programmes d'équité en matière de vulnérabilité du Canada, d'élaborer un cadre de programme de divulgation des vulnérabilités et de promouvoir l'authentification à deux facteurs.

Je commence par la question des politiques de chiffrement responsable. Compte tenu de l'état d'insécurité informatique, il est impératif que le gouvernement du Canada adopte et préconise des politiques responsables de chiffrement. Ces politiques impliquent des engagements à préserver le droit de tous les groupes au Canada d'utiliser des logiciels à l'aide d'un chiffrement fort.

Un chiffrement fort peut largement être défini comme des algorithmes de chiffrement pour lesquels aucune faiblesse ou vulnérabilité n'est connue ou n'a été intégrée, ainsi que des applications informatiques qui ne contiennent pas délibérément des faiblesses visant à miner l'efficacité des algorithmes susmentionnés.

On ne saurait trop insister sur les avantages d'un chiffrement fort. Dans un environnement technologique marqué par des enjeux financiers élevés, une grande interdépendance et une complexité extraordinaire, il est extrêmement important et difficile d'assurer la sécurité numérique. Les coûts liés à une atteinte à la sécurité, à un vol ou à la perte de données de clients ou d'entreprises peuvent avoir des répercussions dévastatrices sur les intérêts du secteur privé et les droits des particuliers. Toute faiblesse dans les systèmes mêmes qui nous protègent contre ces menaces constituerait une politique irresponsable. L'accès à un chiffrement fort encourage les consommateurs à croire que la technologie qu'ils utilisent est sûre.

Il faut reconnaître qu'il y a des risques associés à la disponibilité d'un chiffrement fort. À titre d'exemple, l'un des plus proches alliés du Canada, l'Australie, a adopté des politiques de chiffrement irresponsables qui risquent d'introduire des vulnérabilités systémiques dans les codes utilisés par le secteur financier, ainsi que par d'autres éléments de l'économie. Une fois introduites, ces vulnérabilités pourraient être exploitées par des acteurs qui ont des intérêts contre le Canada ou l'économie canadienne. Par exemple, le réseau SWIFT pourrait être la cible d'activités de menaces si un élément de ce réseau reposait sur des produits cryptographiques rendus vulnérables par les demandes australiennes.

De plus, grâce à un chiffrement fort, on empêche les plus proches alliés du Canada de surveiller les activités financières du pays au-delà des mécanismes de surveillance convenus, comme le CANAFE.

Par exemple, le *Globe and Mail* a révélé que la National Security Agency — NSA — des États-Unis surveillait les tunnels du réseau privé virtuel de la Banque Royale du Canada. L'article laisse entendre que les activités de la NSA pourraient constituer une étape préliminaire d'efforts plus vastes visant « à déterminer, à étudier et, au besoin, à "exploiter" les réseaux de communication internes des organisations ».

Compte tenu de ces menaces, nous suggérons que le gouvernement du Canada adopte une politique de chiffrement responsable. Une telle politique exigerait un engagement ferme et peut-être législatif afin d'exiger que tous les secteurs de l'économie aient accès à des produits de chiffrement forts; elle s'opposerait également à des politiques de chiffrement irresponsables, comme celles qui préconisent les portes dérobées.

Je passe maintenant à la gestion des vulnérabilités informatiques du gouvernement du Canada lui-même. Les vulnérabilités des codes informatiques sont recueillies par le Centre de la sécurité des télécommunications du Canada — CST. Par la suite, le CST détermine s'il y a lieu de conserver ou de divulguer les vulnérabilités. Le CST est motivé à conserver des vulnérabilités pour avoir accès à des systèmes étrangers dans le cadre de son mandat de renseignements électromagnétiques, ainsi qu'à divulguer certaines vulnérabilités afin de mieux protéger les systèmes gouvernementaux.

À ce jour, le CST a refusé de rendre public le processus d'équité précis qu'il utilise pour déterminer s'il doit conserver ou divulguer les vulnérabilités. En revanche, les États-Unis publient la façon dont tous les organismes du gouvernement fédéral doivent évaluer l'existence d'une vulnérabilité, la retenir ou la divulguer.

Les réserves de vulnérabilités du CST pourraient être découvertes et utilisées par des adversaires. C'est ce qui est arrivé à la National Security Agency et à la Central Intelligence Agency aux États-Unis. Les conséquences peuvent entraîner des dommages économiques directs de milliards de dollars.

● (1600)

La présence continue de ces réserves et le manque de clarté au sujet des vulnérabilités qui demeurent dans les entreprises et chez les particuliers ont ébranlé la confiance dans la fiabilité et la sécurité des produits nécessaires pour améliorer l'efficacité et la productivité économiques du Canada. Éventuellement, cela aura aussi ralenti l'adoption, par les Canadiens, de plateformes et d'infrastructures logicielles actuelles et à venir.

Pour dissiper ces préoccupations, nous suggérons que le gouvernement canadien diffuse ses programmes actuels d'équité en matière de vulnérabilités et tienne des consultations sur l'efficacité de ceux-ci à protéger les logiciels et équipements utilisés dans le cadre d'activités financières. De plus, le gouvernement pourrait inclure des intervenants du milieu des affaires et de la société civile dans le programme — actuel ou mis à jour — d'équité en matière de vulnérabilités. L'inclusion de ces intervenants favoriserait une divulgation accrue des vulnérabilités, ce qui aurait pour effet d'accroître la disponibilité de logiciels bien rédigés et de réduire les menaces qui planent sur le secteur financier.

Il est également important de reconnaître que les chercheurs en sécurité découvrent régulièrement des vulnérabilités dans le matériel et les logiciels utilisés dans tous les milieux, y compris dans le secteur financier. Toutefois, relativement peu d'organisations ont des procédures explicites qui guident les chercheurs dans la façon de divulguer de façon responsable ces vulnérabilités aux entreprises touchées. La divulgation des vulnérabilités informatiques en l'absence d'un programme de divulgation peut amener les entreprises à menacer les chercheurs éthiques en sécurité informatique d'intenter indûment des poursuites contre eux. Ces risques réduisent la volonté des chercheurs de divulguer les vulnérabilités.

En plus de l'étude des lois entourant l'accès non autorisé au code informatique, je recommanderais que le Comité et le gouvernement établissent une ébauche de politique que les entreprises du secteur financier pourraient adopter. Une telle politique de divulgation devrait déterminer les personnes à qui les vulnérabilités sont signalées, la manière dont les rapports sont traités en interne et le temps qu'il faudra pour corriger une vulnérabilité. Cette politique devrait également stipuler que les chercheurs en sécurité ne peuvent être tenus responsables tant qu'ils ne divulguent pas publiquement la vulnérabilité avant la fin de la période établie. De plus, le gouvernement devrait élaborer et adopter un programme de divulgation semblable pour ses propres ministères afin de tirer avantage des signalements des vulnérabilités des systèmes gouvernementaux par les chercheurs.

Enfin, je passe à la question de l'authentification à deux facteurs, c'est-à-dire au fait qu'une personne doit être en possession d'au moins deux facteurs pour obtenir l'accès à son compte. Les facteurs les plus généralement utilisés pour l'authentification comprennent quelque chose que vous connaissez — par exemple, un NIP ou un mot de passe —, quelque chose que vous avez — par exemple, un jeton matériel ou un jeton produit par un logiciel — ou quelque chose que vous êtes — de la biométrie, par exemple le balayage d'une empreinte digitale ou de l'iris. Grâce à ces facteurs multiples, le fait de perdre son nom d'utilisateur et son mot de passe n'ouvre pas forcément l'accès à des tiers qui voudraient pénétrer dans un système ou un stock de données protégé.

Il est important que les systèmes d'ouverture de session destinés aux clients intègrent un solide processus d'authentification à deux facteurs afin d'empêcher des tiers non autorisés d'accéder à des comptes financiers personnels. Un tel accès peut mener à une meilleure analyse pour savoir si des personnes pourraient être ciblées par un adversaire étranger à des fins de recrutement d'espionnage, causer des situations financières personnelles chaotiques afin de distraire une personne pendant qu'une autre activité informatique est entreprise, ou transférer de l'argent à des parties inscrites à des listes de surveillance de terroristes ou de criminels.

Il est vrai que certaines institutions financières canadiennes offrent l'authentification à deux facteurs, mais le processus généralement utilisé par défaut pour l'authentification du second facteur est faible; il repose sur les messages texte. Cette situation est problématique, car les messages texte sont un médium de communication faible qui peut facilement être contourné par divers moyens. C'est pourquoi des entités comme le National Institute of Standards and Technology des États-Unis ne recommandent plus les messages texte dans le cadre de l'authentification à deux facteurs.

Pour améliorer la sécurité des comptes destinés à la clientèle, je recommanderais que les institutions financières soient tenues d'offrir l'authentification à deux facteurs à tous les clients et, en outre, qu'un tel processus d'authentification utilise des jetons matériels ou logiciels. La mise en œuvre de cette recommandation réduira le risque que des parties non autorisées obtiennent l'accès à des comptes à des fins d'activités de recrutement ou de perturbation.

En conclusion, les entreprises et les particuliers canadiens comptent sur les outils numériques pour tous les aspects de leur vie, y compris les activités qui recoupent le secteur financier. Je tiens à dire que les propositions que j'ai formulées ne régleront pas tous les problèmes liés à la sécurité informatique qui menacent le secteur financier et les intérêts du Canada en matière de sécurité nationale, mais nous croyons qu'elles représentent un pas dans la bonne direction pour contrer les menaces principales. Ces propositions permettraient aussi de renforcer la confiance envers la sécurité de nos outils numériques et la gouvernance en matière de sécurité.

Merci d'avoir pris le temps de m'écouter. Je serai ravi de répondre à vos questions.

● (1605)

Le président: Merci, monsieur Parsons.

Madame McCrimmon.

Mme Karen McCrimmon (Kanata—Carleton, Lib.): Merci beaucoup.

J'aimerais commencer par vous dire merci à tous d'être ici aujourd'hui. Vous avez beaucoup contribué à notre discussion.

Je commencerai par MM. Mosca et O'Higgins. J'ai été ravie de vous entendre parler de la nécessité d'une collaboration. Pouvez-vous nous parler un peu des relations et des réseaux qui existent entre le milieu universitaire, le secteur privé et le gouvernement? Ces liens fonctionnent-ils bien? Y a-t-il des failles que nous devrions chercher à colmater?

M. Michele Mosca: Les universitaires forment une communauté très unie. Nous nous connaissons les uns les autres. Dans la sous-discipline particulière dont il est question ici, nous avons réussi à obtenir une bonne participation. En plus de la recherche de pointe que chacun d'entre nous accomplit séparément, nous étions tous désireux de collaborer et de travailler ensemble pour avoir une incidence positive à l'échelle nationale et internationale.

Il y a des occasions de rencontre pour les gens venant de deux milieux différents; les rencontres réunissant des gens des trois milieux sont plutôt rares. Cela dit, deux fois par année, nous organisons un symposium — dans lequel on met l'accent sur la cybersécurité — avec une quarantaine de personnes qui sont des leaders d'opinion des trois milieux. La question quantique n'est qu'un aspect de cette discussion. Nous discutons du rôle du Canada en tant que chef de file en matière de cybersécurité, de la façon dont nous pouvons accomplir des progrès et travailler ensemble. Nous établissons de bons rapports. Cette rencontre demeure plutôt modeste et ponctuelle. Je pense que nous devrions être plus entreprenants dans l'organisation de ce genre d'activité axée sur le bien et sur la mission de notre travail.

Brian, voulez-vous ajouter quelque chose?

● (1610)

M. Brian O'Higgins: Je pense que vous avez bien cerné le problème. La collaboration entre les trois milieux — le gouvernement, le secteur privé et le milieu universitaire — est presque sans précédent. Le symposium sur la cybersécurité que Michele organise est à peu près le seul exemple du genre que je connaisse. Le gouvernement y participe très peu, mais c'est un début. Le fait d'encourager ce type de symposium et d'y porter une attention particulière serait certainement utile.

Mme Karen McCrimmon: Dans la même veine, que devons-nous faire pour encourager cela? De plus, est-ce que c'est nous qui manquons à l'appel? Comment faire pour encourager les autres à participer à ces discussions?

M. Michele Mosca: Je me dois aussi de mentionner nos collègues du Réseau intégré sur la cybersécurité, le SERENE-RISC. La personne qui est à la tête de SERENE-RISC siège également à notre conseil d'administration. Voilà un autre lieu de rencontre qui comprend un certain nombre d'ateliers et réunit divers intervenants.

Il y a très peu d'organismes comme SERENE-RISC et Quantum-Safe Canada qui ne s'en tiennent pas à... Le problème avec la cybersécurité, c'est que nous sommes tous trop sollicités. Nous sommes très occupés. Chaque fois que nous décidons de faire quelque chose, nous laissons de côté d'autres choses qui sont vraiment importantes. Nous n'avons pas le temps de nous ennuyer. Nous n'avons pas décidé de nous attaquer à la menace quantique pour passer le temps. Nous sommes beaucoup trop occupés par beaucoup trop de choses. Il faut des encouragements. Par exemple, le travail ingrat que font Benoit et le réseau SERENE-RISC... Ils ne reçoivent presque pas d'argent et, pourtant, ils continuent leur travail extraordinaire. Selon moi, il faut encourager ces gens, les soutenir et leur dire merci.

C'est une question de financement, entre autres. Lorsque l'on est professeur et que l'on emploie le mot « financement », les gens supposent que l'on veut plus d'argent pour la recherche autonome. À cet égard, nous sommes déjà très bien servis au Canada. Je parle ici d'un soutien très ciblé et axé sur la mission en question afin d'atteindre ces objectifs très importants pour le Canada et de travailler à rebours à partir de là.

Il existe un petit groupe de personnes dévouées, disséminées à travers le pays, qui pourraient nous aider. Il faut encourager ces personnes de façon proactive. À l'heure actuelle, on leur dit qu'elles doivent continuer de défendre leur mission, mais elles n'ont ni le temps ni les ressources pour ce faire. Les citoyens canadiens doivent reconnaître leur valeur et leur apport, les encourager à continuer leur excellent travail et les aider à en faire plus.

Par ailleurs, je considère que nous ne sommes pas assez nombreux. Pour renforcer l'état-major dans le domaine et faire en sorte que le Canada soit capable de survivre — simplement survivre — dans le cybermonde dans 10 ans, nous avons besoin de capital intellectuel et de main-d'oeuvre. Nous sommes très en retard. Il y a 2 ou 5 ans, j'ai dit que, à moins d'ajouter 20 postes ciblés dans le domaine de la cybersécurité, dont au moins 5 dans le domaine des sciences sociales et humaines — une composante très importante —, nous n'aurions aucune chance de nous défendre 10 ans plus tard.

Sans surprise, le chiffre que je vois circuler actuellement est 50: nos amis en Allemagne parlaient d'environ 50 postes de professeurs dans le domaine de la cybersécurité appliquée à Saarbrücken et je ne sais combien d'autres à l'institut Max Planck. On parle de plus de 200 postes de professeurs dans ce domaine ciblé, parce que c'est vraiment important pour l'économie et la sécurité de l'Allemagne. Au Canada, il n'y a aucun nouveau poste — pas même dans le contexte des CERC ou de Canada 150. Rien. Je pense qu'il y a un énorme rattrapage à faire pour renforcer l'état-major dans ces domaines ciblés.

Mme Karen McCrimmon: D'accord.

Le président: Il vous reste une minute.

Mme Karen McCrimmon: Je vais vous poser ma dernière question en espérant que nous aurons l'occasion d'en discuter tout à l'heure.

Monsieur Parsons, vous avez parlé de politiques de chiffrement responsable. Y a-t-il un modèle en la matière? Y a-t-il un pays qui a de bonnes politiques? Vous pouvez aborder ce sujet ainsi que celui des programmes de vulnérabilité.

M. Christopher Parsons: Je pense qu'actuellement, il y a des difficultés au sein du Groupe des cinq composé du Canada, des États-Unis, de la Nouvelle-Zélande, de l'Australie et du Royaume-Uni.

En dehors du champ de l'application de la loi, les États-Unis ont manifesté un vif désir d'appuyer un chiffrement solide. La National Security Agency, la Central Intelligence Agency et, à vrai dire, toutes les parties à l'exception du FBI, sont d'ardents défenseurs d'un chiffrement solide et indéfectible à des fins de renseignement, parce qu'elles en ont besoin dans leurs propres activités. Ainsi, nous pouvons, selon moi, nous inspirer des services de renseignement de notre allié au sud de la frontière.

En ce qui concerne les programmes de divulgation des vulnérabilités, certaines entreprises possèdent de bons modèles à cet égard. Aux États-Unis, HackerOne a travaillé avec le département de la défense. Aussi, récemment, une mesure législative a été sinon adoptée, du moins débattue, mesure qui autoriserait les programmes de divulgation des vulnérabilités à englober le département d'État.

C'est ainsi que cela fonctionne au gouvernement, il me semble. C'est une initiative solide et positive grâce à laquelle d'importantes vulnérabilités sont corrigées. On constate également que, grâce à HackerOne, un grand nombre d'entreprises privées adoptent petit à petit des programmes de divulgation plus englobants. Dans les deux cas de figure, l'infrastructure du gouvernement et l'infrastructure de l'entreprise sont sécurisées, et ce, pour un coût souvent modique.

● (1615)

Le président: Merci, madame McCrimmon.

Monsieur Motz, vous avez sept minutes.

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

Merci de votre présence, messieurs.

Mes premières questions s'adressent à M. Mosca et à M. O'Higgins.

Un des témoins ayant comparu devant le Comité a dit n'avoir absolument pas confiance en la capacité du Canada à affronter les problèmes de cybersécurité. Quelle est la somme de travail que nous devons encore accomplir pour que nos systèmes gouvernementaux soient protégés contre une attaque de ce genre?

M. Michele Mosca: Voulez-vous commencer?

M. Brian O'Higgins: Je n'irai pas jusqu'à dire que nous ne sommes pas du tout préparés. En fait, dans le domaine, le Canada a bonne réputation. Le gouvernement fédéral canadien représente environ un dixième de la taille du gouvernement fédéral des États-Unis, par exemple. Sa taille est presque celle d'un ministère américain. S'il y a un effort ciblé pour se concentrer sur la cybersécurité, nous occuperons une meilleure position dans le domaine, ce qui est très bien.

Dans le secteur financier, quelques grandes banques canadiennes jouissent généralement d'une excellente réputation et sont des modèles positifs à l'international. Elles pourraient en faire beaucoup plus, certes, mais c'est un bon point de départ. Nous sommes plutôt... J'ai participé à des activités liées à la cybersécurité dans une cinquantaine de pays et je peux vous dire que les Canadiens sont toujours bien accueillis lorsqu'il s'agit de parler de technologie et des actions de notre gouvernement et de nos entreprises.

M. Michele Mosca: À mon avis, nous disposons de tous les éléments de base pour avoir du succès dans ce domaine. En revanche, nous n'avons pas de plan pour assembler ces éléments et en tirer parti.

M. Glen Motz: Le témoin dont je parlais partageait les mêmes doutes à l'égard de l'assemblage des différents éléments.

M. Michele Mosca: Il me semble que le plan de match nous échappe. La création d'un centre de cybersécurité est une excellente première étape, mais il y a simplement... La rondelle était derrière notre filet. Maintenant, nous sommes en train de patiner vers notre propre ligne bleue. Nous sommes trop loin du filet pour gagner la partie et j'attends toujours de voir un plan de match qui nous permettrait d'y arriver. Ce que nous avons fait... Je le répète: nous avons d'excellents éléments de base, des éléments de calibre mondial, mais nous ne sommes plus à l'abri du danger. Il y a une menace potentielle.

M. Glen Motz: J'ai une brève question à vous poser avant de passer à M. Parsons.

Si un ordinateur quantique lance une attaque, le saura-t-on? À l'heure actuelle, ces activités peuvent-elles passer inaperçues pendant de longues périodes de temps? Disposons-nous actuellement de systèmes permettant de les détecter?

M. Michele Mosca: C'est une excellente question.

Il est difficile de prédire comment les auteurs de ces menaces exploiteront la technologie. C'est un jeu effrayant. Si vous aviez un ordinateur quantique, qu'en feriez-vous? Quel est votre objectif? Voulez-vous détruire la planète? Voulez-vous être riche? Que voulez-vous faire? Selon les résultats que vous voulez obtenir, votre stratégie et vos tactiques seront différentes. Chose certaine...

C'est comme le film *The imitation Game — Le Jeu de l'imitation*, en français —, qui porte sur la Seconde Guerre mondiale. Après que les Alliés eurent décrypté le code Enigma, ils ont réagi de façon très tactique. Ils ne voulaient pas laisser savoir qu'ils possédaient une machine Enigma.

Il existe des indices qui vous échappent peut-être. Lorsque l'on commence à voir des choses qui semblent provenir de Microsoft, entre autres — des choses qui portent leur signature officielle, mais ne viennent pas de ces entreprises —, il s'agit de signaux d'alarme. Voilà le noeud du problème. Déchiffrer la cryptographie revient à remettre à quelqu'un une clé numérique lui permettant d'entrer dans le système par la grande porte. Il est très facile de passer inaperçu, je dirais.

Je ne sais pas si Brian veut ajouter quelque chose.

M. Glen Motz: Merci beaucoup.

Monsieur Parsons, je crois que vous étiez à Washington lorsque mon collègue PPH, Pierre Paul-Hus...

Des voix: Oh, oh!

M. Glen Motz: Désolé.

Vous y avez rencontré des agents du renseignement. À peu près au même moment, notre directeur du Centre canadien pour la cybersécurité, M. Jones, a fait allusion devant le Comité à la supériorité de nos installations d'essai par rapport à celles de nos alliés. Selon lui, grâce à ces installations, nous serions différents et capables de faire affaire avec des entreprises — comme Huawei, peut-être — provenant éventuellement d'États hostiles.

Pourriez-vous expliquer au Comité ce que nos homologues américains ont dit au sujet des capacités du Canada en matière de sécurité?

● (1620)

M. Christopher Parsons: Nous en avons beaucoup parlé à Washington et partout aux États-Unis. Les fonctionnaires américains ont fait preuve de beaucoup de circonspection. Ils n'ont pas dit explicitement s'ils croyaient que la politique du Canada était bonne ou mauvaise. Ils ont plutôt indiqué que, si nous prenions la décision d'adopter une approche semblable à celle du Royaume-Uni — en inspectant et en évaluant le matériel étranger avant de le laisser pénétrer dans le secteur des entreprises —, nous devrions examiner ce qui s'est passé dans ce pays. Ils ont souligné le fait que, l'année dernière, le Royaume-Uni a reconnu éprouver de graves problèmes dans la gestion de l'offre. Aux dernières nouvelles, l'an dernier, le pays n'est pas à même de garantir la sécurité du matériel de Huawei.

M. Glen Motz: Monsieur Parsons, pouvez-vous utiliser le temps qu'il me reste — une minute et demie — pour décrire, en vous basant sur vos recherches et sur votre opinion, les dangers auxquels nous pourrions être confrontés au Canada si nous permettions à une entreprise comme Huawei de faire partie de notre réseau 5G?

M. Christopher Parsons: Voilà qui soulève tout un ensemble de problèmes. D'abord, il y a la possibilité que le matériel soit mis à jour d'une manière qui compromette la sécurité nationale du Canada. Il pourrait s'agir d'une mise à jour du micrologiciel qui modifierait le fonctionnement des éléments fondamentaux des cartes électroniques. Il pourrait également s'agir de modifications des systèmes logiciels qui se trouvent une strate au-dessus sur l'équipement de routage.

Ensuite, si des vulnérabilités sont créées accidentellement — les bogues dans le code sont chose courante —, le gouvernement chinois pourrait émettre une ordonnance sommant Huawei de ne pas les corriger. C'est peut-être le genre de vulnérabilité le plus important, parce qu'il ne s'agit pas d'une vulnérabilité créée délibérément. En fait, les membres du Groupe des cinq ont aussi exploité de telles vulnérabilités, sans que cela soit prescrit par la loi, à notre connaissance.

Voilà les principaux enjeux. On pourrait alors utiliser ce genre de porte dérobée pour modifier des données, une pratique qui est sans doute aussi dangereuse, sinon plus dangereuse encore, que l'extirpation des données. Soudain, on ne pourrait plus savoir si les données que l'on reçoit et qui transitent par le réseau sont exactes, inexactes ou autres.

M. Glen Motz: On ne saurait jamais si cela a eu lieu. Dans le premier cas de figure, il s'agirait d'un code malveillant ou d'un quelconque bogue non corrigé. Cependant, s'ils ajustaient délibérément leur équipement et installaient des logiciels et du matériel de surveillance, les réseaux de notre pays ne pourraient jamais détecter cela.

M. Christopher Parsons: Ce serait extrêmement difficile à déterminer. En raison des mises à jour, nous pourrions passer d'un état de sécurité à un état d'insécurité à un moment donné dans le futur.

Le président: Merci.

Monsieur Dubé, vous avez sept minutes.

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

Merci à tous d'être ici.

Je veux reprendre là où M. Parsons et mon collègue M. Motz ont laissé.

Même si le réseau est sécurisé... Je pense en particulier au logiciel espion Pegasus sur l'iPhone; votre organisme a travaillé sur Pegasus — il en a même été victime, si je ne m'abuse. Même si le réseau est complètement sécurisé — quelqu'un a utilisé la métaphore d'un véhicule blindé protégé par des boîtes en carton —, je me demande si, à l'ère de l'Internet des objets, on ne s'inquiète pas d'avoir toujours accès à des appareils à distance. Les mises à jour des micrologiciels ne sont peut-être pas fournies aux appareils eux-mêmes, alors il se peut que les données passent — je m'exprime ici en termes simples — d'un appareil à un autre par le biais d'un réseau très sécurisé, mais une fois que les données aboutissent à un appareil bon marché — pour ainsi dire —, un appareil désuet ou autre, est-ce un problème?

Je vous écoute. Ensuite, si les autres témoins veulent aussi intervenir, j'aimerais bien les entendre.

M. Christopher Parsons: Du point de vue du Citizen Lab et du milieu de la sécurité informatique en général, la sécurité est un état continu. Elle impose des frictions et réduit la probabilité qu'une activité opportuniste ait lieu, mais la sécurité parfaite n'existe pas.

Pegasus, dont vous avez parlé, a été mis au point par NSO Group, une société israélienne qui produit des cyberarmes pour un certain nombre d'organisations et de pays. L'entreprise exploite des vulnérabilités pour lesquelles il n'existe aucun correctif connu. Les fabricants ne connaissent pas les vulnérabilités elles-mêmes. On craint qu'une entité comme NSO Group ou autre puisse cibler le matériel de Huawei parce qu'il présente une vulnérabilité que personne ne connaît. C'est une préoccupation très réelle.

En parallèle, les données transitent par ces appareils non sécurisés, ce qui ouvre également la possibilité d'une modification des données transmises à partir de l'Internet des objets. J'aime donner l'exemple suivant: votre thermostat indique qu'il fait 25 °C à l'intérieur et que vous profitez d'un bel hiver chaud à Ottawa, alors qu'en réalité il fait -30 °C dehors et votre thermomètre n'envoie pas de données à votre appareil de chauffage.

Ce serait un exemple de ce qui se passe dans l'Internet des objets lorsque la communication entre les appareils est modifiée par un point intermédiaire instable.

● (1625)

M. Brian O'Higgins: Dans l'exemple de Huawei, la confiance que nous avons envers le réseau est primordiale parce que tout le monde utilise ce réseau. Il est impossible de contrôler chaque appareil que les gens utilisent. Lorsqu'il y a une attaque très ciblée, des personnes précises seront compromises, c'est toujours le cas, mais il est très important de protéger le réseau que l'ensemble de la population et le monde utilisent.

M. Matthew Dubé: Voilà qui est intéressant. On vient de dire que les fabricants, ainsi que le public évidemment, ne connaissent peut-être pas certaines des lacunes des appareils.

Lorsque HackerOne était présent, on a quelque peu discuté des primes de bogue — de la découverte et du signalement des bogues —, mais il y a des inquiétudes au sujet du destinataire du signalement en raison du phénomène du « plus offrant ».

Je me demande quel est votre point de vue là-dessus. Comment devrions-nous aborder ce problème? Avons-nous besoin de règles explicites au sujet de la divulgation des vulnérabilités, particulièrement lorsque ce sont des organismes gouvernementaux qui font la découverte? Que se passerait-il, par exemple, si le Centre de la sécurité des télécommunications était au courant de graves lacunes sur des appareils que tous les Canadiens utilisent?

M. Christopher Parsons: Le CST, soit le Centre de la sécurité des télécommunications, possède ce qu'on appelle un programme d'équité en matière de vulnérabilités. Il détermine ainsi s'il divulguera ou conservera les vulnérabilités qu'il découvre. Ce n'est pas public. On ne sait pas exactement quelle est son efficacité ni quelles données sont ou ne sont pas présentées aux fabricants. Il est donc important, à mon sens, de démêler et de présenter tout cela.

Les chasses aux bogues ont une très grande utilité prospective. Bien souvent, les chercheurs en sécurité ne sont pas nécessairement motivés par l'argent qu'ils en retirent; c'est le prestige, et ces processus sont efficaces. Il s'agit souvent du dernier stade d'un nouveau programme de divulgation des vulnérabilités.

Je dirais que l'une des préoccupations relativement à la loi australienne est qu'elle laisse planer la possibilité que le gouvernement aille dire aux entreprises: « Nous voulons connaître tous les bogues de votre logiciel dont vous êtes au courant, mais que vous n'avez pas encore corrigés », afin de mener des enquêtes policières ou de sécurité nationale. C'est une grave préoccupation, car si c'est ainsi que le gouvernement choisit d'interpréter sa loi — et on donne à entendre que c'est ce qu'il fera —, cela signifie que les chasses aux bogues et les programmes de divulgation des vulnérabilités pourront effectivement servir à canaliser les données qui sont alors utilisées par d'autres États, au risque que ces vulnérabilités ne soient pas toujours utilisées à l'avantage du Canada.

M. Brian O'Higgins: Les vulnérabilités, bien sûr, sont des plus précieuses, surtout pour qui veut causer beaucoup de dommages. La NSA, c'est-à-dire la National Security Agency, avait ses stocks secrets de vulnérabilités. Le secret a été mis au jour d'une façon ou d'une autre et cet ensemble de vulnérabilités a révélé une série des virus et des logiciels malveillants les plus dommageables de mémoire récente, si bien que le problème est généralisé.

M. Michele Mosca: Mettons les choses en contexte: pour les comparer et les mettre en contraste avec la menace quantique — vu qu'il y a tellement de façons de se faire pirater et que cela peut vraiment engendrer la confusion —, briser la cryptographie serait essentiellement la mère de toutes les vulnérabilités, parce qu'il est tout simplement impossible de réparer le code. Il n'y a pas d'algorithme à corriger. Une bonne mise en oeuvre d'un mauvais algorithme demeure vulnérable.

Deuxièmement, si nous traitons cela comme une crise, les pirates informatiques auront beaucoup plus de vulnérabilités à exploiter sans ordinateur quantique.

M. Matthew Dubé: Ma dernière question porte sur les applications de tiers, dans les services bancaires en particulier. Étant donné qu'il y a beaucoup de renseignements de nature névralgique, faudrait-il plus de réglementation, une fois que l'on sort de... l'application sur son téléphone, à RBC, par exemple, et ensuite du type de renseignements qui sont communiqués?

Que pouvons-nous faire à ce sujet également? C'est une préoccupation qui a été soulevée.

M. Christopher Parsons: Il y a certainement une crainte que les applications de tiers aient accès à l'information et lui trouvent des utilisations dont on n'est pas au courant. Cela se voit dans tout l'écosystème des applications.

Il y aurait diverses mesures à prendre. L'une des moins risquées serait de voir à ce que les chercheurs légitimes en sécurité, comme nous au Citizen Lab, qui nous penchons sur ces genres d'applications ne soient pas tenus légalement responsables ou menacés lorsqu'ils les examinent. Nous nous sommes déjà retrouvés dans une situation où nous avons été confrontés à des organisations litigieuses à cause de notre travail en sécurité. Nous ne cherchons pas à briser les choses pour ruiner l'Internet; nous voulons le faire pour la sécurité de tout le monde. Nous sommes une organisation relativement bien financée et bien située.

Lorsque des personnes qui participent à cette recherche, et je vous parle d'expérience personnelle, sont poursuivies ou menacées de l'être une fois, ce n'est pas que les chercheurs en sécurité arrêtent de faire le travail. Ils continuent de le faire, mais ils ne l'annoncent pas. Ils ne le font pas pour le plaisir de pirater; ils le font parce que c'est là leur motivation. Par curiosité intellectuelle. Nous devons trouver un moyen de les aider à nous aider plutôt que de les envoyer se cacher dans l'ombre par crainte d'une responsabilité légale.

● (1630)

Le président: Merci, monsieur Dubé.

Monsieur Spengemann, vous avez sept minutes.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Merci, monsieur le président.

Messieurs, merci d'être des nôtres. Je veux résumer la conversation que nous venons d'avoir en la remettant sous la lentille des défis et des possibilités structurels auxquels nous sommes confrontés ici, et peut-être même en la situant dans l'optique de l'investissement dans l'infrastructure. Nous avons entendu toute la gamme des préoccupations. Monsieur Parsons, je pense que vous avez décrit le Canada comme un pays atteint d'une profonde insécurité cybernétique. Monsieur Mosca, vous avez dit qu'il y a des perspectives économiques à l'autre extrémité du spectre; si nous faisons bien les choses, nous pourrons réaliser des gains économiques positifs.

En utilisant la lentille de l'investissement, pourriez-vous commencer par faire la distinction entre la partie quantique et la partie non quantique du problème. Jusqu'où devons-nous nous préoccuper de l'informatique quantique à ce stade-ci? Dans quelle mesure est-elle une menace future? Dans la constellation actuelle de problèmes connus de cybersécurité par rapport au quantum, comment les choses se passent-elles? Où est le noeud du problème?

M. Michele Mosca: Je pourrais peut-être tenter une réponse rapide. Malheureusement, il faut tenir compte de tout ce qui précède. De toute évidence, la nature humaine est d'éviter la catastrophe imminente, et il est toujours possible de faire fi, sans conséquence immédiate, de la catastrophe qui pourrait frapper dans 10 ans. Nous avons besoin de discipline pour faire les deux en même temps, ce qui est difficile.

Dans les activités quotidiennes, les menaces changent rapidement. Pendant que nous cherchons une solution à un problème, des gens profitent d'un nouveau problème. Ce qui n'était pas jadis le moyen le plus économique de pirater un système l'est peut-être devenu. Nous devons mener de front les tactiques et la stratégie.

Quantum offre deux choses. L'une est un moyen de contournement. La sécurité n'est jamais parfaite, mais nous voulons faire de notre mieux. Si nous travaillons dans le cadre d'une gestion du cycle de vie, si nous faisons une transition proactive des fondements de notre cybersécurité pour écarter les menaces futures, c'est une occasion de... C'est comme lorsqu'il faut réparer son sous-sol. Pendant que l'on y est, on refait la plomberie et le câblage. Il est possible de réoutiller les fondations de notre cyberinfrastructure. Ce ne sera pas parfait, mais ce sera sacrément mieux que bien des cataplasmes appliqués par-dessus des vieux cataplasmes comme nous le faisons maintenant.

L'occasion est excellente de nous réoutiller, de bien faire les choses. Ce ne sera pas parfait, mais ce sera beaucoup mieux qu'aujourd'hui.

M. Sven Spengemann: C'est très utile.

Monsieur Parsons, dans quelle mesure pourrions-nous simplement refermer l'écart par la mise au point d'un cadre stratégique national convaincant?

M. Christopher Parsons: Je crois que cela aiderait beaucoup. Idéalement, toute stratégie devrait être claire et directe. Je pense que c'est un domaine dans lequel nous pouvons nous tourner vers les États-Unis — il leur a fallu une dizaine d'années, mais la plupart des agences, c'est-à-dire la collectivité du renseignement, ont commencé à se rapprocher — pour dire: voici comment nous abordons la sécurité nationale. Nous pouvons être d'accord ou pas sur le cadre stratégique qu'ils proposent, mais il est cohérent dans toutes les agences. Cela signifie que tous les éléments tendent à peu près au même but. C'est productif... pour les gens du gouvernement, de voir où ils doivent aller; pour ceux de l'extérieur du gouvernement, de voir quels services sont nécessaires; et pour les universitaires et les autres, de voir quelles technologies ou quels buts le pays doit viser.

M. Sven Spengemann: Quelqu'un d'entre vous a-t-il des données, ou pourrait-il nous proposer une estimation éclairée qui nous dirait si les entreprises canadiennes du secteur privé au Canada dépensent, en pourcentage de leurs dépenses d'exploitation, plus ou moins que les entreprises du Groupe des cinq en ce moment? Que devraient-elles dépenser désormais pour bien faire les choses, s'il y a une norme d'excellence pour les administrations qui ont bien fait les choses.

M. Brian O'Higgins: La réponse à la cybermenace est typiquement orchestrée par les secteurs du gouvernement et des finances, et c'est ainsi partout dans le monde. Le Canada n'est pas mauvais dans les deux cas, en particulier parce que nous n'avons que cinq ou six banques, plutôt que 30 000 comme aux États-Unis. Nos banques sont généralement grandes et font un assez bon travail. Le reste de l'industrie accuse un retard lamentable, et certains secteurs sont vraiment pathétiques. Je suis de plus en plus inquiet, surtout lorsque je songe aux infrastructures essentielles, à la production d'électricité et ainsi de suite et que j'y vois beaucoup d'équipement intégré qui comporte des vulnérabilités. Les mises à jour sont très difficiles à faire. De nos jours, les pirates deviennent plus astucieux et plus motivés dans les États-nations, et le risque est de plus en plus grand.

● (1635)

M. Sven Spengemann: Dans quelle mesure pensez-vous que c'est un facteur de la taille de notre économie nationale, de la taille de notre marché, de notre statut comme nation de moyenne importance? L'un d'entre vous a dit en parlant de l'Allemagne qu'il y a 50 personnes oeuvrant dans ce domaine, alors que nous en avons zéro. Je lis dans votre mémoire que la Chine investit des milliards de dollars dans la recherche quantique. La taille de notre économie, notre structure économique, est-elle un facteur, pour ce qui est des limites à respecter pour ce que nous pouvons ou devrions investir?

M. Christopher Parsons: Je dirais seulement que c'est un domaine où le gouvernement peut être très efficace. Si vous comparez les investissements du gouvernement canadien avec ceux de nos proches alliés, il est évident que les États-Unis sont le géant du Sud. Vous pouvez aussi voir ce qui se passe au Royaume-Uni et ailleurs dans le monde. Vous pouvez aller en Europe. Les Européens investissent énormément plus d'argent dans la recherche de moyens d'assurer la cybersécurité plus efficacement.

L'autre élément, pour reprendre ce que mon collègue a dit, c'est que les grandes banques sont comparativement bien protégées, mais que la majorité des entreprises canadiennes sont des petites et moyennes entreprises et que, franchement, nous ne nous retrouverons tout simplement pas dans une situation où une entreprise de 3 à 30 employés peut se payer un expert en sécurité à l'interne. Il est donc essentiel en ce sens, dans une perspective structurelle, que le gouvernement ou un autre groupe ou organisme trouve moyen de faciliter la sécurité dans ces organismes. C'est là que travaillent de nombreux Canadiens. C'est de là que vient souvent notre croissance économique, et c'est là que se trouvent, à mon avis, les cibles les plus importantes à ce stade-ci.

M. Sven Spengemann: Il me reste une minute. Pour revenir sur cette question, dans quelle mesure les gouvernements ou les économies du secteur privé peuvent-ils rester pour une période prolongée à la fine pointe de la cadence du changement? Autrement dit, tout le monde est-il en train de faire du rattrapage ou essayons-nous seulement d'être les meilleurs pour cela? Ou y a-t-il effectivement une façon de prendre les devants et d'être proactifs et positifs?

M. Brian O'Higgins: Oui, cela a été mentionné plusieurs fois. Il est à peu près impossible d'être parfaitement en sécurité, mais, à toutes fins utiles, il y a moyen de bien se protéger, parce que la définition de la sécurité est qu'il suffit d'avoir un tout petit peu d'avance sur l'effort que le pirate est prêt à faire pour atteindre son but. S'il y a un niveau de sécurité dans l'industrie et qu'on n'est qu'un grand coquelicot, et un peu mieux même, on est en sécurité, parce que les attaques seront ciblées ailleurs.

M. Sven Spengemann: Et c'est mesurable.

M. Brian O'Higgins: Il s'agit d'y porter attention, de toujours suivre les pratiques exemplaires et d'établir un budget en conséquence, avec tous les incitatifs pour nous amener à faire attention. Il y aura une loi sur la responsabilité et toutes sortes de choses au fur et à mesure qu'on prendra conscience d'une cybermenace. Cela commence lentement, mais nous avons besoin de plus d'incitatifs.

Le président: Merci, monsieur Spengemann.

Monsieur Eglinski, vous avez cinq minutes.

M. Jim Eglinski (Yellowhead, PCC): Merci, monsieur le président.

J'aimerais remercier nos trois témoins d'aujourd'hui.

J'ai toujours été pas mal en sécurité dans la vie, jusqu'à ce que nous commencions cette étude ici, et que je commence à entendre le témoignage de types comme vous. C'est comme: « Oh, finalement je ne suis plus aussi en sécurité. » Je sors de cette réunion avec un sentiment d'insécurité, mais quoi qu'il en soit...

Monsieur Mosca, vous avez dit quelque chose de très intéressant. Vous avez parlé du terrain de football et de qui élabore ce plan. Nous n'arrivons pas tout à fait à la ligne bleue.

Qui élabore le plan? Quelle est la recommandation que vous avez à nous faire pour l'élaboration de ce plan? Nous sommes là pour vous entendre parler de cybersécurité, mais nous devons savoir ce que nous devons faire. Devons-nous travailler avec les universités? Devons-nous travailler avec l'industrie, le gouvernement, etc.? Qu'en pensez-vous?

M. Michele Mosca: Je pense que nous devons réunir une poignée de leaders d'opinion de chacun des secteurs pour élaborer le plan. Comme je l'ai dit, personne n'est l'unique dépositaire du savoir-faire ou de la capacité de mettre en oeuvre le plan, ni même de comprendre ce que devrait être le plan global. Ensemble, nous pouvons trouver la solution, mais il faut s'y mettre. La question n'est pas théorique. Nous devons réunir ce groupe de leaders d'opinion et lui confier la mission de nous donner la plus grande cybersécurité possible... y compris Quantum-Safe. Soyons des leaders économiques dans cet espace.

Je parle des paliers supérieurs de gouvernement. Le mandat doit être de haut niveau. Il doit être implicite dans toutes les lettres de mandat pertinentes des ministres. L'industrie sera là. Dans les milieux universitaires, nous sommes là pour vous aider. Nous devons renforcer nos rangs, mais ceux d'entre nous qui sont ici y sont pour aider, si nous sommes effectivement appelés à travailler à ce mandat. Nous savons que ce n'est pas aux milieux universitaires de protéger les citoyens contre les cyberattaques mortelles ou de surveiller la stratégie de développement économique du Canada, mais nous voulons certainement aider. Nous travaillerons à cette table, mais il faudrait nous y amener très proactivement.

● (1640)

M. Jim Eglinski: Dans ce cas, je pense qu'une façon de voir ce que vous dites est qu'il nous faut un quart-arrière pour nous guider. À votre avis, qui cela devrait-il être?

M. Michele Mosca: Eh bien, nous avons besoin d'un entraîneur et d'un quart-arrière, oui.

M. Jim Eglinski: Un entraîneur et un quart-arrière... Pensez-vous que ce devrait être le gouvernement fédéral?

M. Michele Mosca: Je pense que le gouvernement fédéral a toute l'autorité morale pour gérer cela, avec les leaders de l'industrie et les leaders d'opinion en recherche.

M. Jim Eglinski: Tout à l'heure, mon collègue vous a demandé combien de temps il nous faudrait pour détecter une attaque contre nous. Y a-t-il quelqu'un qui surveille ce qui se passe actuellement au Canada, un organisme qui surveille ce dont vous avez parlé, ou nous contentons-nous d'espérer attraper l'insaisissable?

M. Michele Mosca: Eh bien, je ne sais pas ce qui se passe dans l'espace classifié. Je m'attendrais qu'il y ait de l'activité de ce côté-là. Dans les milieux universitaires, nous observons et expliquons très ouvertement ce que nous savons.

Il y a une chose importante que je n'ai pas soulignée: à un moment donné, nous ne saurons pas, et nous devons écarter cette menace. Pourquoi jouons-nous à la boule de cristal alors que nous savons comment écarter la menace? Comme je le disais tantôt, ce sont vraiment les auteurs des menaces qui décident s'ils veulent nous saigner lentement ou nous décimer complètement. C'est leur choix. Nous espérons qu'il n'est pas dans leur intérêt commercial de nous anéantir, mais ils peuvent le faire s'ils le veulent. Donc, pourquoi voudrions-nous même aller là? Écartons cette menace.

M. Jim Eglinski: À un moment donné, le Canada était un chef de file en informatique quantique, si je me souviens bien, à l'Université de Waterloo et dans quelques entreprises basées en Colombie-Britannique. Selon vous, où en sommes-nous aujourd'hui par rapport au reste du monde? Nos jeunes montrent-ils de l'intérêt par les milieux universitaires? Y a-t-il des gens qui s'intéressent à ce domaine, ou avez-vous de la difficulté à recruter?

M. Michele Mosca: Je pense que nous sommes toujours les meilleurs dans le domaine des sciences fondamentales et du développement technologique et ainsi de suite. Nous avons rédigé le plan d'affaires pour la propriété du monde quantique, et nous nous sommes précipités pour le mettre en oeuvre, et nous avons encore un produit de calibre mondial, dont nous pouvons être fiers, partout au pays — au Québec, en Ontario, dans l'Ouest et dans les Maritimes. Il y a bien des choses qui nous intéressent dans le domaine des sciences fondamentales en technologie, et nous avançons un peu vers un plus grand nombre de choses appliquées.

C'est en quelque sorte distinct de la cybersécurité. Quantum-Safe Canada peut être l'un des piliers d'une stratégie quantique plus vaste visant à s'approprier le podium pour les retombées économiques de ces décennies d'investissements, mais cette coordination ne se fait pas encore. Le besoin est urgent, parce que nous parlons de dizaines de milliards de dollars investis dans le monde pour en quelque sorte prendre ce déjeuner que nous préparons depuis de nombreuses décennies.

Nous devons agir très rapidement si nous sommes sérieux à ce sujet. Nous ne voulons pas que ceci devienne le quantum Arrow d'Avro, si bien qu'il est très urgent de coordonner ces merveilleux produits que nous avons en quantum. Encore une fois, Quantum-Safe Canada pourrait être le chef de file dans le domaine, et au fur et à mesure de l'arrivée à maturité de ces autres éléments, nous pourrons également nous approprier le podium économiquement dans le domaine de la technologie quantique — pas seulement la technologie, mais aussi les applications, les logiciels, et ainsi de suite, les utilisations de l'informatique quantique et de la technologie quantique.

Le président: Merci, monsieur Eglinski.

Monsieur Picard.

[*Français*]

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

Je partage votre passion, celle de cerner de tels défis dans un secteur qui nous est à ce point inconnu. C'est le domaine de Quantam-Safe Canada. Je vais vous exposer mes idées et vous pourrez me corriger si je fais erreur.

Vous considérez que la menace est vraiment importante et que, de toute évidence, le Canada est très en retard par rapport à ses concurrents pour ce qui est de sa capacité à se défendre contre les menaces extérieures. La menace n'est pas à proprement parler surévaluée, mais elle est sûrement plus importante que ce qu'en perçoivent les gens en général.

Vous proposez des solutions d'ordre mécanique, technique, technologique. Compte tenu de votre grande expertise, nous pourrions croire que ces solutions répondent au problème auquel nous devons faire face. Je ne crois pas nécessairement qu'il s'agisse d'une surévaluation, mais je pense que la confiance à l'égard des solutions proposées est très grande. Pourtant, plus nous parlons de l'aspect technique, moins nous considérons un aspect précis. Je parle ici du seul risque dont vous n'avez aucune maîtrise: les ressources humaines. Personne n'a été en mesure de m'apporter une piste de solution jusqu'à présent à ce sujet.

Même si vous avez le plus beau système, un système en béton, le facteur humain étant imprévisible, vous allez perdre la maîtrise de la situation. Votre système va s'écrouler comme un château de cartes parce que le facteur humain à l'interne, ou le piratage psychologique, y feront obstacle. Pourtant, je ne suis pas certain que l'intelligence artificielle est la solution pour gérer le risque humain. J'aimerais entendre votre avis à ce sujet.

● (1645)

M. Michele Mosca: Je vous remercie de la question.

[*Traduction*]

Vous avez tout à fait raison. Le facteur humain est l'une des plus grandes vulnérabilités, sinon la plus grande, et cela ne changera pas fondamentalement. La nouvelle mathématique, l'enchevêtrement quantique, ne va pas changer notre faillibilité et notre corruptibilité comme êtres humains, mais une bonne cryptographie nous rend moins dépendants de personnes dignes de confiance. Nous en avons encore besoin, mais nous en sommes moins dépendants, et c'est vraiment important.

En second lieu, les vulnérabilités intrinsèques dans les erreurs humaines et les compromis humains ont tendance à être plus éphémères et réglables. S'il y a une personne corrompue, si quelqu'un utilise un mauvais mot de passe ou clique là où elle ne devrait pas, on détecte et on corrige. C'est en quelque sorte au sommet de la pile de choses qui font mal... C'est très courant. Cela ne va pas disparaître, mais nous avons une chance de nous en tirer en adoptant une meilleure discipline et de meilleurs mécanismes de détection et, encore une fois, devenons moins tributaires d'une approche intelligente — pas intelligente; nous sommes tous intelligents — mais de personnes qui ne commettent pas d'erreurs, parce que, bien sûr, des erreurs, nous allons en commettre. Nous pouvons réduire cette vulnérabilité, mais pas la ramener à zéro.

Plus loin dans la pile, il n'y a pas de remède rapide pour les cryptographies percées.

Vous avez parfaitement raison — on ne peut pas traiter une solution unique de façon isolée, parce que c'est tout l'écosystème qui fonctionne ensemble. C'est certainement la raison pour laquelle je voulais défendre ces 20 chaires supérieures de recherche pour le Canada. Aujourd'hui, c'est 50, parce qu'il y a du rattrapage à faire. Environ un quart d'entre elles doivent être dans les sciences sociales et humaines pour nous aider à trouver la meilleure façon de gérer tous ces aspects.

M. Michel Picard: Monsieur Parsons, vous avez quelque chose à dire?

M. Christopher Parsons: Je pense qu'il y a un défi fondamental à relever pour bâtir une infrastructure et des systèmes sûrs. C'est très difficile. Pour vous donner un exemple, il a probablement fallu 10 ou 15 ans pour arriver à ce que, lorsqu'on met à jour son navigateur Web ou son système d'exploitation, il fonctionne, et nous pouvons le garantir.

Si je dis cela, c'est parce que le chiffrement est compliqué, et tout effort visant à miner les quelques systèmes qui fonctionnent aurait des conséquences dévastatrices. Malheureusement, nous constatons que cela est arrivé dans certains pays, comme en Australie... et que cela justifierait de le faire dans d'autres domaines, par exemple aux États-Unis à des fins d'application de la loi, et dans une moindre mesure au Canada, également pour l'application de la loi.

Nous sommes dans une situation où il ne s'agit pas seulement d'évaluer comment nous pouvons être protégés. Il s'agit aussi de voir comment évaluer ce que nous devons faire. Mon argument, et certainement celui du Citizen Lab, est que nous devons préserver les quelques outils fonctionnels que nous avons déjà pour faciliter les systèmes sécurisés, plutôt que de les mettre à risque dans la poursuite d'enquêtes à court terme pour les services d'application de la loi.

M. Michel Picard: Merci.

Le président: Sur ce, avant de conclure, le président a une question. Je vais la poser à M. Mosca.

S'agissant d'être à la fine pointe de la technologie, le Canada ne rate jamais l'occasion d'en rater une. Vous avez donné l'exemple d'Avro. Vous avez décrit une situation critique où, si nous ne faisons pas bien les choses, nous allons tout simplement nous écarter de la cybercarte, si je puis dire.

M. Parsons a présenté une série de suggestions sur les mesures que nous devons prendre en tant qu'entité organisatrice. Comme vous, peut-être, je suis un peu sceptique au sujet de la capacité du gouvernement d'y arriver. Que pensez-vous de sa série de suggestions sur la façon dont nous devrions aborder nos vulnérabilités cybernétiques?

● (1650)

M. Michele Mosca: De ma perspective, elles m'apparaissaient de bonnes approches des enjeux à court et à moyen terme, que nous devons absolument régler. Pour moi, cela doit s'inscrire dans un programme cybernétique plus vaste pour le Canada. Nous devons simultanément décider que c'est là que nous voulons être dans 10 ans et que ce sont là toutes les importantes disciplines et pratiques que nous devrions à tout le moins envisager, ou adopter sous une forme quelconque, comme solution aux problèmes qu'il dit que nous devons résoudre. Le but final, par contre, devrait également inclure la résilience aux attaques futures.

En fin de compte, nous voulons construire un système immunitaire cybernétique plus solide. Il ne s'agit pas de résoudre les derniers... ou d'appliquer un moyen de défense après l'autre, comme colmater des brèches dans un barrage. Dix ans dans l'avenir, ce n'est pas si loin. Nous n'avons qu'à trouver un moyen de mettre en place un meilleur système immunitaire cybernétique, où nous serons mieux en mesure de détecter les menaces nouvelles et émergentes et de nous adapter rapidement pour y faire face, au lieu de nous contenter tout le temps de boire l'eau des tuyaux d'incendie.

Cela exige un effort mieux coordonné au Canada. Je pense que Brian O'Higgins a préconisé une organisation de type RAND, où la recherche sur la cybersécurité doit être financée par le gouvernement. On veut que le gouvernement reçoive des conseils fiables, objectifs et éclairés, afin de pouvoir réagir rapidement aux menaces nouvelles et émergentes. Selon moi, c'est un élément fondamental d'un système immunitaire cybernétique national. Ce n'est pas la seule partie, mais c'est l'un des prochains éléments que je préconiserais fortement, en plus du centre de cybersécurité existant et de toutes les choses formidables qui contribuent à notre cause.

Le président: Merci.

Allez-y, monsieur O'Higgins.

M. Brian O'Higgins: Je vais vous donner un autre exemple d'un modèle que j'ai bien aimé. Lorsque j'ai fondé Entrust, un fournisseur de technologie de chiffrement de calibre mondial, le gouvernement fédéral canadien a été notre tout premier client. De fait, c'est grâce à lui que l'entreprise a pu démarrer. Cela a débouché sur un marché d'exportation, et le temps de le dire, nous étions dans 50 gouvernements nationaux. Une grande victoire.

Nous continuons de nous inspirer de ce genre d'aura selon laquelle les Canadiens sont bons en technologie de chiffrement. Il y a aujourd'hui une occasion à saisir avec la résistance quantique. Le chiffrement doit changer du tout au tout dans le monde. Il doit pouvoir résister à une attaque quantique. Devinez quoi? La technologie quantique canadienne de l'Université de Waterloo et d'ailleurs est de calibre mondial. L'occasion est bonne de répéter ce genre d'effet.

Le président: Espérons de ne pas la perdre.

M. Brian O'Higgins: J'ai bien compris votre commentaire.

Des voix: Oh, oh!

Le président: Sur ce, nous allons suspendre la séance puis accueillir un nouveau groupe.

● (1650)

(Pause)

● (1655)

Le président: Mesdames et messieurs, nous reprenons nos travaux.

Nous accueillons notre deuxième groupe de témoins, M. Masnyk, de SkyBridge Strategies, et Normand Lafrenière, de l'Association canadienne des compagnies d'assurances mutuelles.

Avez-vous tiré à pile ou face pour décider qui va commencer?

Monsieur Lafrenière, nous avons hâte d'entendre ce que vous avez à dire pendant les 10 prochaines minutes.

Merci.

[*Français*]

M. Normand Lafrenière (président, Association canadienne des compagnies d'assurance mutuelles): Merci, monsieur le président.

Je vais partager mon temps de parole pour ma présentation avec mon collègue M. Steve Masnyk, de SkyBridge Strategies.

Je m'appelle Normand Lafrenière et je suis le président de l'Association canadienne des compagnies d'assurance mutuelles, ou ACCAM.

L'ACCAM représente 79 sociétés d'assurance mutuelles au Canada, qui se spécialisent en assurances automobile, habitation et agricole ainsi qu'en assurance d'entreprises.

La création des sociétés d'assurance mutuelles s'est échelonnée sur une période de 100 ans, à compter de 1836. Elles ont vu le jour parce que les agriculteurs ne pouvaient pas se procurer d'assurance ou ne pouvaient pas encore en trouver à un coût raisonnable.

Les sociétés d'assurance mutuelles sont la propriété de leurs détenteurs de police d'assurance. Nous n'avons pas d'actionnaires ni d'actions, et nous ne sommes pas sur le marché boursier. Nos détenteurs de police d'assurance sont ceux qui décident de l'avenir de nos compagnies. Ce sont eux qui élisent les conseils d'administration de celles-ci.

La prime payée par les membres des sociétés d'assurance mutuelles sert à payer les réclamations. Lorsque nous générons du profit, les sommes servent alors à renforcer les surplus de la compagnie en vue de payer des réclamations futures. Le profit permet aussi de rembourser les membres, c'est-à-dire que nous retournons ce profit à nos membres, ou encore cet argent est utilisé au profit de la communauté.

Les sociétés d'assurance mutuelles ont mis en place deux sociétés mutuelles de réassurance — leurs propres réassureurs — pour partager les risques et se trouver de la réassurance sur le marché international.

Nous avons également nos propres fonds de garantie pour indemniser les assurés dans l'éventualité où des compagnies d'assurance mutuelles feraient faillite. Soit dit en passant, au cours des 60 dernières années, depuis que nous avons mis en place ce fonds de garantie, aucune compagnie d'assurance mutuelle n'a fait faillite.

À l'heure actuelle, les sociétés membres de l'ACCAM détiennent 15 % du marché canadien non gouvernemental de l'assurance multirisque. Particulièrement présentes dans les régions rurales au Canada, nos sociétés d'assurance mutuelle assurent 75 % des fermes canadiennes.

Nous vous entretenons aujourd'hui des enjeux liés aux cyberrisques et aux menaces pour le système financier au Canada, plus particulièrement de notre manière de percevoir le système bancaire ouvert comme un risque potentiel d'attaques informatiques.

De manière générale, le secteur des assurances n'est pas une proie potentielle pour le cyberpiratage. À l'exception des numéros de cartes de crédit ou de débit que nos membres détiennent, les sociétés d'assurance mutuelles disposent de très peu de données financières intéressantes pour le piratage informatique.

Nous sommes sérieusement préoccupés par le débat actuel, en particulier en ce qui concerne le système bancaire ouvert. Ce concept a vu le jour en Europe, au Royaume-Uni, en Autriche et au Japon. Comme ce concept n'a été mis en place que récemment, il existe très peu de preuves pouvant nous indiquer dans quelle mesure le système fonctionne bien ou ne fonctionne pas bien.

Nous pouvons toutefois donner notre avis sur les points de discussion soulevés par le gouvernement lorsqu'il a lancé, récemment, une consultation sur le système bancaire ouvert.

● (1700)

[*Traduction*]

L'ACCAM craint particulièrement que le concept du système bancaire ouvert n'affaiblisse l'interdiction de longue date qui empêche les banques de se lancer dans le secteur de l'assurance. Cette interdiction de longue date, appuyée par les gouvernements de toutes allégeances, vise à protéger les consommateurs d'assurances contre les institutions de crédit qui pourraient leur imposer des mesures coercitives pour les obliger à acheter un produit d'assurance qui ne leur convient pas. Nous espérons que pas un cadre de système bancaire ouvert ne minera l'interdiction faite par la loi.

J'aimerais maintenant demander à mon collègue, Steve Masnyk, d'aborder d'autres préoccupations liées au système bancaire ouvert et aux risques cybernétiques.

M. Steve Masnyk (principal, SkyBridge Strategies): Merci, monsieur Lafrenière.

Merci, monsieur le président. Bonjour, membres du Comité.

Je ne sais pas si ce petit diagramme a été distribué à tout le monde. Vous l'avez peut-être devant vous. J'espère qu'il pourra orienter la discussion, car, comme je parle dans l'abstrait, il est un peu plus facile de comprendre le concept si vous avez le diagramme devant vous.

J'aimerais expliquer le concept du système bancaire ouvert et les cyberrisques qu'il représente pour le secteur canadien des services financiers. Je suis sûr que de nombreux membres ne savent pas ce qu'est le système bancaire ouvert.

C'est un concept selon lequel un consommateur peut demander de transférer à des tiers qui sont dans les services financiers toutes ses données que détient sa banque: son compte de chèques, ses opérations de carte de crédit, ses opérations de carte de débit, ses placements, ses REER, son hypothèque, ses assurances et ses autres emprunts. Les tiers sont les sociétés de technologie financière, aussi appelées « fintechs ».

Ces entreprises de technologie financière vont alors offrir un service financier que le consommateur a ou n'a pas déjà, un service fondé sur les données bancaires de sa banque à son sujet. Ce transfert se ferait par un intermédiaire appelé interface de programmation d'application, communément dit API.

Les API sont essentiellement des plateformes ou des applications qui serviraient de conduit entre le client, ses données bancaires et toutes les entités de technologie financière qui y sont associés. Dès lors que le client présente une demande d'API pour autoriser l'API à réunir ses données à la banque et à les diffuser, l'API donnerait suite et diffuserait les données aux entreprises de technologie financière qui y sont affiliées.

Les entreprises de technologie financière auraient l'historique bancaire du consommateur et, à l'aide de ces données, vous offrirait un produit à meilleur prix que ce que vous avez ou vous n'avez pas déjà. En fonction des données, elles sauraient à peu près tout sur vous: quels produits vous avez, quels produits vous n'avez pas et de quels produits vous pourriez avoir besoin.

Telle est l'essence du concept du système bancaire ouvert. Comme vous pouvez l'imaginer, ce ne sont pas les risques et les menaces entourant le système bancaire ouvert qui manquent: Qui réglemente les API et selon quelles normes, provinciales ou fédérales, de protection des renseignements personnels? Qui réglemente les entreprises de technologie financière? À quelles règles de protection des renseignements personnels sont-elles astreintes? Comment le consommateur autorise-t-il ces intervenants à diffuser ses données bancaires? Le consommateur peut-il révoquer son consentement? Qu'arrive-t-il des données une fois que le consommateur a retiré son consentement? Comment le consommateur sait-il quels intervenants détiennent ses données?

Certaines des grandes questions concernant les cyberrisques et le piratage s'appliquent également: Avec quelle facilité l'entreprise de technologie financière peut-elle être piratée? Quelles règles suit-elle, et qui les applique?

Les banques sont des joueurs hautement réglementés qui ont de très rigoureuses normes de protection des renseignements personnels au Canada, tout comme les compagnies d'assurances. Quelle est la place des entreprises de technologie financière dans cette hiérarchie des normes? Les banques canadiennes dépensent des millions, sinon des milliards de dollars en technologie pour protéger les données de leurs clients, ce qui ne les met pas pour autant à l'abri du piratage. Et que dire des entreprises de technologie financière, qui dépensent très peu? Voilà quelques-unes des grandes questions que je laisserai à la réflexion du Comité.

Quant au secteur de l'assurance, comme M. Lafrenière l'a dit, avec les menaces de cyberrisques, nous pouvons dire que, s'agissant des compagnies d'assurance mutuelles, le risque est minime, croyons-nous. Les compagnies d'assurances ne détiennent pas de données financières de grande valeur et ne sont pas aussi exposées au piratage que les banques, par exemple, qui détiennent des données nettement plus précieuses.

Je vous laisserai avec un exemple. Bien sûr, une compagnie d'assurances qui assure la maison ou la voiture du consommateur pourrait être piratée; mais je ne suis pas sûr qu'un pirate trouverait intéressant de savoir quel âge a la voiture ou combien de salles de toilettes il a dans le sous-sol. Certes, le risque de piratage existe, mais c'est une question de degré.

Sur ce, nous serons heureux de répondre à vos questions.

● (1705)

Le président: Merci beaucoup.

Monsieur Spengeman, vous avez sept minutes.

M. Sven Spengemann: Monsieur le président, merci beaucoup.

Merci à vous deux d'être là.

Permettez-moi de commencer par le système bancaire ouvert. Vous avez nommé quelques pays où il est devenu populaire. Qu'est-ce qui l'inspire? Selon vous, quelle est la trajectoire actuelle du système bancaire ouvert? Qu'en est-il des avantages économiques ou sociaux, puisque cela doit bien se faire pour une bonne raison? Quel est l'avantage? Y a-t-il une solution de rechange à la structure actuelle qui pourrait être fonctionnelle?

M. Steve Masnyk: Je vais commencer, puis il pourra ajouter quelque chose.

En Europe, au Royaume-Uni et dans certains pays d'Asie, c'est nouveau depuis un an ou un an et demi. L'avantage du système bancaire ouvert, comme le disent ses partisans, c'est qu'il offre plus de choix aux consommateurs et plus d'efficacité dans le secteur des services financiers. La tendance est au guichet unique plus rapide. Parmi les arguments invoqués, il y a que le client ou le consommateur qui aurait des produits financiers avec de nombreux intervenants différents. Il pourrait avoir une hypothèque avec une banque, un autre emprunt d'une autre banque, et encore un autre produit d'une coopérative de crédit. Toutes les données bancaires et financières du client seraient ainsi regroupées. Voilà certaines des raisons pour lesquelles ces autres pays ont adopté le système bancaire ouvert.

M. Normand Lafrenière: À l'heure actuelle, il y a certains problèmes. Certaines personnes pratiquent ce qu'on appelle, je pense, le grattage d'écran, c'est-à-dire la capture de données d'écran. Essentiellement, elles prennent leurs données. Elles donnent leur nom d'utilisateur et leur mot de passe à des tiers pour qu'ils puissent prendre leurs données d'une banque et de l'autre banque et ainsi de suite et réunir cette information et offrir le service, si vous voulez. Cela disparaîtrait avec l'avancée de l'API. Essentiellement, cela réduirait le risque, en ce sens, pour les gens qui donnent leur nom d'utilisateur et leur mot de passe à des tiers, ce qui, soit dit en passant, constitue une violation de leur contrat avec leur propre banque.

M. Sven Spengemann: C'est encore trop nouveau pour voir si cela devient permanent. Est-ce ce que vous dites, que c'est vraiment un phénomène très récent et que l'on ne sait toujours pas s'il existe une version à la fine pointe du système bancaire ouvert?

M. Steve Masnyk: Vous avez tout à fait raison. Comme je l'ai dit, en Europe et au Royaume-Uni, c'est depuis 12 mois, si bien qu'il n'y a pas de données anecdotiques sur son bon ou son mauvais fonctionnement.

M. Sven Spengemann: Y voyez-vous un symptôme de ce que certains appellent une diminution ou un recul de la littératie financière dans la population? Est-ce en partie ce qui pourrait être à l'origine de tout cela?

M. Steve Masnyk: C'est possible. Je ne suis pas un expert en banque; il faudrait probablement parler à quelqu'un qui s'y connaît beaucoup mieux que moi.

M. Sven Spengemann: D'accord.

À ceux qui diraient: « S'il se consolide, réglemente mieux les technologies financières et chiffre mieux les transmissions de données », le problème serait-il réglé?

M. Normand Lafrenière: Je pense que nous avons besoin de nouvelles normes pour transmettre l'information des banques à des tiers. Elles se présentent sous différents formats.

M. Sven Spengemann: C'est comme la protection des dossiers médicaux. En ce sens, ce serait très semblable.

M. Normand Lafrenière: Je dirais que oui.

M. Sven Spengemann: D'accord.

M. Steve Masnyk: Pour répondre à votre question, monsieur Spengemann, disons que la plupart des entreprises de technologie financière sont enregistrées et réglementées au niveau provincial. Ainsi, dans un régime fédéral, il y aurait un écart de réglementation des entreprises de technologie financière. Par exemple, il y a maintenant 5 ou 10 grands joueurs fédéraux: les banques et les compagnies d'assurances qui sont soumises à une réglementation serrée. Si 2 000 entreprises de technologie financière faibles ou joueurs faibles ne sont pas réglementés au niveau fédéral, comment cela ouvre-t-il la porte à tout le risque de cyberattaque à l'échelle du pays?

M. Sven Spengemann: Je me demande si je pourrais prendre une minute ou deux pour vous poser une question légèrement différente au sujet du secteur de l'assurance. Selon votre témoignage, les données détenues par les compagnies d'assurances ne sont pas sensibles au point qu'il y a un risque disproportionné qu'elles fassent l'objet de cybermenaces. Pensez-vous que le secteur de l'assurance pourrait s'amener et offrir de l'assurance aux institutions financières pour la protection de leurs données? Autrement dit, pouvez-vous offrir de l'assurance contre les cyberrisques? Est-ce quelque chose qui est actuellement en place, envisagé ou en voie d'élaboration?

● (1710)

M. Normand Lafrenière: Il est certain que la protection des données existe. Même si nous représentons moins de risques dans le secteur de l'assurance, cela ne veut pas dire que nous n'avons pas de normes rigoureuses pour la protection des données de nos clients.

M. Sven Spengemann: Mais pour ce qui est du développement des produits et des régimes d'assurance, si une entreprise en démarrage se lance, au lieu de mettre au point son propre système de cybersécurité, elle pourrait demander à une tierce partie de le faire pour elle et ensuite prendre une police d'assurance contre les violations. Est-ce un modèle qui...?

M. Steve Masnyk: La cyberassurance existe. Il y a de très grands joueurs qui travaillent dans la cyberassurance. Mais la question est de savoir ce qu'on assure exactement. Assure-t-on quelqu'un pour lui procurer une nouvelle identité, et comment cela fonctionne-t-il? Combien d'argent paierait-on pour permettre de se faire une nouvelle identité? Combien en coûte-t-il ou combien difficile est-il d'obtenir un nouveau numéro d'assurance sociale au Canada? Je l'ignore.

Ce produit existe bel et bien, et ce sont là certains des arguments que proposent les entreprises de technologie financière — la cyberassurance est disponible et couvrirait ces risques. Mais quel est le coût d'une nouvelle identité? Comment quantifier cela?

M. Sven Spengemann: Très bien. Voilà qui est utile.

Il me reste un peu de temps. Je me demande si nous pourrions profiter de votre présence pour ajouter au témoignage du groupe précédent en ce qui concerne votre évaluation de la situation du secteur bancaire canadien en matière de protection par rapport à d'autres pays — peut-être le Groupe des cinq et le genre de trajectoire qu'il suit en ce qui concerne les menaces futures et les menaces changeantes.

M. Steve Masnyk: Je pense qu'il faudrait probablement en parler au secteur bancaire. Ce n'est pas une question sur laquelle nous aurions une opinion intelligente.

M. Normand Lafrenière: Bien sûr, nous n'avons qu'un certain nombre de joueurs à l'heure actuelle, et nous savons qu'ils dépensent beaucoup d'argent pour protéger leurs données. Notre préoccupation est, bien sûr, que lorsque s'amènent une foule de nouveaux joueurs, même s'il s'agit d'entreprises financières, nous ne sommes pas sûrs que les données jouiront de la même protection.

M. Sven Spengemann: J'ai posé la question tout à l'heure au sujet de la taille du marché canadien ou de notre économie, et j'ai demandé si c'était une contrainte en ce qui concerne l'investissement net provenant de sources du secteur privé ou du secteur public dans la cybersécurité. J'ai eu l'impression que, oui, dans d'autres pays, il y a beaucoup plus d'investissements parce que les économies sont plus grandes et plus complexes et qu'il y a plus d'intervenants.

Est-il donc juste de dire qu'un engagement et une contribution publics accrus dans le domaine de la cybersécurité seraient bénéfiques pour le Canada?

M. Steve Masnyk: En ce qui concerne la cyberassurance, la plupart des compagnies d'assurances qui vendent ce type de produits sont mondiales. Par exemple, il y a des assureurs multinationaux qui font ça. Je pense à Lloyd's, une très grande compagnie d'assurances multinationale. Elle fait beaucoup de cybersécurité.

Encore une fois, ce ne serait pas l'entité autonome canadienne; ce serait tout le groupe qui serait dans ce secteur d'activité. C'est assez global... Je ne pense pas que la taille de l'économie canadienne et la population soient vraiment importantes.

Le président: Merci, monsieur Spengemann.

Monsieur Motz, vous avez sept minutes.

M. Glen Motz: Merci, monsieur le président.

Merci, messieurs, d'être ici.

Malheureusement, la plupart des Canadiens, j'en suis sûr, ont suivi les travaux du Comité de la justice et ce qui se passe à cet égard, l'implosion du gouvernement actuel et les pressions qui ont été exercées sur un membre de son propre gouvernement. Maintenant, je dis que...

M. Michel Picard: J'invoque le Règlement...

M. Glen Motz: Un instant. Cela s'en vient.

Une voix: Pertinence...

M. Glen Motz: Je dis cela parce que je comprends que vous avez vécu quelque chose de semblable, messieurs. L'an dernier, vous avez soulevé des préoccupations au sujet de la cybersécurité et vous avez subi des pressions de la part du cabinet d'un ministre pour ne pas témoigner, pour garder le silence...

M. Sven Spengemann: Monsieur le président, il met des mots dans la bouche du témoin.

J'invoque le Règlement...

M. Glen Motz: Laissez-moi terminer ma question et vous comprendrez.

M. Jim Eglinski: Il ne s'agit pas de faire dire...

Le président: À l'ordre.

Tout d'abord, monsieur Motz, vous vous écartiez un peu du sujet...

M. Glen Motz: C'est exactement une question de cybersécurité...

Le président: Excusez-moi.

Vous faisiez une digression à propos de ce qui pourrait ou non se passer aujourd'hui et c'est votre interprétation. Cela étant dit, la question de savoir s'il y a eu des discussions entre les représentants de ces entreprises et un ministre, dans la mesure où elles n'étaient pas protégées par le privilège et qu'ils sont prêts à en parler, est une question valable.

M. Glen Motz: Lorsque vous avez soulevé ces questions et qu'on vous a demandé de jouer le jeu de leurs plans dans le budget de l'année dernière... Vous a-t-on déjà expliqué pourquoi le gouvernement ne voulait pas que le public, en particulier, le sache et pourquoi il ne voulait pas que les députés de tous les partis soient au courant des préoccupations que vous avez soulevées au sujet de la cybersécurité?

● (1715)

M. Steve Masnyk: Non.

M. Normand Lafrenière: Il s'agissait surtout de la question des services bancaires ouverts. Nous avions des préoccupations, les mêmes que nous venons d'exprimer et on nous a encouragés à ne pas parler aux députés.

M. Glen Motz: Dans ce projet de loi d'exécution du budget, les libéraux disent que leur intention était de permettre aux entreprises de technologie financière d'avoir accès aux données et de les utiliser pour fournir des services. Est-ce exact?

M. Steve Masnyk: Pas exactement. Cela permettait aux banques de vendre ou de transmettre leurs données à des fournisseurs tiers, y compris les entreprises de technologie financière.

M. Glen Motz: Cela semblait être une mesure législative légitime. Est-ce que, s'ils voulaient vous convaincre, ils pourraient vous montrer un projet de règlement ou vous donner l'occasion de commenter les questions avant... Cela s'est-il produit? Vous a-t-on permis de le faire dans le cas des entreprises de technologie financière?

Le président: Monsieur Motz, vous évoquez des conversations qui ont peut-être eu lieu ou peut-être pas à un autre moment. Nous limitons notre étude au secteur financier, sans aller au-delà. Si vous pouviez concentrer vos questions sur la façon dont ces messieurs peuvent contribuer au concept de banque ouverte, je pense que ce serait utile, par opposition à d'autres domaines.

M. Glen Motz: À propos de cybersécurité et de services bancaires ouverts, connaissez-vous quelqu'un d'autre à qui l'on aurait demandé de ne pas parler aux comités des changements relatifs à l'échange de renseignements entre les banques et d'autres entreprises ou groupes?

Le président: Maintenant, on s'éloigne vraiment du sujet. Je ne crois pas qu'il s'agisse d'une question pertinente et importante pour le Comité à ce stade-ci. Ce que ces messieurs présentent est pertinent pour le Comité et non pas ce qui a pu arriver à d'autres personnes qui font autre chose.

Veuillez autant que possible axer vos questions sur ce qu'eux savent ou ne savent pas et non sur ce que d'autres peuvent savoir ou ne pas savoir.

M. Glen Motz: Bien sûr.

Messieurs, vos membres ont-ils des mécanismes de partage de la cybersécurité ou la plupart d'entre vous appartiennent-ils à d'autres organisations de réduction des menaces ou de sensibilisation?

M. Steve Masnyk: Je ne comprends pas la question.

M. Glen Motz: Avez-vous vos propres mécanismes de cybersécurité? Vous protégez-vous vous-mêmes ou partagez-vous ces mécanismes avec d'autres industries semblables? Est-ce que vous les sous-traitez? Faites-vous appel à des organismes de sensibilisation pour assurer la sécurité de vos données?

M. Normand Lafrenière: Les entreprises membres utilisent des services pour s'assurer que leur système demeure intact.

On croit comprendre que toutes les entreprises font appel à des agents extérieurs différents, si vous voulez, pour les aider à faire cela, ou qu'elles utilisent des compétences internes, des employés internes. Les modalités sont très diverses, mais toutes dépensent de l'argent pour s'assurer que leur système reste intact.

M. Glen Motz: D'accord.

Pas d'autres questions. Merci, monsieur le président.

Le président: Merci, monsieur Motz.

Monsieur Dubé.

M. Matthew Dubé: Merci, monsieur le président.

Je ne veux pas prétendre savoir ce que M. Motz demandait, mais je tiens à dire pour le compte rendu que, d'après mes informations, le gouvernement a tenu des consultations sur la notion de banque ouverte. Si la question allait dans ce sens, sa pertinence pour la discussion ne fait aucun doute, à mon humble avis.

Le président: Si la question avait été formulée de cette façon, elle aurait peut-être été plus appropriée.

M. Jim Eglinski: Il a été continuellement interrompu.

M. Matthew Dubé: Très bien, monsieur le président. Je respecte votre décision, mais il est certain que lorsque l'on fait taire ses collègues à coup de rappels au Règlement, le président a le droit de rendre une décision à ce sujet.

Messieurs, merci d'être ici. Le profane que je suis réclame votre indulgence. Lorsqu'on parle d'applications, je me demande si ça couvre aussi les applications dans les médias sociaux et ce genre de choses. Là où je veux en venir, c'est que dans le cas de Cambridge Analytica, une partie de l'enjeu tenait au fait qu'il y avait une zone grise légale concernant les données qui étaient recueillies lorsqu'un utilisateur de Facebook faisait un de ces tests de personnalité ou quelque chose du genre. En cliquant sur « OK », ils cédaient un tas de données sans s'en rendre compte.

Craignez-vous qu'en ouvrant la porte à une foule de demandes de tiers concernant les services bancaires, quelqu'un puisse, disons, ouvrir une session sur une application dans l'intention légitime de l'utiliser pour une vérification de crédit ou autres choses de ce genre — il existe une offre abondante de tels services —, puis tout simplement parcourir le site, comme beaucoup de gens le font, et cliquer sur « OK », et ce faisant, céder une foule de renseignements financiers très privés?

En soi, ce n'est pas nécessairement mauvais; le gestionnaire de l'application peut les utiliser de façon correcte, mais en cas d'infraction, comme dans le cas d'Equifax, on se rend vite compte que les données sont utilisées à des fins malveillantes — surtout du fait que l'application d'une tierce partie n'a pas nécessairement le même type de protocoles de sécurité en place qu'une grande institution comme l'une des banques, souvent beaucoup plus expérimentée en la matière.

Voilà sans doute une façon longue et alambiquée de poser la question: jusqu'où cela peut-il aller?

● (1720)

M. Steve Masnyk: Pour répondre à votre question, monsieur Dubé... Premièrement, qu'est-ce qu'un consentement explicite et éclairé? À quoi consent une personne lorsqu'elle commence à fréquenter une tierce partie ou une application, qu'elle commence à avoir une relation quelconque? À quoi le consommateur consent-il? Le consommateur comprend-il à quoi il consent? Comment s'y prendre pour révoquer ce consentement? Quelles sont les implications? Peut-on le faire? Les gens lisent-ils les 75 pages où il est écrit: « Êtes-vous d'accord... » lorsqu'ils achètent un produit en ligne? Quelqu'un a-t-il déjà lu ces 75 ou 150 pages, au lieu d'aller tout droit au bas de la page pour donner son accord? Je pense que la grande question est de savoir à quoi les gens consentent.

Une fois que vous avez donné votre consentement aux applications un, deux et trois, ont-elles des relations avec les entreprises de technologie financière a, b, c ou d par la suite? Sait-on vraiment jamais à quoi on consent?

Je pense que si on savait vraiment à quoi on consent, ce serait beaucoup plus logique. Il s'agirait d'un consentement éclairé donné en connaissance de cause. Dans ce cas-ci, en ce qui concerne ces API et ces entreprises de technologie financière, à quoi consent-on vraiment? C'est une des réponses à vos questions, je l'espère.

M. Matthew Dubé: Je me demande comment on pourrait clarifier ce qui est cédé et les conséquences de cela. Autrement dit, ce qui me préoccupe, c'est que la reddition de comptes pourrait être différente pour une application tierce par rapport à un gros joueur comme une banque qui, simplement en raison de la taille de l'entreprise et de son rôle dans la société, a en fin de compte une responsabilité différente envers le public.

La question porte sur la prolifération potentielle de ce phénomène. Faut-il envisager des règles plus strictes concernant la façon dont les données sont traitées et la façon dont elles sont extraites des banques, surtout si cette transaction a lieu sur un appareil qui n'est peut-être pas lui-même sûr?

M. Steve Masnyk: Si j'étais un leader en matière de politique publique, je crois que la généralisation de ces pratiques me terrifierait. Comme je l'ai dit, de 2 000 à 4 000 entreprises de technologie financière sillonnent le pays. Qui sait qui les réglemente, quelles normes elles ont ou quel budget elles consacrent à la protection de la vie privée? On ouvre tout grand les vannes au cyberpiratage massif.

[*Français*]

M. Matthew Dubé: Avez-vous quelque chose à ajouter, monsieur Lafrenière?

M. Normand Lafrenière: Notre position, c'est que le consommateur devrait être le propriétaire de ses renseignements personnels, et non les institutions financières qui les détiennent actuellement. Le consommateur devrait être celui qui décide à qui il communique ses renseignements personnels et financiers. Nous espérons que des standards seront établis en ce qui concerne le transfert de renseignements entre les banques et ces entreprises de technologie financière afin que le risque de perte d'information soit réduit.

Cela étant dit, dans le cas où des informations venant d'une institution financière seraient acheminées à une entreprise de technologie financière qui les perdrait par la suite, l'institution financière se sentirait responsable de la teneur et du maintien de ces informations. Nous ne sommes pas certains que les entreprises de technologie financière qui seront mises en place et qui interviendront dans ce système auront les mêmes standards en matière de protection des renseignements personnels.

● (1725)

M. Matthew Dubé: Ma question concerne les assureurs dans le contexte de cette nouvelle réalité numérique. L'exemple que je vais vous donner est peut-être un peu particulier, mais j'espère que vous allez saisir ce que je veux faire valoir. Au Québec, le Code de la sécurité routière nous oblige à utiliser des pneus d'hiver pendant une période précise de l'année. En Ontario, c'est facultatif, mais cela a une incidence sur les primes d'assurances.

S'inquiète-t-on à l'idée que l'on permette différents standards dans le domaine de la cybersécurité, ce qui pourrait, par exemple, se répercuter sur le montant des primes? Les standards pourraient alors être moins élevés pour certains et plus élevés pour d'autres. Les standards en matière de cybersécurité devraient-ils être uniformes dans votre industrie, de façon à faciliter les transactions et, essentiellement, les assurances?

M. Normand Lafrenière: Oui, dans le cas des entreprises de technologie financière, le système devrait être très fort. Nous savons qu'il l'est dans le cas des institutions financières, des compagnies d'assurance et des banques. Nous voudrions que les entreprises de technologie financière, pour qu'on leur permette de jouer sur ce terrain, adoptent des standards de protection très élevés en matière de renseignements personnels.

[*Traduction*]

Le président: Merci, monsieur Dubé.

Madame McCrimmon, vous avez sept minutes.

Mme Karen McCrimmon: Merci.

Merci beaucoup de votre témoignage et de votre présence aujourd'hui.

Je veux simplement clarifier une chose. Si je vous ai mal compris, veuillez me corriger. Si j'ai bien compris, il y a un risque minimum pour la cybersécurité de vos entreprises ou de vos clients. Est-ce exact?

M. Normand Lafrenière: « Minimum » est probablement un grand mot, mais il y a moins de risque, simplement parce que le type de données que l'on conserve est moins intéressant — sauf pour les numéros de carte de crédit et de carte de débit dont se servent les compagnies d'assurances pour accepter les paiements. À part cela... Encore une fois, suivant votre exemple sur la taille des salles de bain, cela ne présente pas beaucoup d'intérêt pour une tierce partie.

Mme Karen McCrimmon: Vous dites simplement que vous n'êtes pas une cible attrayante.

M. Normand Lafrenière: Nous le sommes moins.

Mme Karen McCrimmon: D'accord. C'est bien.

M. Steve Masnyk: À moins que quelqu'un veuille savoir combien de toilettes il y a dans votre sous-sol... Je suis sûr que quelqu'un trouverait cela très utile de savoir cela, mais...

Mme Karen McCrimmon: Nous allons donc mettre de côté la question de la cybersécurité et parler des services bancaires ouverts. Il est important de ne pas confondre les deux.

Le ministère des Finances vient de tenir des consultations. Y avez-vous participé?

M. Normand Lafrenière: Oui.

Mme Karen McCrimmon: Avez-vous témoigné? J'aurais aimé l'avoir...

M. Normand Lafrenière: Nous n'avons pas témoigné. Nous avons participé aux consultations.

Mme Karen McCrimmon: J'aurais aimé en avoir une copie. Cela aurait été pratique. Nous aurions été mieux placés pour avoir une véritable discussion sur les défis que pose l'ouverture des services bancaires. J'ai fait quelques recherches, mais sans approfondir.

Votre organisation, l'ACCAM, a de la difficulté avec ce système bancaire ouvert. Vous pensez qu'il y a des problèmes importants.

M. Normand Lafrenière: Eh bien, la question qui touche les compagnies d'assurances... Il y a un mur entre les banques et les compagnies d'assurances. Comme vous le savez peut-être, pour revenir aux quatre piliers, un mur sépare les banques et les compagnies d'assurances. Une banque ne peut pas vendre l'assurance de la banque. Elle peut avoir une organisation qui vend de l'assurance, mais complètement distincte de la banque. Les données de la banque ne peuvent pas être partagées avec cet organisme. Le but est d'empêcher la coercition, si je peux m'exprimer ainsi — empêcher que la banque ne force le client à acheter son produit au moment où elle lui accorde un prêt. Donc, les deux sont séparés, non pas pour empêcher les banques de se lancer dans le secteur de l'assurance, mais il faut qu'il y ait des organisations distinctes et qu'il n'y ait pas de partage de données entre les deux.

Avec ces entreprises de technologie financière, ce mur tomberait. Il serait possible pour une banque de partager des données avec une telle entreprise, laquelle pourrait très bien partager ses données avec une tierce organisation, qu'il s'agisse d'une compagnie d'assurances ou d'autre chose. Par conséquent, la séparation ou le mur entre les deux tomberait tout simplement.

Mme Karen McCrimmon: J'ai du mal à comprendre pourquoi l'ACCAM s'y oppose, mais pas l'Association des courtiers d'assurances du Canada. Vous devez vous rendre compte qu'il y a une pièce de ce casse-tête qui nous manque.

● (1730)

M. Steve Masnyk: Madame McCrimmon, l'ACCAM ne s'y oppose pas. L'ACCAM dit qu'il faut établir des paramètres et un cadre qui protègent le droit à la vie privée et qui étendent les normes de protection de la vie privée des banques et des compagnies d'assurances à ces tierces parties ou à ces entreprises de technologie financière. L'ACCAM ne s'y oppose pas. La discussion devrait être guidée par certains principes afin que ce cadre soit mis en place.

Mme Karen McCrimmon: D'accord, mais les courtiers d'assurances ne sont-ils pas exactement du même avis?

M. Steve Masnyk: Je ne sais pas. Je ne parle pas en leur nom.

Mme Karen McCrimmon: Dans le dernier article, on dit que les courtiers et les mutuelles sont divisés sur les tactiques, sur la question de savoir s'il faut appuyer ou non les services bancaires ouverts.

M. Normand Lafrenière: Nous ne sommes pas nécessairement opposés à l'ouverture du système bancaire. Nous disons qu'il devrait y avoir des paramètres à cet égard.

Mme Karen McCrimmon: D'accord.

M. Normand Lafrenière: De plus, il y a un mur qui sépare les banques et les compagnies d'assurances. Dans le cadre du nouveau système, dans le cadre d'une banque ouverte, on aimerait que ce mur soit maintenu.

Mme Karen McCrimmon: De toute évidence, vous avez des préoccupations que l'Association des courtiers d'assurances du Canada n'a pas.

M. Normand Lafrenière: C'est peut-être le cas.

Mme Karen McCrimmon: Voilà le problème. Ce serait vraiment bien si nous pouvions obtenir les choses à l'avance...

M. Normand Lafrenière: Absolument.

Mme Karen McCrimmon: ... pour que nous puissions nous préparer à vous poser des questions.

Parlons des services bancaires ouverts. Ne pensez-vous pas qu'il y a des façons d'atténuer ces risques, ou craignez-vous simplement que nous ne soyons pas au courant de tous les risques?

M. Steve Masnyk: Nous croyons qu'un système de banque ouverte est beaucoup plus exposé aux cyberrisques et au cyberpiratage que le régime actuel. Comme je l'ai dit, les banques consacrent beaucoup d'argent aux normes de protection de la vie privée et malgré cela, elles se font pirater, alors qu'en est-il de ces nouveaux venus, des entreprises de technologie financière, qui dépenseraient probablement très peu comparativement aux banques ou aux compagnies d'assurances? Les décideurs publics, comme vous, doivent garder cela à l'esprit lorsqu'ils élaborent des politiques publiques à ce sujet. C'est vraiment la question que nous soulevons.

Mme Karen McCrimmon: D'accord.

J'ai bien aimé ce que vous avez dit au sujet du consentement complet et éclairé. Comment pouvons-nous améliorer cela? Quelles sont les approches qui s'offrent à nous?

M. Steve Masnyk: Je ne suis ni un expert en cybernétique ni un expert en technologie. Il vous faudrait probablement quelqu'un de beaucoup plus compétent sur ce sujet.

Mme Karen McCrimmon: D'autres pays ont adopté ce système bancaire ouvert. Ils doivent être protégés.

M. Steve Masnyk: La plupart des pays européens qui ont adopté cette mesure ont un gouvernement unitaire, alors il n'y a pas d'arbitrage entre le provincial et le fédéral. Les règles qui s'appliquent aux banques, aux interfaces de programmation d'applications et aux technologies financières s'appliqueraient à l'ensemble du pays. Ils n'ont pas de fédérations, essentiellement.

Mme Karen McCrimmon: C'est un défi, cela ne fait aucun doute.

M. Normand Lafrenière: La plupart des entreprises de technologie financière sont constituées en vertu d'une loi provinciale et ne sont pas réglementées. Ce sera un nouveau monde pour ce qui est de savoir si elles doivent être réglementées et par qui.

Mme Karen McCrimmon: D'accord.

M. Steve Masnyk: Il y a un exemple au Royaume-Uni...

Le président: Madame McCrimmon, il vous reste 15 secondes.

Mme Karen McCrimmon: C'est bien. Merci.

Le président: Avant de passer à M. Eglinski, de quelle étude parlez-vous? S'agit-il d'une étude du Comité des finances ou d'une étude du ministère sur cette question?

M. Normand Lafrenière: Le ministère tient des consultations.

Le président: D'accord.

M. Normand Lafrenière: C'est le ministère qui a demandé les consultations. Il a mis sur pied un comité qui...

Le président: Cette étude a-t-elle été publiée?

M. Normand Lafrenière: Non, pas encore.

Le président: D'accord.

Monsieur Eglinski.

M. Jim Eglinski: J'adresserai mes questions à M. MacKenzie.

Le président: Monsieur MacKenzie, bienvenue encore une fois au Comité.

M. Dave MacKenzie (Oxford, PCC): Merci, monsieur le président. Oui, je suis tout nouveau.

Je remercie les témoins de leur présence.

L'une des choses intéressantes... Vous parlez des mutuelles et elles constituent, je pense, une partie importante de l'équation, mais il y a davantage à dire aussi sur les compagnies d'assurances. Je sais que vous parlez plutôt de l'assurance responsabilité civile des mutuelles, mais aujourd'hui les grandes compagnies d'assurances, comme Sun Life ou Manuvie, offrent aussi des services quasi financiers ou des hypothèques et tout le reste.

Le partage de ces renseignements et le couplement des services d'une institution financière, comme une banque, avec ce genre de compagnies d'assurances mettraient beaucoup de renseignements sur les consommateurs à la disposition des agences d'assurances. Cette évaluation vous semble-t-elle juste?

● (1735)

M. Steve Masnyk: Je vais essayer de répondre à la question.

L'interdiction est à sens unique, elle vise les banques qui font de l'assurance et non les compagnies d'assurances qui offrent des produits bancaires. Pourquoi l'interdiction est-elle à sens unique? Parce que les banques font le commerce du crédit et que le crédit est un outil très puissant. Si puissant qu'on peut s'en servir pour forcer un consommateur à acheter d'autres produits. Voilà pourquoi.

Vous avez mentionné Manuvie. Manuvie a une banque et cette banque suit les mêmes règles que les cinq grandes banques.

M. Dave MacKenzie: Manuvie a une banque ou bien est-elle associée à une banque pour faire ses transactions bancaires?

M. Steve Masnyk: Elle a une banque qui s'appelle Banque Manuvie ou Manuvie One, je crois. Je ne suis pas sûr du nom.

M. Dave MacKenzie: Il y en a actuellement qui disent être des banques, mais je pense qu'elles sont associées par l'entremise de l'une des banques à charte.

Quoi qu'il en soit, tout cela mis à part, l'autre aspect, c'est que les banques ont presque toutes des établissements dans d'autres pays, je pense. La plupart sont aux États-Unis, d'autres en Amérique du Sud et d'autres en Europe. Lorsque des renseignements sont transmis à une banque canadienne qui a des filiales dans d'autres pays qui peuvent ou non avoir les mêmes règles en matière d'assurance, voyez-vous là un problème?

M. Steve Masnyk: C'est aux autorités compétentes de décider. Les banques canadiennes exercent leurs activités au Canada en vertu des lois canadiennes. Une banque canadienne exerçant ses activités aux États-Unis serait assujettie à la loi américaine ou à la loi de l'État.

M. Dave MacKenzie: Je n'en disconviens pas, mais l'accès à l'information pourrait très bien être également accessible aux établissements de la banque à l'étranger.

TD Canada Trust est probablement la plus connue au Canada et aux États-Unis. Ses succursales sont...

M. Normand Lafrenière: Il y a plus de succursales du côté américain, je crois.

M. Dave MacKenzie: Oui. Vous pouvez faire vos opérations bancaires à TD aux États-Unis — où on l'appelle TD; on ne dit pas « Canada Trust » — et votre compte bancaire est directement relié à votre compte bancaire au Canada.

On peut bien avoir nos règles au Canada et nos règles dans les provinces, mais une fois que ladite banque dispose de l'information, qu'est-ce qui pourrait l'empêcher — dans le cadre de ce qui a été proposé — de la vendre à une autre entreprise de technologie financière?

M. Steve Masnyk: Je ne sais pas. Dans le cas de TD, il faudrait probablement poser la question à TD.

M. Dave MacKenzie: Cela vous préoccupe-t-il?

M. Steve Masnyk: Je ne sais pas comment fonctionne TD ou les autres banques. Il vous faudrait leur poser la question.

M. Dave MacKenzie: C'est l'échange transfrontalier de renseignements qui me préoccupe. On passe des accords un jour et, le lendemain, la technologie vient tout bouleverser. C'est ce qui m'inquiète. Je sais que le président a été sensible à l'article du *Globe and Mail* d'il y a quelques mois, mais le gouvernement a sans doute une bonne raison de ne pas vouloir en parler. C'est ça qui m'inquiète.

M. Steve Masnyk: Je n'ai rien à ajouter à ce sujet.

M. Normand Lafrenière: Les deux articles de la loi qui ont été approuvés dans le budget de l'an dernier permettaient essentiellement aux banques ou aux institutions financières d'échanger des renseignements avec d'autres organisations. Ils leur permettaient de vendre, de transmettre ou d'échanger des renseignements avec des entreprises en technologie financière.

Ce sont les préoccupations que l'on avait exprimées à l'époque. Qu'en est-il aujourd'hui? Qui va contrôler cette information? Ce sera le consommateur ou l'institution financière? On ne fait que soulever des questions qui nécessitent des réponses.

M. Dave MacKenzie: Merci.

Le président: Merci, monsieur MacKenzie.

[*Français*]

Monsieur Picard, vous avez la parole pour cinq minutes.

M. Michel Picard: Merci, monsieur le président.

Monsieur Lafrenière, est-ce que des compagnies d'assurance-vie font partie de votre association?

M. Normand Lafrenière: Non, seules des compagnies d'assurances générales en font partie.

M. Michel Picard: D'accord.

Par ailleurs, personne ne se soucie que j'aie un ou deux réfrigérateurs dans mon appartement. Je suis d'accord avec vous. Par contre, le fait que j'en aie trois ou quatre ou encore que je possède des biens d'une certaine valeur va peut-être intéresser les gens qui veulent savoir quelle est ma situation personnelle. N'êtes-vous pas d'avis que des renseignements personnels particuliers qui vous semblent anodins peuvent, dans un autre contexte, être extrêmement importants?

● (1740)

M. Normand Lafrenière: Oui.

M. Michel Picard: Les nouvelles dispositions permettent l'échange d'informations, comme vous l'avez mentionné tout à l'heure, de sorte que les compagnies d'assurance peuvent obtenir de l'information auprès des banques. Pourriez-vous préciser la nature de ces échanges?

M. Normand Lafrenière: Ce n'est toujours pas en application. Cela doit être réglementé.

M. Michel Picard: D'accord.

M. Normand Lafrenière: La loi a été changée pour permettre cela, mais il faut que les règlements soient mis en vigueur. Or ils ne le sont pas.

M. Michel Picard: D'accord.

M. Normand Lafrenière: Ils ne sont pas en vigueur parce qu'il y a justement des études sur le système bancaire ouvert à l'heure actuelle. C'est ce que l'on cherche à déterminer.

M. Michel Picard: Est-ce que certaines transactions faites par des membres de votre association peuvent être considérées comme une forme de transaction financière, comportant en quelque sorte un certain bénéfice commercial?

M. Normand Lafrenière: Bien sûr, comme nous faisons partie des institutions financières, nous faisons des échanges financiers. Étant donné que les gens paient leurs assurances, cela en fait partie.

M. Michel Picard: Comment comparez-vous le niveau de protection de vos systèmes par rapport à celui des banques?

M. Normand Lafrenière: La protection de nos systèmes est très bonne.

M. Michel Picard: Comment se compare-t-elle à celle des banques?

M. Normand Lafrenière: Je ne connais pas celle des banques, mais je peux vous dire que nos membres déboursent beaucoup d'argent pour veiller à la protection de leurs systèmes.

M. Michel Picard: Qui sont ces sociétés membres?

M. Normand Lafrenière: Des sociétés d'assurance mutuelles.

M. Michel Picard: À votre connaissance, la proportion que représente le montant des investissements de vos membres en matière de sécurité par rapport à celui de leurs opérations courantes se compare-t-elle à celle du domaine bancaire?

M. Normand Lafrenière: Certainement.

M. Michel Picard: C'est donc une supposition pour l'instant, vu que nous ne disposons pas de cette information. Est-ce exact?

M. Normand Lafrenière: Nous n'avons effectivement pas l'information, mais en pourcentage, c'est certainement le cas.

M. Michel Picard: Dans votre industrie, comment définissez-vous une menace cybernétique?

M. Normand Lafrenière: C'est la possibilité, pour une tierce partie, de pénétrer dans nos systèmes et d'aller y chercher de l'information.

M. Michel Picard: À ce moment-ci, quels sont vos critères de recrutement du personnel pour vous assurer que vous avez un certain contrôle relativement au risque humain?

M. Normand Lafrenière: Personnellement, je ne fais que représenter l'association. Ce n'est pas notre personnel; ce sont les compagnies qui engagent du personnel et qui ont les systèmes informatiques.

Malheureusement, je ne peux pas répondre à cette question.

M. Michel Picard: Pour l'instant, existe-t-il un lien quelconque ou un échange informatique entre vos membres et les banques?

M. Normand Lafrenière: Non.

M. Michel Picard: Pour l'instant, il n'y a aucun accès. Donc, il est raisonnable de croire que les membres de votre association ne représentent pas une porte d'entrée vulnérable dans le système bancaire, par personne interposée.

M. Normand Lafrenière: Absolument.

M. Michel Picard: Merci.

J'ai terminé, monsieur le président.

[*Traduction*]

Le président: Merci, monsieur Picard. Vous avez posé l'avant-dernière question et j'aimerais poser la dernière avant de lever la séance.

Je me demande si vous minimisez l'importance des données que vous détenez. Vous parlez sans cesse du nombre de salles de bain et qui s'en soucie, mais en fait, cela peut constituer des données pertinentes pour certaines personnes malintentionnées.

Je me demande si, en fait, vous n'adoptez pas une approche un peu trop désinvolte à l'égard de votre propre cybersécurité, du point de vue de la protection des données, parce que — et notre comité est sans doute plus sensibilisé à la question — on ne sait jamais vraiment comment des personnes ayant des intentions malveillantes peuvent utiliser ces données contre les titulaires de police et les institutions elles-mêmes.

Je vous renvoie à une poursuite de 100 millions de dollars contre Zurich Insurance. Dans les procès sur la cybersécurité, qui révèlent soudainement aux détenteurs des données leur importance jusque-là insoupçonnée, on voit tout le monde être saisi de tournis.

J'aimerais savoir ce que vous pensez de la valeur de vos données.

M. Normand Lafrenière: On est toujours attentif aux données que l'on détient. On détient des renseignements personnels, des noms, des adresses et ce genre de choses. Bien sûr, on ne peut pas demander autant de renseignements que d'autres, combien vous gagnez, quel est votre travail et ce genre de choses. C'est différent de ce que demandent les compagnies d'assurances. Elles veulent savoir quel genre d'utilisation vous faites de votre véhicule. C'est le genre de renseignements qu'elles demandent et que contiennent leurs dossiers.

● (1745)

Le président: Google est à l'affût de tout ce que je fais avec ma voiture. Quand je l'ai prise au garage dimanche matin, Google m'a dit qu'il me fallait 21 minutes pour me rendre à mon église. Il était un peu surpris, je pense, que je sois allé à l'église.

Des données que je qualifierais d'anodines se chargent de sens entre d'autres mains.

M. Steve Masnyk: Monsieur le président, vous avez tout à fait raison. On ne sait pas ce que l'on ne sait pas jusqu'à ce que quelqu'un découvre ce que l'on ne sait pas et cela devient précieux.

Le président: Oui.

M. Steve Masnyk: Peut-être ne prend-on pas toute la mesure du problème, mais c'est une question de degré. Les banques et les institutions financières ont 100 000 fois plus de données sur vous en tant que consommateur qu'une compagnie d'assurances. Bien sûr, les compagnies d'assurances possèdent des données personnelles, de même que les courtiers, les agents et ainsi de suite, mais c'est une question de degré.

Le président: Je n'insisterai pas, mais votre argument ne me convainc guère.

Quoi qu'il en soit, je vous en remercie.

Sur ce, la séance est levée.