CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 152 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le lundi 18 mars 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le lundi 18 mars 2019

● (1545)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): J'ai le privilège d'ouvrir la séance et d'inviter les représentants de l'Association des banquiers canadiens et de la Chambre de commerce du Canada à s'adresser au Comité. On a informé les deux groupes des paramètres pour les exposés.

Avez-vous joué à roche-papier-ciseaux pour savoir qui commencera, ou allons-nous tout simplement donner la parole à l'Association des banquiers canadiens.

Allez-y, monsieur Docherty.

M. Charles Docherty (avocat général adjoint, Association des banquiers canadiens): Merci beaucoup. Bonjour.

Je tiens à remercier le Comité pour cette occasion de pouvoir vous parler aujourd'hui de cybersécurité et du secteur financier.

Je m'appelle Charles Docherty. Je suis avocat général adjoint de l'Association des banquiers canadiens, ou l'ABC. Se joint à moi mon collègue Andrew Ross, directeur, Paiements et Cybersécurité.

L'ABC est la voix de plus de 60 banques canadiennes et étrangères qui contribuent à l'essor et à la prospérité économiques du pays. L'ABC préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique capable d'aider les Canadiens à atteindre leurs objectifs financiers.

Les banques au Canada sont des chefs de file de la cybersécurité. Elles ont massivement investi dans les mesures de protection du système financier et des renseignements personnels de leurs clients contre les cybermenaces. Malgré le nombre croissant de tentatives, les banques affichent un excellent bilan en matière de protection de leurs systèmes contre les cybermenaces. En effet, elles prennent au sérieux la confiance que les Canadiens leur accordent pour garder en sécurité leurs dépôts ainsi que leurs renseignements personnels et financiers.

Par ailleurs, les Canadiens s'attendent à plus de simplicité dans l'obtention de services financiers. Les banques ont innové en vue d'assurer à leurs clients des modes d'accès et d'utilisation plus rapides et plus pratiques lorsqu'il s'agit de services bancaires. Les consommateurs peuvent accéder aux services bancaires pratiquement n'importe quand et de n'importe où dans le monde grâce aux services en ligne et aux applications mobiles qui leur donnent un accès en temps réel à leurs renseignements financiers. Aujourd'hui, au Canada, 76 % des consommateurs utilisent principalement les services bancaires en ligne et sur leurs appareils mobiles, une hausse par rapport aux 52 % d'il y a tout juste quatre ans. Avec l'augmentation des opérations effectuées électroniquement, les réseaux et les systèmes deviennent de plus en plus interconnectés. Ainsi, les banques, le gouvernement et d'autres secteurs doivent collaborer pour veiller à ce que le cadre de la cybersécurité au Canada soit solide et capable de s'adapter à l'économie numérique.

L'ABC a participé activement aux consultations lancées par Sécurité publique Canada sur l'examen de la Stratégie nationale de cybersécurité. Notre secteur est un partenaire actif, motivé à faire cause commune avec le gouvernement fédéral pour atteindre les objectifs décrits dans la stratégie, l'objectif commun étant de faire évoluer la cyberrésilience au Canada.

Le secteur bancaire appuie vivement la démarche du gouvernement fédéral visant la mise sur pied du Centre canadien pour la cybersécurité, sous la gouverne du Centre de la sécurité des communications, à titre de point de contact unique où obtenir, auprès de spécialistes, des avis, des conseils et du soutien au sujet de questions opérationnelles de sécurité. Nous accueillons également la création de l'unité centralisée de lutte contre la cybercriminalité de la GRC.

Une des priorités clés du nouveau centre sera de veiller à ce que les secteurs clés au Canada soient cyberrésilients. Pour ce faire, le Centre devra encourager un environnement de collaboration et agir comme point de contact vers lequel les secteurs public et privé pourront se tourner pour obtenir conseils et directives en la matière.

La sécurité des infrastructures essentielles du Canada doit être assurée afin de protéger la sécurité et le bien-être économique des Canadiens. Le secteur bancaire compte sur d'autres secteurs qui représentent des infrastructures névralgiques, comme les télécommunications et l'énergie, pour offrir des services financiers aux Canadiens. Nous encourageons le gouvernement à utiliser et à promouvoir des normes de cybersécurité sectorielles communes qui s'appliqueraient aux entités formant ces secteurs névralgiques.

Nous sommes conscients que certaines infrastructures essentielles, comme l'énergie, relèvent de diverses autorités. Ainsi, nous recommandons au gouvernement fédéral de collaborer avec les provinces et les territoires à la définition d'un cadre de cybersécurité qui s'applique à l'ensemble des secteurs infrastructurels essentiels. Des normes de cybersécurité cohérentes et bien définies permettront une supervision plus rigoureuse et donneront l'assurance que les systèmes sont efficaces et bien protégés.

Une communication efficace des renseignements sur les cybermenaces et de l'expertise sur la protection est une composante essentielle de la cyberrésilience, qui devient de plus en plus importante dans l'économie canadienne axée sur le numérique et les données. Les avantages de la communication des renseignements sur les cybermenaces s'étendent à d'autres secteurs que les finances, au gouvernement et aux forces de l'ordre notamment, en leur permettant de minimiser l'impact des cyberattaques. Les banques appuient des initiatives — et y participent activement — comme l'Échange canadien des menaces cybernétiques, un organisme qui fait la promotion de l'échange d'information sur la cybersécurité et les pratiques exemplaires entre le gouvernement fédéral et les entreprises en vue d'améliorer la cyberrésilience à travers l'ensemble des secteurs.

Afin d'encourager la communication de renseignements et d'assurer l'efficacité de tels forums, nous recommandons au gouvernement d'envisager la voie législative, par exemple en modifiant la législation en matière de renseignements personnels et en ajoutant des dispositions refuge, ce qui ajoutera les protections adéquates lors de la communication d'information sur les cybermenaces.

La protection contre les menaces posées par les entreprises ou par d'autres pays nécessite une bonne défense coordonnée entre le gouvernement et le secteur privé. Le gouvernement peut donc jouer un rôle central dans la coordination entre les partenaires représentant des infrastructures essentielles et les autres intervenants, mettant à profit les efforts en cours pour limiter les cybermenaces. L'établissement de processus clairs et simplifiés entre les principaux acteurs augmentera la capacité du Canada à répondre efficacement aux cybermenaces et à s'en protéger.

Nous comprenons que le gouvernement compte introduire un nouveau cadre législatif qui traitera des répercussions et des obligations dans un monde de plus en plus interconnecté. Nous serons ravis de discuter de ce cadre avec le gouvernement.

Par ailleurs, l'ABC est d'avis que la sensibilisation à la cybersécurité auprès des Canadiens est essentielle. La sensibilisation de la population est, et doit être, la responsabilité à la fois du gouvernement et du secteur privé. Veiller à ce que les particuliers participent activement aux efforts de lutte contre les cybermenaces passe par des connaissances générales du sujet et par une prise de conscience individuelle de la responsabilité de chacun à ce sujet. Le secteur bancaire sera heureux de collaborer davantage avec le gouvernement sur les initiatives publiques de sensibilisation et de responsabilisation, comme l'ajout de la cybersécurité aux efforts fédéraux de promotion de la littératie financière.

Une main-d'oeuvre compétente en matière de cybersécurité capable de s'adapter à une économie axée sur le numérique et les données est également importante non seulement pour notre secteur, mais aussi pour tous les Canadiens. Chaque année, l'ABC travaille avec ses membres à l'organisation de l'un des plus grands sommets sur la cybersécurité au Canada réunissant les responsables des banques avec les principaux experts pour parler des plus récentes menaces et consolider ainsi les connaissances de nos professionnels de la cybersécurité.

La hausse des cybermenaces engendre une plus grande demande de talent en cybersécurité au Canada et ailleurs. La nouvelle stratégie canadienne en matière de cybersécurité reconnaît que les lacunes actuelles de talent dans ce domaine représentent à la fois un défi et une occasion pour notre pays. Afin de remédier à ce manque, nous encourageons le gouvernement fédéral, en collaboration avec les provinces et territoires, à promouvoir l'établissement de programmes de cybersécurité dans les écoles, les collèges et les universités, ainsi que des programmes d'éducation permanente dans l'objectif de permettre aux étudiants de développer leurs compétences en cybersécurité.

Pour conclure, j'aimerais rappeler que la cybersécurité est en haut des priorités des banques au Canada qui continuent à collaborer et à investir dans la protection des renseignements personnels et financiers de leurs clients. Aussi, les banques appuient le travail du gouvernement dans la protection des consommateurs tout en encourageant l'innovation et la concurrence. Toutefois, le secteur est conscient du fait que les menaces et les défis évoluent constamment. Nous désirons collaborer davantage avec le gouvernement et les autres secteurs pour que le Canada demeure un lieu stable, solide et sécuritaire où faire des affaires.

Merci beaucoup de votre temps. Je suis impatient de répondre à vos questions.

● (1550)

Le président: Merci, monsieur Docherty.

Nous passons maintenant à la Chambre de commerce du Canada.

[*Français*]

M. Trevin Stratton (économiste en chef, Chambre de commerce du Canada): Merci beaucoup, monsieur le président et membres du Comité. C'est un grand plaisir d'être parmi vous aujourd'hui.

[*Traduction*]

Je m'appelle Trevin Stratton. Je suis économiste en chef à la Chambre de commerce du Canada. La Chambre de commerce est la porte-parole du milieu des affaires au Canada et représente un réseau de plus de 200 000 entreprises de toutes tailles, de tous les secteurs et de toutes les régions. Je suis accompagné de mon collègue de la chambre, Scott Smith, qui est directeur principal, Propriété intellectuelle et politique d'innovation.

Les transactions bancaires se font de plus en plus souvent de nouvelles façons, alors que 72 % des Canadiens les effectuent surtout en ligne ou à l'aide d'un appareil mobile. Des attaques perturbatrices ou destructrices contre le secteur financier pourraient donc avoir des répercussions importantes sur l'économie canadienne et menacer la stabilité financière. Cette situation pourrait survenir directement sous forme de pertes de revenu, ainsi qu'indirectement avec la détérioration de la confiance des consommateurs et des répercussions qui se feront sentir au-delà du secteur financier, sur lequel reposent d'autres secteurs de l'économie. Par exemple, les cyberattaques qui perturbent les services essentiels, qui minent la confiance envers certaines entreprises, ou le marché proprement dit, ou qui nuisent à l'intégrité des données pourraient avoir des conséquences systémiques sur l'ensemble de l'économie canadienne.

Les banques ont investi massivement dans des mesures ultra-modernes de cybersécurité pour protéger le système financier et les renseignements personnels de leurs consommateurs contre les cyberattaques. En fait, les mesures et les procédures de cybersécurité font partie de l'approche globale des banques en matière de sécurité, ce qui comprend des équipes d'experts qui surveillent les transactions, qui préviennent et détectent les fraudes, et qui assurent la sécurité des comptes clients.

Les systèmes de sécurité sophistiqués qui sont en place protègent les renseignements personnels et financiers des clients. Les banques surveillent activement leurs réseaux et effectuent sans cesse une maintenance de routine pour faire en sorte que les menaces en ligne n'endommagent pas leurs serveurs et ne perturbent pas les services offerts aux clients.

Cependant, les questions de cybersécurité sont caractérisées par d'importantes asymétries de l'information, alors que de grandes institutions comme le gouvernement fédéral, la Banque du Canada et quelques entreprises du secteur privé, y compris des institutions financières, possèdent une quantité disproportionnée du renseignement et de la capacité. Pourtant, les PME sont aussi vulnérables. Il est important pour elles de mettre en place un écosystème de cybersécurité. Elles sont également confrontées à des asymétries croissantes sur le plan des ressources, de la technologie et des compétences pour se défendre contre des adversaires malveillants qui, avec des compétences et des ressources relativement rudimentaires, peuvent causer d'importants dommages financiers et nuire grandement à leur réputation.

Mon collègue, Scott Smith, va maintenant décrire les cybermenaces auxquelles font face les PME du Canada.

● (1555)

M. Scott Smith (directeur principal, Propriété intellectuelle et politique d'innovation, Chambre de commerce du Canada): Je crois que vous avez entendu au cours des derniers mois plusieurs témoins au sujet des cybermenaces en constante évolution, de certaines des attaques subies de façon générale, de la façon dont la situation change et du problème que cela pose. Aujourd'hui, je vais plutôt attirer votre attention sur la surface d'attaque croissante et sur la façon dont les perturbations économiques ayant une incidence sur la sécurité nationale viennent parfois d'endroits inattendus.

Le bien-être économique du Canada repose sur les petites entreprises. Même si 99,7 % des entreprises au Canada comptent moins de 500 employés, elles emploient plus de 70 % de la main-d'œuvre du secteur privé. Les PME représentent 50 % du PIB du Canada, 75 % du secteur des services et 44 % du secteur de la production de biens. Elles représentent également 39 % du secteur des finances, des assurances et des biens immobiliers.

On s'attend à ce que le taux de croissance continue annuel du secteur de la technologie financière soit de 55 % en 2020. Le Canada est un centre névralgique de la croissance du secteur de la technologie financière, surtout pour ce qui est des paiements mobiles, et la majorité des nouvelles entreprises sont des PME. Ensemble, elles constituent une très grande surface d'attaque, qui a d'ailleurs attiré l'attention des pirates informatiques.

Pour donner des exemples du lien entre les chaînes d'approvisionnement et les perturbations majeures, en 2018, cinq exploitants de gazoducs ont vu leurs activités être perturbées lorsqu'un fournisseur tiers de données électroniques et de services de communication a été victime d'un piratage au printemps. Le piratage d'un fournisseur tiers de plus de 100 entreprises manufacturières a été découvert en juillet 2018. Environ 157 gigaoctets de données que possédait Level One Robotics ont été exposés au moyen de la synchronisation à distance, qui est un protocole de transfert de fichiers couramment utilisé pour copier ou sauvegarder de grands ensembles de données sur d'autres serveurs.

En 2017, l'infection par le maliciel NotPetya a forcé le géant du transport Maersk à remplacer 4 000 serveurs, 45 000 ordinateurs personnels et 25 applications sur une période de 10 jours, ce qui a entraîné d'importantes perturbations.

Qu'est-ce qui explique le problème? Les criminels sont un peu comme les eaux de crue, qui empruntent la voie de la moindre résistance. Les PME font face à plusieurs difficultés en matière de sécurité: des ressources financières limitées, des ressources humaines limitées et une culture d'incrédulité, à savoir la fausse idée selon laquelle elles sont trop petites pour être victimes de piratage.

L'économie numérique s'est révélée être une bénédiction pour la croissance des petites entreprises, car elle leur a permis d'entrer dans les chaînes d'approvisionnement mondiales. Cependant, cette innovation et cette croissance s'accompagnent d'un risque si on ne donne pas suite aux préoccupations en matière de sécurité, surtout compte tenu de la sophistication des cybercriminels. Ils sont passés des perturbations attribuables aux virus, aux chevaux de Troie et des vers informatiques il y a 10 ans, dont on entendait couramment parler, à la production de certificats numériques de sécurité qui permettent de contourner le facteur humain.

L'objectif doit être la réduction de la surface d'attaque, en faisant des entreprises canadiennes des cibles moins intéressantes pour les criminelles. La solution est un changement de culture, grâce à l'éducation, à la sensibilisation et à l'établissement de normes de l'industrie, sans étouffer l'innovation. C'est un grand défi. Cela signifie qu'il faut investir dans les relations et les capacités relatives à l'application de la loi pénale à l'échelle internationale.

Je vais m'arrêter ici. C'est avec plaisir que je répondrai aux questions.

Le président: Merci à vous deux.

Notre premier intervenant est M. Picard.

[*Français*]

Vous avez sept minutes.

M. Michel Picard (Montarville, Lib.): Merci, monsieur le président.

Messieurs, bienvenue à notre comité.

[*Traduction*]

Je vais poser ma question en français, si vous voulez bien mettre votre oreillette pour entendre la traduction.

[*Français*]

Ma question s'adresse d'abord aux gens de l'Association des banquiers canadiens, puisqu'ils travaillent dans le secteur financier, qui est l'objet de notre étude.

Quelle stratégie avez-vous utilisée pour élaborer votre programme de cybersécurité? Quels sont les angles ou les opérations de vos clients que vous avez pris en compte pour établir les étapes menant à l'établissement de mesures de cybersécurité?

● (1600)

[*Traduction*]

Le président: À qui posez-vous la question?

M. Michel Picard: Elle s'adresse à l'association des banquiers.

M. Charles Docherty: Le secteur bancaire prend très au sérieux ses responsabilités pour protéger les renseignements des clients. Nous sommes reconnaissants de la confiance qu'ils nous accordent pour protéger leurs renseignements personnels.

Sur le plan stratégique, les banques — qui protègent déjà leurs propres systèmes et leur propre infrastructure — contribuent aussi à la cyberrésilience partout au Canada. Ils apportent une énorme contribution à l'Échange canadien des menaces cybernétiques ce qui permet non seulement aux banques, mais aussi à d'autres secteurs d'avoir accès à de l'information concernant les cyberincidents et les menaces. Bien entendu, elles ont investi des milliards de dollars pour que leurs infrastructures informatiques soient sûres et sécuritaires.

[*Français*]

M. Michel Picard: J'aimerais que votre approche soit plus concrète.

Le but de cette étude est de demander au secteur privé, notamment à votre association, de nous aider à trouver des moyens d'améliorer notre infrastructure de services financiers.

Vous êtes dans le secteur financier. Nous savons que vous gérez des données personnelles. Sur le terrain, vous avez commencé quelque part: quelqu'un s'est réveillé un matin et a décidé de commencer par examiner tel type d'opérations, par utiliser tels outils, par se pencher sur tel secteur des services bancaires. En effet, vous avez toute une diversité de services financiers. Pouvez-vous résumer le processus qui a mené à l'élaboration de votre stratégie en cybersécurité?

[*Traduction*]

M. Andrew Ross (directeur, Paiements et Cybersécurité, Association des banquiers canadiens): De toute évidence, c'est un milieu en constante évolution et notre stratégie évolue parallèlement.

Au bout du compte, les banques ont recours à des cadres rigoureux de gestion des risques pour évaluer les différentes menaces qu'elles observent.

Comme mon collègue l'a mentionné, nous croyons notamment être doués pour détecter les cybermenaces. Nous avons également contribué à la stratégie du gouvernement. Je pense qu'un aspect pour lequel nous pouvons en faire plus est celui de la communication de l'information, pour apporter des améliorations non seulement au secteur financier proprement dit, mais aussi au-delà.

Au bout du compte, c'est une question d'atténuation des risques. Il faut cerner les menaces sur lesquelles il faut se pencher, les évaluer et se défendre contre elles.

M. Michel Picard: Bien.

J'ai le choix entre deux questions épineuses.

Tout d'abord, pourquoi les banques demandent-elles à leurs clients de payer des frais pour souscrire une protection supplémentaire contre le vol d'identité? Je croyais que lorsque je faisais affaire avec les banques, comme je dois leur donner tous mes précieux renseignements, elles allaient s'en occuper sans que je doive payer davantage pour faire protéger les mêmes renseignements. Est-ce parce que votre système ne protège pas assez mon identité? Ou est-ce tout simplement une opération de marketing?

M. Charles Docherty: Comme je l'ai mentionné d'emblée, les banques prennent très au sérieux leurs responsabilités pour protéger les renseignements personnels de leurs clients. Elles offrent des produits et des services à leurs clients afin que leurs renseignements personnels demeurent en sécurité.

Je ne peux pas parler précisément du modèle économique auquel vous faites allusion et qui consiste à demander des frais supplémentaires pour la surveillance de renseignements sur l'identité. Cela dit, dans certains cas, si un client veut qu'une surveillance supplémentaire soit exercée, il devrait pouvoir opter pour une surveillance plus étroite de ses renseignements personnels. Dans ce cas, c'est un produit ou un service qu'une banque pourrait être disposée à lui offrir.

M. Michel Picard: Donc, si je comprends bien, je peux dire sans me tromper que mes renseignements personnels sont en sécurité dans les banques au Canada, puisqu'elles ont tous les moyens et tous les outils pour les protéger.

M. Charles Docherty: Tout à fait.

M. Michel Picard: Excellent.

À propos de la communication de l'information, nous parlons de plus en plus du système bancaire ouvert. Quelle est votre opinion à ce sujet?

M. Andrew Ross: Nous participons certainement aux consultations entamées par le ministère des Finances pour examiner le bien-fondé du système bancaire ouvert.

De notre point de vue, le secteur appuie l'innovation et la concurrence dans les services financiers. Comme nous l'avons expliqué, nous devons examiner non seulement les avantages, mais aussi les risques associés au système bancaire ouvert. La cybersécurité est un de ces éléments. Si ces consultations nous permettent en tant que pays d'atténuer ces risques ainsi que de cerner et de voir les avantages, nous pensons que nous serons favorables à un système bancaire ouvert.

● (1605)

M. Michel Picard: Quelle est la nature des risques que vous avez cernés dans votre entreprise?

M. Andrew Ross: Comme je l'ai dit précédemment, il risque d'y avoir, dans l'espace financier, d'autres joueurs qui n'ont peut-être pas les mêmes ressources qu'une banque. Je crois que c'en est un.

En général, plus il y a d'entités qui interviennent, plus il y a une multitude de canaux interconnectés, plus les risques de cybermenace sont grands.

M. Michel Picard: Merci, messieurs.

[*Français*]

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

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

Bonjour, messieurs. Je vous remercie d'être parmi nous.

En matière de banques, il y a le volet qui s'adresse aux entreprises et le volet qui s'adresse aux particuliers. Comme je possède des entreprises, je sais que des technologies comme celles de SecureKey sont requises pour accéder aux comptes. L'accès à un compte d'entreprise est très complexe, comparativement à l'accès à un compte personnel.

Mon collègue a posé cette question, mais j'aimerais savoir si, de l'extérieur, il est plus facile d'attaquer un compte d'entreprise que d'attaquer un compte personnel ou si cela revient au même.

[*Traduction*]

M. Charles Docherty: Je crois que les risques seraient certainement les mêmes. Il faudrait nécessairement que les sociétés aient mis en place des contrôles, car il y a au sein d'une société un plus grand nombre de personnes qui peuvent avoir accès au système bancaire de la société.

M. Pierre Paul-Hus: Comprenez-vous ce que je veux dire ?

[*Français*]

J'aimerais savoir si, selon vous, la protection des comptes d'entreprises contre les cyberattaques est supérieure à la protection des comptes de particuliers.

[*Traduction*]

M. Charles Docherty: Non. Ce serait la même chose. Les banques prennent leurs obligations au sérieux, peu importe le type d'entité dont il est question.

[*Français*]

M. Pierre Paul-Hus: D'accord.

Des témoins nous ont dit que, dans certains pays, il était obligatoire de divulguer les cas de cyberattaque. Ici, les banques sont-elles tenues de divulguer au gouvernement du Canada les cyberattaques dont leurs systèmes font l'objet?

[*Traduction*]

Le président: Excusez-moi, Pierre. Nous avons perdu l'interprétation pendant 10 secondes environ.

Pourriez-vous répéter ce que vous avez dit ? Je vous remercie.

[*Français*]

M. Pierre Paul-Hus: D'accord, je reprends ma question.

Plusieurs témoins nous ont mentionné que, dans certains pays, les banques étaient tenues de divulguer les cyberattaques. Est-ce la même chose au Canada? Par exemple, la Banque Royale doit-elle, dans un délai prescrit, en avertir le gouvernement?

[*Traduction*]

M. Charles Docherty: Oui. Les banques, comme n'importe quelle autre organisation soumise à la LPRPDE, la loi fédérale sur la protection des renseignements personnels, sont obligées d'informer de toute atteinte à leurs mécanismes de sécurité le Commissariat à la protection de la vie privée et tous les particuliers touchés.

[*Français*]

M. Pierre Paul-Hus: Y a-t-il de la réticence de la part des banques? Si, par exemple, la Banque de Montréal subit une attaque, cela peut nuire à sa réputation. Pensez-vous qu'il y a de la réticence ou que, au contraire, cela se fait de façon automatique sans que ce soit remis en question?

[*Traduction*]

M. Charles Docherty: Les banques ne sont pas réticentes à dévoiler les attaques qu'elles subissent. C'est une obligation imposée par la loi. De plus, parce que les clients font confiance aux banques, ces dernières veulent que leurs clients soient mis au courant des rares cas de cyberattaque.

M. Andrew Ross: Puis-je ajouter que le Bureau du surintendant des institutions financières, le BSIF, exige aussi que les banques signalent tout incident?

[*Français*]

M. Pierre Paul-Hus: J'aimerais que nous parlions maintenant des particuliers, des individus.

[*Traduction*]

Le président: Nous avons un problème avec l'interprétation, et il vaudrait mieux que j'arrête la minuterie, sans quoi Pierre va se fâcher.

On me dit qu'il y a des problèmes techniques dans la cabine d'interprétation et que faute d'interprétation, nous allons être obligés de nous arrêter, malheureusement. C'est la faute de Pierre, si tout s'écroule.

Une voix: J'espère que vous n'avez pas été piratés.

Des voix: Ha, ha!

● (1610)

M. Pierre Paul-Hus: Je ne vais pas faire de plainte au sujet de la langue officielle. Je vais poser ma question dans l'autre langue également.

Le président: Pour que nous puissions continuer de cette façon, je dois avoir le consentement unanime du Comité.

Des députés: Non.

Le président: Nous allons suspendre la séance.

● (1610)

(Pause)

● (1620)

Le président: Mesdames et Messieurs, apparemment, nous avons réglé les problèmes que nous avions.

Nous avons commencé avec environ 10 ou 15 minutes de retard, et nous venons de perdre encore 5 minutes à cause de cela. Notre prochain groupe de témoins sera inévitablement retardé. Je pense que nous pourrions simplement ajouter 15 minutes pour le groupe actuel et commencer plus tard avec l'autre groupe. Est-ce acceptable? Je crois que nous devrons encore voter, alors nous n'allons nulle part de toute façon. Cela pourrait fonctionner.

Est-ce que cela vous convient, monsieur Motz?

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Je croyais que vous alliez me payer à souper entre les deux, alors cela me préoccupait un peu.

Le président: Monsieur Motz, le jour où je vais vous payer à souper, ce sera…

Des députés: Ha, ha!

M. Glen Motz: À votre retraite.

Le président: Oui.

Monsieur Paul-Hus, nous allons vous donner quatre minutes.

[*Français*]

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

Dans le mémoire de l'Association des banquiers canadiens, que vous avez déposé tantôt, vous parlez de la sécurité des infrastructures essentielles du Canada: « Le secteur bancaire compte sur d'autres secteurs qui représentent des infrastructures névralgiques, comme les télécommunications et l'énergie, pour offrir des services financiers aux Canadiens. » Cela m'amène à la question suivante, qui traite d'infrastructures essentielles à l'étranger, soit aux États-Unis, en Europe ou ailleurs dans le monde.

Collaborez-vous et discutez-vous avec des entités qui représentent le secteur financier d'autres pays pour savoir quelles sont les techniques appropriées et quelles entités étrangères commettent des cyberattaques contre leurs systèmes?

[*Traduction*]

M. Andrew Ross: Oui. Nos banques collaborent à divers groupes internationaux, dont un en particulier aux États-Unis, qui s'appelle FS-ISAC. C'est un centre de mise en commun de l'information qui a été créé aux États-Unis, mais dont la portée est mondiale. Nos banques participent à cela, tout comme nous collaborons à l'intérieur du Canada.

[*Français*]

M. Pierre Paul-Hus: Récemment, les Américains ont exprimé des inquiétudes au sujet de compagnies de télécommunications en ce qui concerne les infrastructures. Discutez-vous avec vos partenaires américains des problèmes qui pourraient être liés à l'intégration du réseau 5G au Canada?

[*Traduction*]

M. Andrew Ross: Du point de vue de la sécurité nationale, ce n'est pas une chose au sujet de laquelle nous avons beaucoup de renseignements. Il vaudrait certainement mieux poser cette question à l'industrie des télécommunications.

[*Français*]

M. Pierre Paul-Hus: D'accord, mais les banques canadiennes qui sont membres de votre association ont-elles déjà exprimé des inquiétudes à l'égard des télécommunications et des informations bancaires?

[*Traduction*]

M. Andrew Ross: Encore là, nous attendrions de tout fournisseur de services de télécommunications faisant son entrée au Canada qu'il fasse preuve de diligence raisonnable du point de vue de la sécurité nationale. De toute évidence, tout fournisseur de services Internet faisant son entrée au Canada serait tenu de faire plus que soutenir le secteur financier seulement. Nous miserions donc sur l'examen des activités de sécurité nationale et sur le secteur des télécommunications.

[*Français*]

M. Pierre Paul-Hus: En ce qui concerne la protection des avoirs, autant pour les entreprises que pour les particuliers, les banques qui sont membres de votre association disposent-elles de moyens pour compenser les pertes découlant de transactions frauduleuses, d'attaques ou d'hameçonnage? Comment cela fonctionne-t-il? Premièrement, est-ce un problème majeur? Deuxièmement, les clients de vos banques subissent-ils des pertes financières?

[*Traduction*]

M. Charles Docherty: Il n'y a pas de problème. Dans les rares cas de cyberattaques causant des pertes financières à leurs clients, les banques vont rembourser les clients.

● (1625)

[*Français*]

M. Pierre Paul-Hus: Je crois qu'un maximum de 100 000 $ est fixé pour le remboursement.

Y a-t-il un maximum quant à l'assurance ou l'obligation de la banque?

[*Traduction*]

M. Charles Docherty: Vous parlez peut-être de l'assurance-dépôts de la SADC. Ce n'est pas lié aux cybermenaces ou aux cyberattaques. En ce qui concerne la limite pour les banques, s'il y a eu une fraude et que les clients ne sont pas fautifs, mais que les mécanismes de sécurité ont été compromis, les clients seront remboursés.

M. Pierre Paul-Hus: Est-ce que ce serait le montant total?

M. Charles Docherty: Oui, monsieur: 100 %.

M. Pierre Paul-Hus: D'accord.

Je vous remercie.

[*Français*]

Le président: Monsieur Dubé, vous avez sept minutes.

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

Messieurs, merci d'être ici.

J'ai une question sur la relation entre les banques et les entreprises de cartes de crédit. Cette relation est plus compliquée que les gens ne le pensent.

Il y a cette croyance selon laquelle c'est la banque qui est responsable de plusieurs éléments d'une transaction par carte de crédit, mais, dans les faits, c'est l'entreprise de cartes de crédit qui l'est.

Le commissaire à la protection de la vie privée nous a fait part d'inquiétudes liées au fait que les serveurs des entreprises de cartes de crédit se trouvent souvent ailleurs, notamment aux États-Unis. Les protections légales auxquelles les clients ont droit en raison de leur citoyenneté n'y sont pas nécessairement les mêmes. Il y a aussi le fait qu'un acteur malveillant pourrait poser des risques additionnels, si jamais les relations entre deux pays se dégradaient. Dans cette optique, des serveurs sur lesquels nos données se trouvent, par exemple des serveurs américains, pourraient devenir une cible.

Les banques, qui font affaire avec ces entreprises, ont-elles un rôle à jouer dans cela? Le gouvernement canadien peut-il faire quelque chose pour protéger les données et les transactions des Canadiens?

Selon ce que je comprends, les entreprises de cartes de crédit sont indépendantes des banques. Néanmoins, les banques font affaire avec ces entreprises pour certains aspects importants de leurs activités.

[*Traduction*]

M. Andrew Ross: Je crois pouvoir dire que les banques et les sociétés émettrices de cartes de crédit sont interreliées. Il y a des échanges de données. Les sociétés émettrices de cartes de crédit possèdent des données relatives à la transaction, mais c'est également le cas des banques. Au bout du compte, si la carte de crédit est émise au Canada, de toute évidence, les banques sont obligées de respecter les exigences énoncées dans la loi canadienne.

[*Français*]

M. Matthew Dubé: Je veux m'assurer de bien comprendre.

Il y a les obligations qui vous sont imposées. Si vous faites affaire avec une entreprise de cartes de crédit, que ce soit Visa, Mastercard ou une autre, les données sur les transactions des clients par carte de crédit sont maintenues sur les serveurs de l'entreprise de cartes de crédit. Cela pose-t-il un problème relativement à la protection légale offerte dans le pays où les données sont entreposées? Est-ce toujours la même obligation qui s'applique? Si Visa, par exemple, a connaissance d'une fuite sur des serveurs américains, est-ce la banque canadienne qui porte la responsabilité de cette fuite?

[*Traduction*]

M. Charles Docherty: Je peux vous affirmer que les banques demeurent responsables de l'information personnelle de leurs clients. Quand elles établissent un contrat avec un tiers, par exemple, et qu'elles externalisent le traitement des données, elles ont alors la responsabilité de veiller à ce qu'il y ait en place des mécanismes de sécurité et de protection des renseignements personnels. Elles le feraient savoir à leurs clients si leurs données étaient conservées à l'étranger et soumises aux lois de ce pays.

Ce qu'il est important de ne pas oublier, c'est que quand les banques externalisent le traitement des données, cela ne signifie pas qu'elles se dégagent de leurs obligations. Les Canadiens peuvent avoir la certitude que leurs données sont protégées par le secteur bancaire.

M. Matthew Dubé: Je veux simplement m'assurer de bien comprendre votre réponse. Je m'excuse; je ne cherche pas à vous piéger de quelque façon que ce soit. J'essaie simplement de mieux comprendre ce qui se passe avec les données qui transitent un peu partout. Cela fait partie de l'objectif de notre étude.

Disons qu'une banque a conclu une entente avec une société émettrice de cartes de crédit qui se trouve aux États-Unis. Nous allons présumer que ces sociétés se trouvent en majorité aux États-Unis. Si les serveurs de la société émettrice de cartes de crédit sont là-bas, qu'il se produit quelque chose à l'étranger, avec cette société, et que des clients canadiens en subissent les effets, conformément à l'entente que vous avez avec elle, vous respecteriez les obligations imposées aux banques par la loi canadienne.

● (1630)

M. Charles Docherty: S'il s'agit d'un accord d'impartition, oui, absolument. S'il s'agit d'un tiers indépendant, les lois du pays où l'information est détenue par ce tiers pourraient s'appliquer.

M. Matthew Dubé: Quand vous le dîtes « tiers indépendant », est-ce que c'est semblable à ce que nous disons dans le contexte du système bancaire ouvert et ce genre de choses?

M. Charles Docherty: Oui, mais je tiens à vous rappeler que quand il est question des banques et de la protection des renseignements de leurs clients, si les mécanismes de sécurité de la banque ont été compromis — ce qui est très rare —, la banque se conformerait à la loi canadienne et prendrait toutes les mesures nécessaires pour indemniser entièrement ses clients.

M. Matthew Dubé: Si les mécanismes de sécurité d'une société émettrice de cartes de crédit faisant affaire avec de multiples banques sont compromis, est-ce que les banques estiment que la responsabilité relative aux clients touchés leur incombe? Est-ce que je comprends bien?

M. Andrew Ross: Oui. Les banques assumeraient la responsabilité directe de leurs relations avec les clients en pareilles circonstances.

[*Français*]

M. Matthew Dubé: C'est parfait, merci.

Il y a un autre élément que je veux aborder.

Dans votre présentation, vous avez mentionné que 72 % des Canadiens utilisent Internet ou des applications mobiles pour effectuer leurs transactions bancaires.

Un aspect qui revient souvent concerne les réseaux sans fil. On peut bien avoir le réseau le plus sécurisé au monde, mais, si les mises à jour des logiciels sur notre équipement ou notre téléphone cellulaire ne sont pas faites à temps, cela peut créer des brèches et causer des ennuis assez importants relativement aux transactions financières.

Par le passé, votre organisation a dit qu'on devrait adopter des normes pour les produits que les gens utilisent afin d'accéder à leurs données. Pourriez-vous nous en dire un peu plus? On évoque souvent le concept d'Internet des objets, une expression que j'aime bien. Cela peut avoir des conséquences sur les transactions financières.

[*Traduction*]

M. Andrew Ross: En ce qui concerne les réseaux sans fil, encore là, cela relève du secteur des télécommunications et des mécanismes que le secteur serait tenu d'adopter. L'utilisation de réseaux sans fil a des effets qui dépassent les services financiers et les transactions financières. Cela étant dit, nous parlons très clairement à nos clients de la question de la communication des renseignements. Cela nous ramène à l'éducation des clients, qui doivent savoir où faire et ne pas faire des transactions financières. Nous continuons de leur transmettre ce message. L'information du public est un aspect pour lequel nous encouragerions certainement le gouvernement à en faire plus, de sorte que les Canadiens puissent se sentir en sécurité, sans égard au type de transaction qu'ils réalisent au moyen de réseaux sans fil, qu'il s'agisse de transactions financières ou autres.

Le président: Merci, monsieur Dubé.

Madame Sahota, vous avez sept minutes.

Mme Ruby Sahota (Brampton-Nord, Lib.): J'aimerais commencer par dire aux gens de l'Association des banquiers canadiens que jusqu'à maintenant, le Comité n'a entendu que d'excellentes choses à propos de l'efficacité des banques dans le domaine de la cybersécurité. La plupart des témoins nous ont dit que les banques sont en fait des chefs de file.

J'aimerais beaucoup que vous me disiez ce que cela représente comme investissement pour les banques, et que vous me décriviez la façon dont vous travaillez avec d'autres banques à l'étranger ainsi que les partenariats que vous avez. Vous avez mentionné, dans votre exposé, que vous trouvez important que le gouvernement investisse dans le milieu universitaire. Je crois que vous parliez de la création d'un programme d'études sur la cybersécurité et de la nécessité d'investir dans ce domaine.

Est-ce que vous le faites déjà du côté du secteur privé? Dans l'affirmative, pouvez-vous nous en dire plus sur les institutions avec lesquelles vous travaillez et où vos experts de la cybersécurité obtiennent leur formation ou leur perfectionnement?

Je sais que je vous pose beaucoup de questions, mais je vous en saurais gré de répondre à chacune.

M. Charles Docherty: Je vais certainement répondre à certains éléments.

En ce qui concerne le perfectionnement, les banques investissent massivement dans des événements comme des marathons de programmation, qu'on appelle des hackathons, dont l'objectif est de faire la promotion des compétences cybernétiques au Canada.

Andrew, est-ce que vous voudriez ajouter quelque chose?

● (1635)

M. Andrew Ross: Bien sûr, les banques ont la chance d'avoir les ressources nécessaires pour contrer les risques relatifs à la cybersécurité. Comme nous l'avons dit dans notre exposé, la confiance est au cœur de tout ce que nous faisons dans le domaine bancaire. Nous devons donc investir beaucoup en matière de cybernétique. Nous faisons diverses choses dans le secteur privé. Nous avons mentionné le sommet sur la cybersécurité au Canada que l'ABC organise et qui réunit un millier d'experts de la sécurité venant de diverses banques pour une séance d'une journée. De plus, de nombreuses banques ont investi dans des partenariats avec des universités de partout au pays de même qu'à l'étranger.

Mme Ruby Sahota: Quelles sont les universités qui pavent la voie dans ce domaine?

M. Andrew Ross: Il y en a plusieurs. Waterloo en est une, avec l'informatique quantique. Il se fait aussi beaucoup de travail dans l'Ouest. Le Nouveau-Brunswick accorde beaucoup d'attention à la cybersécurité. Divers centres continuent d'apparaître. De toute évidence, les banques canadiennes veulent offrir leur soutien à cela. Nous pensons fermement qu'il y a de bons résultats à relater au Canada; les choses vont bien. Il y a cependant une pénurie à l'échelle mondiale, et il y a une pénurie chronique d'experts en cybersécurité. Il faut veiller à ce que cela soit constamment présent à l'esprit des Canadiens, et c'est la raison pour laquelle nous suggérons que ce soit intégré dans les programmes d'enseignement public, pour amener les gens à penser avant toute chose à la cybersécurité.

M. Charles Docherty: Pour ce qui est d'exemples précis d'investissements, nos membres ont financé des laboratoires de cybersécurité à l'Université de Waterloo. Des membres ont investi à l'étranger, notamment à l'Université Ben-Gurion, en Israël, un centre de cybersécurité de renommée mondiale. Un autre membre a conclu une alliance stratégique avec la Banque Leumi, d'Israël, ainsi qu'avec la Banque nationale d'Australie, afin de coopérer dans les domaines des services bancaires numériques, de la technologie financière et de la cybersécurité. Nous avons quelques exemples d'investissements dans des institutions canadiennes et étrangères.

Mme Ruby Sahota: Où vont vos membres pour embaucher des professionnels? Sont-ils capables de trouver des gens au Canada ou doivent-ils aller à l'étranger? S'ils doivent aller à l'étranger, où vont-ils précisément?

M. Charles Docherty: Ils ne sont pas limités concernant les gens qu'ils embauchent. Il y a assurément une pénurie mondiale d'experts en cybernétique. Ils doivent donc aller voir dans tous les pays pour trouver des talents en cybernétique qui soient capables d'assurer la protection des renseignements personnels de nos clients.

Mme Ruby Sahota: Est-ce qu'il y a eu des répercussions sous la forme d'amendes ou est-ce que la seule motivation est la sécurité publique et le maintien des activités commerciales?

M. Andrew Ross: Je crois que c'est parce que les Canadiens en sont venus à s'attendre à ce que le secteur bancaire soit digne de leur confiance. Je crois que c'est la stabilité financière de l'économie en général.

Nous exprimons très clairement que nous souhaitons faire profiter d'autres secteurs de nos connaissances. Nous l'avons mentionné dans nos déclarations précédentes, que les banques sont d'ardents partisans de l'Échange canadien de menaces cybernétiques. Cela permettra essentiellement aux banques, qui détectent très efficacement les cyberincidents, de faire profiter de leurs compétences d'autres organisations qui n'ont pas les mêmes capacités.

Mme Ruby Sahota: Combien de temps me reste-t-il?

Le président: Un peu moins de deux minutes.

Mme Ruby Sahota: D'accord.

Récemment, nous avons entendu parler d'une société de monnaie numérique appelée Quadriga. Je me demande si vous en avez entendu parler. Au décès du propriétaire, on a découvert que la monnaie numérique dans laquelle des gens avaient investi n'avait aucune valeur et qu'il n'y avait pas un sou. On appelait cela des « portefeuilles », apparemment, ou quelque chose de ce genre. C'est comme le Bitcoin, je pense bien.

Que pensez-vous de la réglementation à laquelle ces sociétés sont soumises, par rapport à la réglementation à laquelle l'industrie bancaire est soumise? Avez-vous des observations ce sujet?

● (1640)

M. Andrew Ross: Que je sache, le gouvernement envisage des mesures législatives visant les cryptomonnaies. Ces entités ne relèvent pas pour le moment du secteur financier. Du moins, elles ne sont pas soumises aux exigences et règlements qui visent les banques.

Mme Ruby Sahota: Je sais que le gouvernement envisage cela. Avez-vous des suggestions ou des opinions sur les façons dont ces entreprises pourraient être réglementées de sorte qu'elles puissent mieux protéger la cryptomonnaie qu'elles offrent?

M. Andrew Ross: Je ne ferai qu'un commentaire général. Alors que nous passons à un environnement numérique, les secteurs qui continuent de faire leur entrée dans cet espace doivent s'assurer d'exercer une surveillance pertinente garantissant l'adoption de dispositions relatives à la cybersécurité.

Le président: Monsieur Motz, vous avez cinq minutes.

M. Glen Motz: Merci, monsieur le président.

Je vous remercie de votre présence.

Vous avez indiqué précédemment que l'éducation est un élément important pour améliorer la cybersécurité et contrer la cyberfraude. Est-ce que vos banques soutiennent des organisations particulières qui travaillent à améliorer l'éducation ou les meilleures pratiques de vos consommateurs ou des Canadiens en général?

M. Charles Docherty: L'Association des banquiers canadiens appuie en effet des initiatives visant la littératie financière. Cette éducation vise en partie à empêcher les gens de tomber dans les pièges des fraudeurs, entre autres choses. Nous avons également de l'information sur notre site Web. Nous sommes en plein Mois de la prévention de la fraude, et nous participons à cela.

Je sais que nous contribuons dans une très grande mesure à l'Échange canadien de menaces cybernétiques et que nous communiquons de l'information au sujet des cybermenaces.

M. Andrew Ross: Nous travaillons aussi avec Sécurité publique Canada au Mois de la sensibilisation à la cybersécurité.

M. Glen Motz: D'accord.

Quand cette étude a été lancée, mon collègue Michel Picard voulait que nous portions notre attention sur… Quand nous avons parlé de cybersécurité, nous avons dit que nous voulions nous concentrer sur les incidences économiques que cela avait sur les Canadiens et sur les aspects financiers de cela, du point de vue de la cybersécurité. À ce jour, ce que nous avons entendu de la part de nombreux témoins, presque exclusivement, c'est de l'information technique au sujet de la façon dont cela se produit et au sujet des vulnérabilités de notre Internet et de notre infrastructure.

Je pense bien que du point de vue du consommateur canadien, du point de vue du public canadien, il faut que vos deux organisations aient une idée de la façon dont nous pouvons tirer le maximum de toute cette étude, si vous le voulez, ou de l'ensemble du concept de la cybersécurité, afin de réduire les risques de vol d'identité pour les consommateurs canadiens. Nous savons tous que le vol de données est le plus important élément du marché noir, du Web invisible. De toute évidence, il y a des gains financiers à faire.

Compte tenu de cela, d'après vous, qu'est-ce que le comité devrait recommander pour garantir que le public canadien est… Je sais que les Canadiens contribuent à leur propre vulnérabilité — nous comprenons cela —, mais du point de vue du gouvernement, comment pouvons-nous atténuer ce risque?

M. Andrew Ross: Pour moi, c'est une question de sensibilisation du public. Si le gouvernement est capable de diffuser le message et que le secteur financier est prêt à travailler avec le gouvernement, au bout du compte, nous faisons de notre mieux dans le secteur pour informer les consommateurs des vulnérabilités qui existent. Nous devons reconnaître qu'il y a beaucoup de vulnérabilité en dehors du secteur financier. Si les sociétés canadiennes de tous les secteurs peuvent, avec le secteur public, diffuser le message sur les risques qui existent, ce serait pour moi la première étape.

M. Glen Motz: Cela étant dit, si des entreprises d'un côté ou de l'autre, qu'il s'agisse de membres de la chambre ou d'institutions bancaires, détectent une vulnérabilité dans leurs propres systèmes, seraient-elles portées à les signaler ou tenteraient-elles de les camoufler? S'il est question de protéger les Canadiens, il y a une frontière, et nous devons nous assurer que nous sommes tous sur la même longueur d'onde afin de tenter de corriger une vulnérabilité. Selon vos observations, que font les industries et les entreprises pour corriger leurs propres vulnérabilités afin de protéger les Canadiens?

● (1645)

M. Scott Smith: Si vous n'y voyez pas d'objection, je voudrais répondre à cette question. L'Échange canadien de menaces cybernétiques, ou ECMC, a été évoqué à quelques reprises. Il s'agit d'un regroupement d'entreprises qui se sont réunies sous une seule enseigne pour échanger des renseignements sur les vulnérabilités.

Peut-être devrions-nous nous attarder au vocabulaire un instant. Il existe une différence substantielle entre une vulnérabilité et une atteinte à la sécurité. Une vulnérabilité est une porte arrière dont on ignore l'existence. Le fait qu'une menace existe sur un réseau ne signifie toutefois pas nécessairement qu'il y a une atteinte à la sécurité ou qu'une atteinte cause des torts considérables; cela veut dire qu'il existe une lacune qu'il faut corriger. L'échange de renseignements est important, et c'est une activité à laquelle s'adonne actuellement un groupe de grandes entreprises, dont des banques, des compagnies d'assurances et des entreprises de télécommunications. Elles échangent des renseignements actuellement. À l'heure actuelle, le message n'atteint pas la vaste majorité des entreprises, lesquelles n'ont aucune idée des menaces auxquelles elles sont exposées. Je pense que c'est un problème que le gouvernement pourrait contribuer à éliminer en favorisant la transmission de certaines informations aux petites entreprises.

Je sais que l'ECMC cherche des moyens de mobiliser les petites entreprises afin de faire passer l'information au milieu des affaires, au-delà des grandes banques, des compagnies de télécommunications et des grandes entreprises de transport, qui protègent toutes fort bien les Canadiens à l'heure actuelle. L'ECMC s'est d'ailleurs adressé à nous et nous cherchons des moyens de l'aider à cet égard.

Le président: Merci, monsieur Motz. Cela nous amène malheureusement à la fin de notre période de questions.

Notre prochain témoin est M. Masson, lequel avance, dans son mémoire, que les industries sont plus à risque qu'elles ne le pensent. Il indique que chez les entreprises du palmarès Fortune 500, son entreprise a détecté dans 80 % des cas une cybermenace ou une vulnérabilité dont la compagnie n'était pas consciente, qu'il s'agisse de maliciels, d'une mauvaise configuration du réseau ou d'un autre problème. Chez les petites entreprises, ce risque bondit à 95 %.

Monsieur Smith, que diriez-vous à M. Masson? Il est assis juste derrière vous.

M. Scott Smith: Je dirais qu'il a probablement raison à propos des petites entreprises. Je pense qu'une menace perdure pendant 271 jours en moyenne sur le réseau avant d'être détectée. Le problème est probablement moindre dans les grandes entreprises. Honnêtement, je ne pourrais pas avancer de chiffre. Les chiffres diffèrent selon les sondages, mais ils sont plus élevés qu'ils ne le devraient.

Le président: Sur ce, je vais malheureusement devoir mettre fin à cette partie de la séance.

Nous suspendrons brièvement la séance pendant qu'un nouveau groupe de témoins s'installe.

Merci.

● (1645)

(Pause)

● (1650)

Le président: Mesdames et messieurs, nous reprenons la séance.

Nous recevons M. Andrew Clement, qui témoigne par vidéoconférence depuis Salt Spring Island, en Colombie-Britannique.

La température est plus clémente là où vous vous trouvez, monsieur.

Nous recevons également M. David Masson.

Comme nous éprouvons aujourd'hui des problèmes techniques à divers égards, je pense qu'il serait probablement préférable d'entendre M. Clement en premier pour éviter toute difficulté technique potentielle.

M. Andrew Clement (professeur émérite, Faculty of Information, University of Toronto, à titre personnel): Je remercie le Comité de m'offrir l'occasion de contribuer à ses importantes délibérations sur la cybersécurité dans le secteur financier comme un enjeu de sécurité économique nationale.

C'est avec plaisir que je réponds à votre invitation à formuler des observations sur les infrastructures essentielles, le routage Internet, le routage de données et les technologies de l'information.

Vous avez entendu un grand nombre d'observations pertinentes au cours des séances précédentes, notamment sur le fait que les infrastructures essentielles ne concernent pas que le secteur financier, mais aussi l'économie canadienne en général; que ces infrastructures évoluent rapidement, de manières risquées qui ne sont, de façon générale, pas transparentes ou bien comprises; et que les menaces à la sécurité de ces infrastructures comportent de multiples facettes, sont complexes et se multiplient.

En ce qui concerne ces risques, j'appuie particulièrement la recommandation que M. Leuprecht a formulée précédemment, à savoir:

que le Canada mette en oeuvre une stratégie de localisation de données souveraines, renforcée par des incitatifs législatifs et fiscaux, qui obligerait les données essentielles à être conservées uniquement sur le territoire canadien, qui établirait des normes et des attentes claires pour la résilience des infrastructures de communication canadiennes, qui surveillerait cette résilience et qui imposerait des pénalités aux entreprises d'infrastructures de communication essentielles qui ne respectent pas les normes ou ne prennent pas les mesures nécessaires pour éliminer leur vulnérabilité.

J'en dirai davantage sur cette recommandation qui concerne les réseaux 5G, mais je l'appliquerai à la réduction des menaces que posent les volumes excessifs de communications de données canadiennes, notamment les données financières qui passent par l'extérieur du pays même lorsqu'elles sont envoyées vers des destinations canadiennes. Ces flux de données ajoutent une kyrielle de risques superflus à la cybersécurité, des risques qui affaiblissent la sécurité économique du Canada de manière générale.

Pour être souverain sur les plans économique et politique, un pays doit exercer un contrôle efficace sur ses infrastructures Internet, veillant à ce que les éléments essentiels restent sur son territoire, sous son autorité juridique, et soient exploités dans l'intérêt public. À l'évidence, cela concerne l'emplacement des bases de données. Le lien avec les voies que les données empruntent entre les bases de données est moins évident, mais ce facteur est tout aussi important. Or, ce domaine primordial est bien moins bien compris; j'en traiterai donc dans mon exposé.

Je m'appelle Andrew Clement, professeur émérite à la faculté de l'information de l'Université de Toronto. Ayant étudié en informatique au début des années 1960, j'ai été témoin de changements remarquables, des bons et des mauvais, dans l'infrastructure numérique qui est maintenant essentielle à notre vie quotidienne. J'ai passé une bonne partie de ma vie universitaire à tenter de comprendre les conséquences sociétales et stratégiques de l'informatisation. J'ai cofondé une entité multidisciplinaire appelée ldentity, Privacy and Security lnstitute afin de m'attaquer de façon concrète et holistique aux questions les plus épineuses soulevées par la numérisation de la vie quotidienne. À l'heure actuelle, je suis membre du comité consultatif sur la stratégie numérique qui prodigue des conseils à Waterfront Toronto sur le projet de ville intelligente qu'il élabore avec Sidewalk Labs.

Dans le cadre de mes recherches, j'ai principalement cherché à cartographier les voies d'acheminement des données sur Internet afin de révéler les endroits par lesquels passent les données et les risques qui se posent en chemin. Mon équipe de recherche a mis au point un outil appelé IXmaps, une sorte d'instrument de cartographie des échanges Internet qui permet aux internautes de voir le chemin que leurs données suivent quand ils accèdent à des sites Web.

Au début de nos recherches, nous avons détecté un cheminement appelé routage boomerang, qui figure sur la première image. Il montre le chemin que parcourent les données entre mon bureau à l'Université de Toronto et le site Web du programme d'aide aux étudiants de l'Ontario, lequel est hébergé dans le complexe du gouvernement provincial, qui se trouve à quelques minutes de marche.

Ce chemin nous a étonnés, d'autant plus que la voie que les données empruntaient pour entrer aux États-Unis et en revenir passait par le même édifice de Toronto, soit le plus grand centre d'échange Internet du Canada, sis au 151, rue Front. Voilà qui était pour le moins contraire à la présomption d'efficacité optimale du routage Internet; cela nous a incités à pousser plus loin notre étude afin de voir à quel point le phénomène était répandu et de comprendre les raisons de ce comportement contre-intuitif. Nous avons baptisé cet aller-retour entre l'étranger et le Canada « routage boomerang », un phénomène qui s'avère fort commun. Nous estimons qu'au moins 25 % du trafic de données canadien passe par les États-Unis. Selon l'Autorité canadienne pour les enregistrements Internet, ou ACEI, ce chiffre serait bien plus élevé.

Plusieurs problèmes qui touchent le routage Internet concernent le Comité.

Plus long est le chemin, plus nombreux sont les risques de menaces physiques, même s'il s'agit de quelque chose d'aussi banal qu'une pelle rétrocaveuse qui coupe un câble à fibres optiques. La distance supplémentaire fait augmenter les coûts et la latence, minant par le fait même l'efficacité et les possibilités économiques.

● (1655)

Les données qui passent par les grands centres de communication sont interceptées en lots par la National Security Agency des États-Unis, ou NSA. Avant même les révélations de M. Snowden, nous savions que c'est à New York et à Chicago que s'effectuent principalement les activités de surveillance de cet organisme. Voilà qui pose un risque non seulement pour la protection de la vie privée des Canadiens, mais aussi pour les institutions financières et d'autres organisations importantes. Lors de votre dernière séance, M. Parsons vous a parlé d'un article du *Globe and Mail* révélant que la NSA surveillait les réseaux privés de la Banque Royale du Canada et de Rogers, pour n'en nommer que deux. Selon cet article, les activités de la NSA pourraient constituer les prémisses de démarches d'investigation s'inscrivant dans un effort global visant à « exploiter » des réseaux de communication interne organisationnels.

Le routage boomerang constitue une autre menace de nature plus générale à la souveraineté nationale. Si un pays dépend d'un autre pour ses cyberinfrastructures essentielles, comme c'est le cas pour le Canada à l'égard des États-Unis, il se rend vulnérable à bien des égards, et pas seulement en raison des organismes espions ou de l'évolution des relations politiques, comme celle que l'on observe actuellement. Le meilleur allié lui-même protégera-t-il les intérêts de ses amis si ses propres infrastructures sont menacées? Si les États-Unis sont la cible d'une cyberattaque, ne seraient-ils pas tentés de couper toute connexion externe, laissant ainsi le Canada en plan? Vous avez entendu dire précédemment que certains considèrent que le Canada constitue une cible plus facile que les États-Unis et pourrait ainsi servir de voie d'accès vers nos voisins du Sud. Les États-Unis pourraient-ils en arriver à voir le Canada comme une source de menace et à couper nos liens?

Jusqu'à présent, j'ai traité du risque que pose le passage du trafic canadien par les États-Unis. Or, un argument semblable s'applique encore plus aux communications du Canada avec des pays tiers. Nos données cartographiques donnent à penser qu'environ 80 % des communications canadiennes avec d'autres pays que les États-Unis passent physiquement par les États-Unis, une situation attribuable au manque relatif de câbles optiques transocéaniques sur les côtes canadiennes, illustré clairement dans les cartes dressées par TeleGeography, un service de cartographie qui fait figure d'autorité dans le domaine. J'espère que vous pouvez voir les diapositives.

Seulement trois câbles optiques transatlantiques arrivent sur la côte Est canadienne, alors que la capacité est de loin supérieure au sud de la frontière. La plus grande partie de notre trafic à destination de l'Europe passe par les États-Unis. Fait remarquable, il n'y a aucun câble optique transpacifique sur notre côte Ouest; tout le trafic vers l'Asie passe donc par les États-Unis. La meilleure manière d'évaluer la capacité des banques à résister à une débâcle financière consiste à les soumettre à une épreuve de tolérance. Que révélerait la mise à l'épreuve des cyberinfrastructures canadiennes? Si, pour une raison quelconque, notre connexion avec les États-Unis était coupée, même si c'était pour des motifs légitimes d'autodéfense, à quel point le réseau Internet du Canada s'avérerait-il résilient? Nous devrions le savoir, mais nous l'ignorons. Les preuves disponibles laissent penser qu'il serait très peu résilient.

Que devrions-nous faire à cet égard? De façon générale, la bonne manière de réagir stratégiquement consiste, comme M. Leuprecht l'a indiqué, à adopter une stratégie de « localisation des données souveraines » incluant le routage des données. Concrètement, il faudrait coordonner un ensemble de mesures techniques, réglementaires et législatives visant à renforcer la résilience.

Nous devrions d'abord exiger que toutes les données de nature essentielle et délicate du Canada soient entreposées, acheminées et traitées au Canada. Nous devrions ensuite soutenir l'établissement et l'utilisation de points d'échange direct de données entre les réseaux en évitant le routage aux États-Unis. L'ACEI montre la voie à cet égard. Nous devrions également accroître la capacité au chapitre de la fibre optique au Canada et entre le Canada et d'autres continents. En outre, nous devrions inclure des exigences de reddition de comptes dans les normes de cybersécurité des institutions financières et des fournisseurs de services de télécommunications en ce qui concerne les pratiques de routage. Enfin, nous devrions établir un observatoire des cyberinfrastructures canadiennes qui serait chargé de surveiller le rendement et la résilience de ces dernières, de répondre aux demandes de recherche et de publier des rapports.

Je vous remercie de votre attention. Je répondrai à vos questions avec plaisir.

● (1700)

Le président: Merci, monsieur Clement.

Monsieur Masson, vous disposez de 10 minutes.

M. David Masson (directeur, Sécurité d'entreprise, Darktrace): Pour rester bref, je ne lirai pas mon exposé en entier, car je pense que vous en avez un exemplaire sur votre bureau.

Monsieur le président, distingués membres du Comité, mesdames et messieurs, bonjour. Je m'appelle David Masson et je suis directeur national du Canada chez Darktrace, une entreprise de cybersécurité.

Il s'agit du chef de file des entreprises d'intelligence artificielle dans le domaine de la cyberdéfense. Elle sert des milliers de clients dans le monde, et notre intelligence artificielle qui apprend d'elle-même peut défendre tout le parc numérique que les gens possèdent. Notre entreprise compte plus de 800 employés — en fait, il y en a maintenant 900 — et 40 bureaux à l'échelle internationale, dont 3 au Canada.

Avant de me joindre à Darktrace et d'établir l'entreprise au Canada en 2016, j'ai eu le privilège et l'honneur immenses, à titre d'immigrant au Canada, de servir mon pays au sein du ministère de la Sécurité publique pendant plusieurs années. J'ai auparavant travaillé dans le secteur du renseignement et de la sécurité nationale du Royaume-Uni, et ce, à partir de la guerre froide. À l'instar du témoin précédent, j'ai assisté à l'évolution de la cybersécurité au fil du temps, de l'époque précédant l'avènement d'Internet jusqu'à aujourd'hui, alors qu'Internet est omniprésent dans notre société.

Au cours de vos séances antérieures, je pense que vous avez énormément entendu parler de l'ampleur et de la taille de la cybermenace qui plane sur le pays; je vais donc m'attarder à trois points. Je veux d'abord vous faire part de certaines raisons pour lesquelles la cybersécurité constitue un défi apparemment insurmontable, puis je parlerai de menaces précises. Je terminerai en présentant des suggestions et des solutions aux problèmes évoqués.

Selon ce que nous observons à Darktrace, la plupart des organisations ne sont malheureusement pas aussi en sécurité qu'elles le croient. Comme vous l'avez fait remarquer plus tôt, monsieur, quand nous installons notre logiciel d'intelligence artificielle dans les réseaux d'une entreprise du palmarès Fortune 500, nous détectons dans 80 % des cas une cybermenace ou une vulnérabilité que l'entreprise ne connaissait tout simplement pas. Chez les autres entreprises, notamment celles de petite taille, le pourcentage d'entreprises compromises de quelconque manière bondit à 95 %. Il y a donc un problème presque tout le temps.

Ces statistiques font ressortir deux faits. Tout d'abord, il est évident qu'aucune organisation n'est parfaite ou à l'abri. Des organisations de toutes les tailles et de toutes les industries sont non seulement vulnérables aux cyberattaques, mais elles courent plus de risque qu'elles ne le pensent. Les attaques qui ont réussi à atteindre certaines des plus grandes entreprises du monde ces dernières années ont révélé que quelque chose ne fonctionne pas. Même les entreprises du palmarès Fortune 500, qui disposent des budgets, des ressources et de l'effectif pour contrer les cybermenaces, s'avèrent encore vulnérables.

Il y a donc lieu de se demander pourquoi un si grand nombre d'entreprises et d'organisations ignorent qu'elles sont la cible d'attaques ou qu'elles sont vulnérables. L'approche traditionnelle que les entreprises adoptaient par le passé pour assurer la cybersécurité ne fonctionne pas face aux menaces et aux environnements d'affaires de plus en plus complexes d'aujourd'hui.

Autrement dit, le problème ne vient pas que de la cybermenace, mais aussi de la complexité du domaine des affaires qui fait que les gens y perdent leur latin.

Par le passé, les entreprises cherchaient à protéger leurs réseaux contre l'extérieur, renforçant leur périmètre au moyen de pare-feux et de solutions de sécurité des points terminaux. Aujourd'hui, la migration vers le nuage et l'adoption rapide de l'Internet des objets rendent presque impossible la protection du périmètre. Une autre approche traditionnelle connue sous le nom de « règles et signatures », reposait sur le principe de la recherche de problèmes connus. Les attaquants sont toutefois en constante évolution, et cette technique ne réussit pas à détecter les attaques nouvelles et ciblées. Mais surtout, ces approches traditionnelles ne permettent pas aux entreprises de savoir ce qu'il se passe sur leurs réseaux, ce qui rend difficile, voire impossible, la détection des menaces qui s'y trouvent déjà.

Je vais maintenant traiter de deux types potentiels d'attaques qui ont des répercussions d'envergure.

Les attaques ciblant les infrastructures nationales essentielles augmentent de par le monde. Quand il est question d'infrastructures essentielles, on pense habituellement aux réseaux de distribution d'électricité et d'énergie, aux services publics, aux compagnies, aux barrages, aux transports, aux ports, aux aéroports et aux routes. Cependant, l'objet de votre étude, soit le secteur financier du Canada, notamment les grandes banques, fait également partie des infrastructures nationales du pays. Tout comme les routes assurent physiquement les liens au pays, ces organisations assurent les liens au sein de l'économie nationale. Une attaque réussie contre ces institutions de base pourrait perturber dramatiquement le rythme du commerce. La sécurité des institutions financières devrait faire l'objet d'une discussion d'une envergure et d'une gravité aussi importantes que celle portant sur la sécurité de nos réseaux électriques.

Les attaques visant à miner la confiance constituent un autre type d'attaques de plus en plus courant ces dernières années. Le gain financier n'en constitue pas l'objectif. Notre entreprise n'a pu découvrir quel pourrait être le gain financier de ces attaques. Elles visent plutôt à compromettre les données et leur intégrité. Imaginez un attaquant qui cherche à cibler une société pétrolière et gazière. Il pourrait simplement faire cesser les activités d'une installation de forage, mais il pourrait aussi recourir à une tactique plus insidieuse en ciblant les données sismiques permettant de trouver de nouveaux lieux de forage, faisant ainsi en sorte que la société creuserait au mauvais endroit.

Je veux aussi traiter brièvement de ce que nous, à Darktrace, pensons pouvoir attendre du futur des cyberattaques. Nous utilisons l'intelligence artificielle pour protéger les réseaux, mais cet outil s'immisce partout, apparemment dans toutes les industries, tombant également entre les mains d'acteurs malintentionnés. Même si le moment où des attaques perpétrées à l'aide de l'intelligence artificielle fait l'objet de débats, nous pensons qu'il pourrait s'en produire une cette année, alors que d'autres pensent que cela pourrait survenir en 2020 ou en 2025. Nous serons certainement confrontés à de telles attaques dans un proche avenir.

● (1705)

Darktrace a déjà détecté des attaques si sophistiquées qu'elles peuvent se fondre parmi les activités quotidiennes du réseau d'une entreprise et passer sous le radar de la majorité des outils de sécurité.

Jusqu'à maintenant, des attaques sophistiquées hautement ciblées ne pouvaient être perpétrées que par des États-nations ou des organisations criminelles très bien dotées en ressources. L'intelligence artificielle abaisse la barre pour ce type d'attaques, permettant à des acteurs moins qualifiés de les perpétrer. L'intelligence artificielle permet d'apprendre à propos de cet environnement cible, de reproduire les comportements normaux des machines et même de se faire passer par des personnes dignes de confiance dans ces organisations.

Les entreprises seront bientôt confrontées à des menaces sophistiquées sans précédent. Nous estimons qu'il est essentiel que les entreprises et le gouvernement — au Canada et dans le monde entier — réfléchissent aux répercussions que ces menaces auront et aux mesures qui doivent être prises pour s'assurer qu'elles peuvent se défendre contre les attaques pilotées par l'intelligence artificielle.

Puisque ce comité et l'industrie se penchent sur des réponses et des solutions, je veux formuler quelques recommandations.

En octobre 2018, $(ISC)^2$ a annoncé que la pénurie de professionnels de la cybersécurité dans le monde avait atteint les trois millions. J'ai vu ce chiffre à répétition ce matin sur LinkedIn. Près de 500 000 de ces postes vacants sont en Amérique du Nord. Au Canada, je pense que c'est 8 000, mais je présume que c'est plus. On s'attend à ce que cette pénurie augmente. Les entreprises ont du mal à embaucher des professionnels. Les gens qu'elles embauchent ont dû mal à suivre le rythme.

Les menaces évoluent très rapidement à l'heure actuelle. Pendant le temps qu'un analyste fait une pause pour aller se chercher une tasse de café, un rançongiciel peut pénétrer un réseau et chiffrer des milliers de fichiers. En plus de ces attaques rapides, les analystes sont aux prises avec une quantité monstre d'alertes concernant des supposées menaces qu'ils doivent examiner, gérer et éliminer. Nous devons trouver un moyen d'alléger le fardeau des professionnels de la cybersécurité, d'élargir le bassin de candidats éventuels en augmentant la diversité dans les processus d'embauche, ainsi que d'outiller ces professionnels en leur fournissant les technologies et les outils nécessaires pour réussir.

Je vais sauter les deux prochains paragraphes.

La collaboration entre les secteurs privé et public sera également essentielle pour résoudre les défis auxquels nous sommes confrontés. Les témoins précédents en ont parlé notamment. Les gouvernements dans le monde entier colligent une mine de renseignements sur les attaques et les techniques d'attaque de leurs adversaires. Bien que certaines restrictions sur ce que les gouvernements peuvent communiquer soient compréhensibles et nécessaires, j'exhorterais le gouvernement canadien et la communauté du renseignement à communiquer les renseignements qu'ils peuvent aux entreprises. L'information est un atout. Si les entreprises comprennent les attaques auxquelles elles sont confrontées, elles pourront mieux se défendre contre ces attaques. L'économie canadienne est mieux protégée contre les répercussions de ces cyberattaques.

Par ailleurs, il est essentiel que les entreprises privées comme la mienne fassent part au gouvernement de leurs points de vue et des leçons qu'elles ont tirées. La capacité du secteur privé de réagir rapidement et de mettre à l'essai de nouvelles technologies crée en quelque sorte un terrain d'essai pour les nouvelles technologies et techniques en matière de cybersécurité. En discutant de ce qui fonctionne ou pas, le gouvernement peut déterminer ce dont les entreprises ont besoin pour recueillir et diffuser ces renseignements — peut-être par l'entremise de l'ECMC qui, je sais, a été mentionné à plusieurs reprises — et aider des industries entières à améliorer rapidement leurs pratiques en matière de sécurité.

Je veux conclure mes remarques en faisant un appel à l'innovation. Les attaquants trouvent constamment de nouveaux moyens d'infiltrer les réseaux, de s'en prendre aux entreprises et de faire des ravages. Il est crucial que nous fassions preuve d'innovation pour nous défendre également. Que ce soit en élaborant de nouvelles technologies, en adoptant des techniques de pointe ou en promulguant de nouveaux règlements, la créativité et la collaboration seront essentielles. Au final, ce n'est pas une question de soutenir le rythme des attaquants, mais d'avoir une longueur d'avance sur eux.

J'ai hâte d'entendre vos questions.

Merci.

● (1710)

Le président: Merci à vous deux de vos exposés.

Sur ce, nous allons passer à Mme Sahota pour sept minutes, s'il vous plaît.

Mme Ruby Sahota: Merci à tous les deux de vos exposés. Ils nous ont beaucoup éclairés.

Récemment, la revue Diplomat & International Canada a publié un sondage dans lequel des sources ont dit être préoccupées par la protection de la vie privée en ligne. Leur première préoccupation était les cybercriminels et la deuxième, les entreprises Internet qui s'en prennent à leurs renseignements personnels.

Pensez-vous que les sociétés, surtout les entreprises de médias sociaux et celles qui sont vos clients, pourraient faire plus, non seulement pour veiller à ce que les données de leurs utilisateurs soient protégées mais aussi pour veiller à ce que les utilisateurs se sentent protégés? À la lumière de votre exposé, le tableau est très sombre. Avec toute la technologie que nous utilisons, tout est maintenant stocké dans le nuage. Le danger est plus élevé que jamais.

Qu'allons-nous faire? Je sais que vous avez proposé quelques solutions. Pour ce qui est de l'innovation et des investissements par le gouvernement, vous avez parlé d'échange de renseignements entre le secteur privé et le gouvernement. À votre avis, comment un gouvernement peut-il stimuler l'innovation?

Vous avez mentionné la réglementation également. Pensez-vous que l'on peut réglementer cela? Est-ce quelque chose que nous pouvons faire? Y a-t-il un pays qui s'en tire mieux que nous à l'heure actuelle? Quelles leçons pourrions-nous tirer?

M. David Masson: Vous avez posé de nombreuses questions.

En ce qui concerne les médias sociaux, puis-je demander au professeur de vous répondre en premier? Je pense que sa position sera un peu plus intéressante que la mienne.

M. Andrew Clement: Eh bien, je ne le sais pas, mais il y a eu de nombreux articles parus récemment sur le rôle que jouent les entreprises de médias sociaux, et plus particulièrement Google et Facebook, en raison de leur modèle d'affaires, qui requiert la monétisation des renseignements personnels et la communication entre personnes.

Je dirais qu'elles doivent plus particulièrement faire l'objet d'une réglementation beaucoup plus stricte et que nous devons beaucoup mieux comprendre ce qu'elles font. C'est un moment, plus particulièrement dans le cas de Facebook, où l'on peut exercer des pressions car on entend parler presque tous les jours du travail que ces entreprises font dans les coulisses pour résister à la surveillance et de la façon dont elles essaient de monétiser les données. Ce serait un point de départ, en commençant avec la plus importante de toutes.

Mme Ruby Sahota: Y a-t-il un pays qui a une longueur d'avance sur nous pour ce qui est de réglementer ces entreprises?

M. Andrew Clement: Eh bien, il y a certainement l'Europe, avec la mise en oeuvre récente du RGPD, le Règlement général sur la protection des données, dont vous avez sans doute entendu parler et qui impose des pénalités sévères. Certaines de ces entreprises ont reçu des amendes pour diverses infractions. La situation en Europe n'est pas forcément idéale, mais l'Europe réussit beaucoup mieux que le Canada et les États-Unis à gérer ce problème.

Mme Ruby Sahota: D'importantes amendes sont certainement imposées. Avez-vous des données sur l'efficacité de créer des règlements qui imposent des amendes? Y a-t-il eu une hausse du nombre d'entreprises qui sont intervenues et qui ont accru leur sécurité en ce qui concerne...

M. David Masson: Je vais vous donner un exemple rapide du fonctionnement du RGPD. Lorsque Facebook a été piraté l'an dernier, le commissaire aux données irlandais en a été informé dans un délai de 24 heures, et la disposition prévue dans le RGPD s'applique dans un délai de 72 heures. L'entreprise n'a pas tardé à intervenir. Elle a reconnu la situation très rapidement. C'est donc un instrument efficace, à mon avis.

Mme Ruby Sahota: Oui.

Vouliez-vous intervenir?

M. Andrew Clement: Oh, je dirais simplement qu'il est encore trop tôt pour tirer des conclusions en ce qui concerne le RGPD. Il n'est entré en vigueur qu'en mai de l'an dernier. Il a certainement attiré l'attention des gens. Je ne pense pas qu'on ait eu le temps d'évaluer son efficacité, mais je dirais que tout indique que c'est un bon premier pas pour régler les problèmes. Le Canada est confronté au défi de déterminer si sa loi sur la protection des renseignements personnels, la LPRPDE, est sensiblement équivalente au RGPD. Il est à espérer que la LPRPDE sera renforcée pour qu'elle soit considérée comme étant équivalente à ce règlement.

● (1715)

M. David Masson: J'assiste à de nombreuses conférences et foires commerciales et, depuis quelques années, tout le monde parle du RGPD. En tant que nouvel immigrant au Canada, j'étais un peu contrarié que personne ne semblait se soucier de la Loi sur la protection des renseignements personnels numériques et de la mise à jour de la LPRPDE que nous allions effectuer. Les gens se souciaient davantage de l'incidence du RGPD que de nos propres lois. Ils avaient probablement raison d'être inquiets, car le RGPD est plus radical que notre réglementation, à mon avis.

En vertu de notre règlement, nous ne sommes pas tenus de signaler les atteintes dans un délai précis; il faut que ce soit fait le plus tôt possible. On a discuté d'amendes allant jusqu'à 100 000 $, mais je n'ai pas vu dans les faits que des montants à payer ont été fixés. Au final, ce sont des atteintes à la vie privée; ce ne sont pas des violations en général. Je pense que le RGPD couvre les deux.

Mme Ruby Sahota: D'accord, merci.

Me reste-t-il une minute?

Le président: Il vous reste un peu plus d'une minute.

Mme Ruby Sahota: D'accord, parfait.

Pour bon nombre de ces travaux, c'est une question d'argent et d'investissements que le gouvernement doit injecter au bon endroit. Nous avons certainement prévu des fonds pour la cybersécurité dans notre dernier budget, à savoir plus de 500 millions de dollars, si bien que c'est un pas dans la bonne direction.

Où voudriez-vous que nous investissions les fonds et, s'il faut plus d'argent, où devrions-nous l'investir?

M. David Masson: Je pense que l'une des meilleures mesures était de créer le Centre canadien pour la cybersécurité en tant que guichet unique, car avant cela, on ne savait pas trop à qui s'adresser. Si on se fait pirater, à qui doit-on s'adresser? Personne ne le sait vraiment. Ce n'est pas une situation idéale.

Les parties intéressées veulent probablement investir plus d'argent pour examiner l'adoption de règlements additionnels. L'histoire nous révèle que d'importants groupes ne font rien jusqu'à ce qu'ils soient contraints d'agir, mais je vous ai signalé que Facebook a certainement fait appel au RGPD lorsqu'il s'est fait pirater, si bien que vous voudrez probablement vous pencher là-dessus. De plus, vous voudrez peut-être examiner la possibilité d'adopter d'autres lois pour mettre fin à l'influence de pays étrangers dans les élections, notamment aux fausses nouvelles et à l'ingérence étrangère. C'est une réalité. Vous voudrez probablement en faire un peu plus à cet égard.

Le président: Nous devons malheureusement vous interrompre. Votre temps de parole est écoulé, madame Sahota.

[*Français*]

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

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

La question de ma collègue correspond à la façon dont je voulais aborder la question.

Vous avez mentionné que les Canadiens disent toujours « s'il vous plaît ». Je pense que nous, les Canadiens, sommes très naïfs lorsqu'il est question de cybersécurité. Nous croyons toujours que c'est le problème des autres ou nous n'osons pas agir.

Monsieur Masson, quand vous observez le comportement général du Canada à l'égard du problème de cybersécurité, sans compter l'intelligence artificielle et les problèmes à venir, constatez-vous qu'il accuse un retard important au chapitre de sa protection?

Notre étude actuelle porte sur les banques et le système financier. Sur une échelle de 1 à 10, quel est le degré de vulnérabilité de notre système bancaire?

[*Traduction*]

M. David Masson: Je vais intervenir en premier, monsieur, mais je serai très bref.

Nous déployons beaucoup d'efforts au Canada pour établir ce que nous ferons après coup. Nous attendons qu'une attaque soit perpétrée pour gérer la situation. Nous menons de nombreux efforts pour gérer les attaques après coup. J'aimerais que le Canada consacre plus d'efforts ou fasse de son mieux pour prévenir les piratages. Nous pourrions déployer plus d'efforts en ce sens.

Pour ce qui est du système bancaire, en dehors du gouvernement, il y a de nombreux renseignements sur la portée des menaces auxquelles nous sommes confrontés au pays. Au gouvernement, où je travaillais, les menaces sont nombreuses. Je ne sais pas si vous avez entendu parler des millions de piratages qui surviennent au gouvernement, mais en dehors du gouvernement, nous ne savons pas trop ce qu'il en est. Avec la LPD qui est entrée en vigueur la semaine dernière et les dispositions pour signaler au Commissariat à la protection de la vie privée les atteintes à la vie privée par l'entremise de cyberactivités, nous avons probablement une occasion de mieux évaluer la portée des menaces en dehors du gouvernement. Je ne suis pas tout à fait certain que le Commissariat à la protection de la vie privée soit le forum approprié pour faire des évaluations, mais il recueillera des renseignements.

Sur une échelle de 1 à 10, je doute que les banques, qui communiquent peu de renseignements — bien qu'elles doivent sans doute faire preuve d'une grande ouverture avec la Banque du Canada —, produiront une évaluation, pour être honnête avec vous. Je dirais qu'elles sont probablement meilleures que la majorité des démocraties occidentales libérales. En fait, le Canada est connu pour avoir d'assez bons règlements pour son système financier, et c'est la raison pour laquelle il a souffert comme tout le monde en 2008. Les banques ont été secouées, mais elles s'en sont raisonnablement bien sorties. Je leur donnerais donc la note de sept ou huit. Voilà.

● (1720)

[*Français*]

M. Pierre Paul-Hus: J'aimerais revenir sur la question de l'attitude. Comme vous l'avez confirmé, il est important aujourd'hui de comprendre l'attitude canadienne à l'égard du problème. Croyez-vous qu'il est important de faire passer le message selon lequel nous devons avoir une position robuste?

Vous avez travaillé dans un autre gouvernement auparavant et vous travaillez maintenant dans le secteur privé. Je sais que les gens ayant travaillé au gouvernement et qui sont maintenant dans le secteur privé ont une vision très différente des problèmes. Des gens qui sont venus nous rencontrer, par exemple d'HackerOne ou d'autres entreprises, ont une vision claire du problème.

D'un point de vue gouvernemental, il y a toujours des difficultés et on parle seulement d'investissement. Oui, l'investissement est important, mais l'attitude que nous devons adopter relativement au problème doit-elle être très différente, et ce, dès maintenant?

[*Traduction*]

M. David Masson: Oui; je dirai oui. Vous avez besoin de la technique du bâton et de la carotte, mais il vous faudra probablement un plus gros bâton. La LPD prévoit que vous devez signaler les atteintes le plus tôt possible. Vraiment? Pourquoi ne pas prévoir un délai de 72 heures comme tout le monde? Oui, vous pourriez certainement allonger le bâton.

Pour ce qui est des investissements, en réponse à ce que Mme Sahota a dit plus tôt, j'investirais dans ces volets du secteur privé canadien, mais probablement davantage dans le milieu universitaire, qui effectue des travaux novateurs à l'heure actuelle pour lutter contre ce problème et qui permet au secteur privé, comme je l'ai déjà dit, de se retourner très rapidement et de tirer des leçons de leurs échecs. C'est ce que nous faisons constamment. Cela ne nous dérange pas; l'échec devient une réussite. Investissez dans ces entreprises qui sont disposées à faire cela pour essayer d'atteindre notre objectif le plus rapidement possible.

Le professeur a sans doute des observations à faire à ce sujet.

M. Pierre Paul-Hus: J'ai une autre question pour lui, si vous me le permettez.

[*Français*]

Monsieur Clement, vous avez écrit un article intitulé « Addressing mass state surveillance through transparency and network sovereignty, within a framework of international human rights law — a Canadian perspective », dans une édition spéciale du *Chinese Journal of Journalism and Communication Studies*. Je voudrais savoir comment votre article a été reçu en Chine.

[*Traduction*]

M. Andrew Clement: C'est une question intéressante. Je ne peux pas vraiment me prononcer à ce sujet. J'ai été invité à une séance sur la gouvernance d'Internet à Beijing, et j'écris à propos de la souveraineté des réseaux depuis un certain temps, mais lors de mon séjour en Chine, je sais que le président Xi Jinping a utilisé l'expression « souveraineté des réseaux » dans une perspective très différente à propos de l'infrastructure Internet chinoise.

J'ai pris la peine de préciser que la souveraineté doit être comprise dans un cadre international des droits de la personne, et c'est ce que j'ai fait. Mon exposé a été très bien reçu par certaines personnes de l'auditoire. J'ai reçu des compliments, et les éditeurs étaient impatients de publier mon article dans la revue, mais c'était en chinois et, malheureusement, je n'ai pas eu d'autres nouvelles d'eux.

Je ne sais pas si c'était le mutisme absolu ou si les gens l'ont apprécié discrètement, et c'est ce que j'espère. Merci d'avoir trouvé cet article.

● (1725)

Le président: Merci, monsieur Paul-Hus.

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

M. Matthew Dubé: Merci à vous deux d'être ici.

Monsieur Masson, pour revenir à l'apprentissage automatique et à l'intelligence artificielle... Dans cette étude, nous avons examiné les répercussions des acteurs non étatiques — des gens qui essaient de voler de l'argent et ce genre de choses. C'est une idée très abstraite, mais je me demande quel est votre avis sur l'utilisation de l'intelligence artificielle par des acteurs non étatiques. Autrement dit, nous avons clairement défini les limites relativement au recours à la force et, par exemple, les limites dans le cadre d'un conflit entre pays, ce qu'est un crime de guerre, etc. Sauf erreur, je ne pense pas que la distinction soit très claire pour ce qui est des attaques à l'égard des infrastructures essentielles, plus particulièrement si nous utilisons ce type de machine.

Je me demande simplement — et cette question est ouverte — comment, d'après vous, les acteurs étatiques déploient ces attaques et quelles sont les préoccupations pour le secteur financier ou d'autres secteurs qui pourraient être touchés, où ces règles d'engagement n'existent pas encore forcément.

M. David Masson: J'ai déjà été diplomate britannique. Je me rappelle qu'il y a 12 ou 14 ans, on m'a expliqué qu'une cyberattaque perpétrée par un État-nation ou un autre État était un acte de guerre. Toutefois, depuis ce temps, il semble que la zone soit devenue bien grise. L'autre semaine, j'ai participé à une conférence durant laquelle le sujet a été amené, et personne ne pouvait dire à quel moment on en est là. C'est peut-être parce que bien souvent, et pour des raisons évidentes, il est plus facile, en particulier pour les démocraties occidentales, de simplement ne pas tenir compte de cette question.

Les acteurs étatiques investissent massivement dans l'intelligence artificielle parce que tout le monde le fait. Les témoins qui ont comparu devant vous précédemment investissent beaucoup dans l'intelligence artificielle pour leurs systèmes bancaires. Cela n'a rien à voir avec la cybersécurité ou les cyberattaques. Ils utilisent l'intelligence artificielle simplement parce qu'elle permet de faire tellement plus de choses, tellement plus rapidement et tellement mieux.

Nous utilisons l'intelligence artificielle parce que nous disons que les êtres humains ne peuvent pas suivre l'ampleur de cette menace, de sorte que nous utilisons l'intelligence artificielle pour accomplir le gros du travail. Dire que l'intelligence artificielle remplacera les gens relève en quelque sorte du mythe. Ce n'est pas le cas. Il n'y a pas de [*Inaudible*]. Cela n'existe pas.

Ce qu'on voit en ce moment, c'est que l'intelligence artificielle est utilisée à des fins précises pour des outils précis dans des domaines précis. Nous nous en servons pour la cybersécurité, mais les méchants — et je suis heureux de dire « les méchants » parce que nous sommes coincés avec l'Internet des objets — l'utiliseront parce qu'elle leur facilitera les choses. Dans ma déclaration, j'ai signalé à quel point certaines des attaques qui ont été perpétrées par un État-nation, comme l'attaque contre Sony — beaucoup de ressources y ont été consacrées —, ou certaines des attaques en Ukraine, ont nécessité des gens, du temps, de l'argent et des efforts. Cependant, en utilisant l'intelligence artificielle, on a moins besoin d'argent, de temps et d'efforts, et, comme je l'ai dit, l'intelligence artificielle abaissera la barre pour ce type d'attaques.

Lorsqu'on pense à la première attaque perpétrée à l'aide de l'intelligence artificielle — notre entreprise croit qu'elle pourrait se produire cette année; nous voyons des signes de cela depuis longtemps, mais elle pourrait se produire plus tard —, bon nombre des techniques et des systèmes qui sont utilisés actuellement pour protéger les réseaux des cybermenaces deviendront désuets du jour au lendemain. Cela arrivera très rapidement.

Certains acteurs qui menacent l'État et d'autres utilisent l'intelligence artificielle sur le terrain de l'influence étrangère, dans les campagnes de désinformation. Il y a beaucoup d'éléments à cet égard. Vous avez peut-être remarqué que certaines des plateformes de média ont été vivement critiquées après l'horrible attentat survenu en Nouvelle-Zélande parce qu'elles n'ont pas réagi assez rapidement. Mais maintenant, si on utilise l'intelligence artificielle — nous pouvons le faire maintenant —, on peut inventer un mensonge à grande échelle et très rapidement. La mesure dans laquelle ce qui est communiqué est manifestement faux importe peu. Si l'on fait cela, ce type de volume engendre une qualité et les gens y croiront. Voilà pourquoi les acteurs malintentionnés commenceront à investir dans l'intelligence artificielle.

M. Matthew Dubé: Donc, voici la question que je me pose: si l'on regarde le projet de loi C-59, par exemple, qui donnera au Centre de la sécurité des télécommunications des capacités défensives et offensives — et il s'agit en partie d'arrêter préventivement des maliciels qui... ou un PI, ou ce genre de choses —, y a-t-il des craintes d'escalade et des préoccupations quant à la ligne tracée?

En partie, cette étude... Le problème, c'est que nous sommes tous des profanes, ou du moins la plupart d'entre nous — je ne parlerai pas au nom de tous —, en ce qui concerne ces choses. Ce que je crois comprendre de l'intelligence artificielle — parce que c'est ce que j'ai entendu aussi —, c'est qu'elle ne correspond pas à ce que nous imaginons par la culture populaire. Cela veut-il dire que si, parce qu'on utilise l'intelligence artificielle pour certaines de ces capacités que la loi confère à différents organismes, l'intelligence artificielle...? Dans quelle mesure l'humain intervient-il dans les ajustements? Si cette ligne est si floue quant à ce que sont les règles d'engagement, faut-il craindre que l'intelligence artificielle apprenne comment arrêter quelque chose, que les conséquences puissent être plus graves qu'elles ne l'étaient au départ, mais que le système évolue par lui-même en quelque sorte? Je ne veux pas m'y perdre. J'ignore quel est le jargon à utiliser ici, mais...

● (1730)

M. David Masson: Il arrive déjà que certaines attaques perpétrées par de grands acteurs aient une seule cible, mais qu'on n'ait pas tenu compte des dommages collatéraux. Il y a quelques années, l'attaque NotPetya a été lancée. Elle ciblait l'Ukraine, mais elle s'est répandue dans le monde entier et a causé des dégâts partout.

Pour ce qui est de la façon dont les gens utilisent l'intelligence artificielle maintenant — lorsque je parle d'intelligence artificielle faible, je parle d'outils précis pour des occasions précises —, si l'on craint qu'une attaque perpétrée à l'aide de l'intelligence artificielle soit lancée et qu'elle se dote d'un esprit et agisse de manière autonome, ce n'est pas le cas. C'est le type d'intelligence artificielle qui comprendra toujours un pilote. Il y a encore des êtres humains aux commandes qui décident de laisser faire les choses. Il y aura toujours des dommages collatéraux, surtout si ce sont des acteurs étatiques non réglementés qui...

M. Matthew Dubé: Si vous me le permettez, puisque mon temps s'écoule...

Je m'intéressais moins à la perte de contrôle des humains et à son portrait qu'à ce qui se passerait s'ils apprenaient les meilleures voies pour être à l'offensive, par exemple.

M. David Masson: Toute offensive d'un pays comme le Canada aura été mûrement et sérieusement réfléchie. Ce n'est pas seulement une question de pouvoir évaluer les répercussions; c'est ce qu'ils feront auparavant.

M. Matthew Dubé: Concernant les voies qu'on ferme peut-être non intentionnellement, ce n'est pas au hasard.

M. David Masson: Il faut être absolument précis dans la démarche.

Le président: Malheureusement, il vous reste environ 20 secondes. Vous pourrez les utiliser au dernier tour. Merci.

Monsieur Graham, bienvenue au Comité. Gardez à l'esprit que les interprètes essayent de traduire vos propos, peu importe la langue que vous utilisez.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): S'ils chiffrent ce que je dis en temps réel, nous serons prêts.

Puisque j'ai beaucoup de questions, je vais vous demander de répondre aussi vite que je les pose, si possible. Elles s'adressent à vous deux, et non pas à l'un d'entre vous en particulier.

Tout d'abord, quelle est la durée de vie d'un serveur non corrigé sur Internet? Si quelqu'un met en place un serveur sur Internet et n'y touche plus, pendant combien de temps reste-t-il en ligne?

M. David Masson: C'est une question de minutes.

M. David de Burgh Graham: C'est un point important.

M. David Masson: Lorsqu'on parle d'un correctif, on devrait apporter le correctif dès qu'on le dit.

M. David de Burgh Graham: À titre d'information, que signifie jour zéro?

M. David Masson: Il s'agit d'une attaque qui n'a jamais été vue auparavant. Elle est totalement nouvelle.

M. David de Burgh Graham: Vous avez parlé un peu plus tôt d'une pénurie d'environ un demi-million d'employés et de professionnels dans le domaine de la cybersécurité. Je m'intéresse à la communauté du logiciel libre depuis environ 20 ans et les gens qui m'entourent sont essentiellement les mêmes qui m'entouraient il y a 20 ans. Comment pouvons-nous attirer des gens dans l'industrie du logiciel et de la cybersécurité? Comment faire en sorte que la prochaine génération s'y intéresse et veut en apprendre à ce sujet?

M. David Masson: Je recommanderais fortement de mener des efforts semblables à ceux que mène le Nouveau-Brunswick, où l'on donne des cours sur la cybersécurité dans les écoles depuis quelques années maintenant, au point où de grandes entreprises s'arrachent maintenant les jeunes de 18 ans lorsqu'ils obtiennent leur diplôme.

M. David de Burgh Graham: D'accord. Intégrons-nous en général la sécurité dès la conception, ou notre société gère-t-elle plutôt les choses de façon réactive?

M. David Masson: À l'heure actuelle, elle est en mode réactif. J'aime beaucoup cela lorsque Mme Ann Cavoukian parle de la protection de la vie privée dès la conception — et l'on devrait parler de « sécurité dès la conception ».

Une nouvelle expression est apparue, Sec et DevSecOps et DevOps — c'est-à-dire qu'en écrivant le code, on devrait tenir compte de la sécurité; absolument.

M. David de Burgh Graham: Monsieur Clement, si vous voulez intervenir, allez-y, car je passe rapidement d'une question à l'autre. Ne vous gênez pas.

M. Andrew Clement: D'accord.

M. David de Burgh Graham: À votre connaissance, y a-t-il des avantages sur le plan de la sécurité d'opter pour un code source ouvert plutôt qu'un code source fermé? Est-il sécuritaire d'avoir un système à code source fermé, qui ne permet pas l'accès public au code?

M. David Masson: Monsieur Clement?

M. Andrew Clement: Être capable de garder un code ouvert de sorte qu'il peut être vérifié est un important moyen d'assurer la fiabilité et la sécurité.

M. David de Burgh Graham: Nous avons beaucoup entendu parler des inquiétudes liées à la sécurité des appareils Huawei et on a beaucoup parlé de la question de savoir si nous devrions bannir Huawei au Canada. Le problème concernant Huawei, c'est que son matériel peut contenir des portes dérobées chinoises, et non des portes dérobées acceptées par les organismes du Groupe des cinq, par exemple. Quelle est la source du problème et existe-t-il un système qui ne peut être compromis?

M. David Masson: Monsieur Clement?

M. Andrew Clement: Je ne crois pas qu'il existe des systèmes qui ne peuvent pas être compromis, et je signalerais qu'à certains égards, Huawei est le reflet de ce qui est arrivé concernant l'affaiblissement de la sécurité dans les technologies en Occident.

● (1735)

M. David de Burgh Graham: Au fil des ans, il a beaucoup été question des logiciels et de l'installation de portes dérobées. Une fois qu'une porte dérobée est en place, y a-t-il moyen de s'assurer que seule l'organisation qui a demandé à ce qu'elle soit installée puisse l'utiliser, ou une fois qu'elle a été introduite, n'importe qui peut l'utiliser?

M. Andrew Clement: Je ne dirais pas que n'importe qui peut l'utiliser, mais une fois qu'une porte dérobée existe, il est possible que des gens qu'on ne connaît pas y accèdent.

M. David de Burgh Graham: D'accord. Savons-nous quelle proportion de notre infrastructure Internet est compromise à l'étape de la fabrication? Il y a deux ou trois mois, on a raconté avoir découvert qu'une puce supplémentaire avait été introduite dans une carte mère à l'étape de la fabrication. Je ne me souviens plus de qui il s'agissait, mais vous êtes probablement tombés là-dessus.

M. Andrew Clement: Je n'ai aucune donnée. Je crois qu'il serait extrêmement difficile d'en trouver, et nous découvrons des choses qui ont été dissimulées il y a bien longtemps. C'est très difficile. Nous avons besoin de beaucoup plus de transparence et il nous faut pouvoir interroger les codes et les appareils.

M. David Masson: Et la chaîne d'approvisionnement.

M. David de Burgh Graham: C'est logique.

Monsieur Clement, dans votre déclaration préliminaire, vous avez parlé de notre capacité de communiquer les données à l'intérieur du pays. Avons-nous présentement la capacité de réseau qu'il faut pour que toutes nos données cheminent sur le territoire canadien, ou est-ce que l'amélioration de l'infrastructure Internet est une question de sécurité nationale?

M. Andrew Clement: Je n'ai pas d'évaluation de la capacité actuelle par rapport à nos besoins, mais j'imagine que nous avons une capacité inutilisée qui est disponible et qu'il nous faudrait pour évaluer nos besoins au pays et ensuite décider d'investir dans les capacités. L'investissement sera très modeste par rapport au type d'investissements que nous avons effectué auparavant dans d'autres infrastructures de réseau, à commencer par le chemin de fer.

M. David de Burgh Graham: D'accord.

Est-ce que l'un d'entre vous connaît Quintillion et son projet dans l'Arctique?

M. Andrew Clement: Non.

M. David de Burgh Graham: J'y reviendrai un autre jour.

Avez-vous des serveurs de base au Canada, parce que tout le trafic commence par une requête DNS? Avez-vous des serveurs de base à part .ca au Canada?

M. Andrew Clement: Je n'en connais pas.

M. David Masson: Je n'en connais pas.

M. David de Burgh Graham: Tout le trafic doit, à un moment donné, communiquer avec l'étranger pour au moins exprimer l'intention initiale quant à savoir qui veut communiquer avec qui. Cette métadonnée est accessible à quiconque a le service, et il s'agit surtout des États-Unis.

M. Andrew Clement: Oui.

M. David Masson: Si le serveur n'est pas ici, quelqu'un d'autre y a accès. N'oubliez pas que lorsqu'on parle du nuage, il ne s'agit pas d'un nuage, mais plutôt d'un serveur quelque part.

M. David de Burgh Graham: Oh, c'est vrai. Il ne s'agit pas d'un nuage; il s'agit de l'ordinateur de quelqu'un d'autre.

Sommes-nous sûrs que des attaques perpétrées à l'aide de l'intelligence artificielle ne sont pas déjà en cours?

M. David Masson: Nous pensions avoir vu un algorithme affronter un autre algorithme en 2015, et nous avons vu des signes de cela depuis, mais nous n'avons pas encore vu une vraie attaque menée à l'aide de l'intelligence artificielle. Lorsque je dis « nous », je parle de l'entreprise. Je ne peux parler pour personne d'autre.

M. David de Burgh Graham: De toute évidence, cela s'en vient. Nul doute que les attaques perpétrées à l'aide de l'intelligence artificielle sont en développement.

Dans le cadre de notre étude, nous avons beaucoup parlé de la vie privée, mais beaucoup moins, à mon avis, de la sécurité. Dites-moi, pour ce qui est des causes profondes de la cybervulnérabilité — et je sais qu'il ne me reste plus beaucoup de temps —, quel rôle jouent les mots de passe par défaut et les portes dérobées par défaut? J'ai parlé des portes dérobées un peu plus tôt. Dans énormément de cas, le nom d'utilisateur et le mot de passe du matériel sont tous les deux « admin », et on peut en faire ce qu'on veut. Dans quelle mesure cet aspect constitue-t-il un problème?

M. David Masson: C'est un problème majeur. C'est l'une des choses dont je parle sans cesse. Si vous achetez un appareil de l'Internet des objets, pour l'amour du ciel, changez le mot de passe par défaut dès que vous arrivez à la maison, s'il est possible de le faire.

M. David de Burgh Graham: Ai-je le temps de poser une autre question?

Le président: Non.

David, en sept minutes, vous avez posé un nombre de questions équivalant à environ trois réunions de comité.

M. David de Burgh Graham: J'aime presser les témoins de questions.

Le président: En effet; c'était très condensé. David vous pressait de questions.

Monsieur Motz, vous serez certainement moins insistant, j'espère.

M. Glen Motz: Monsieur Clement, vous avez voulu intervenir à plusieurs reprises, mais n'en avez pas eu l'occasion. Je veux vous donner l'occasion d'interrompre David et de livrer votre pensée.

M. Andrew Clement: J'ai possiblement manifesté mon intérêt parce que j'étais d'accord avec certains propos de M. Masson. Ce que je tenais à dire, c'est que c'est une question d'investissement. Je suppose que la question est de savoir si le gouvernement canadien était assez bien préparé pour faire face à ces cybermenaces.

À mon avis, le problème auquel nous sommes confrontés actuellement résulte en grande partie du fait que l'Internet et les services qui y sont offerts ont presque été entièrement développés en fonction des intérêts commerciaux des entrepreneurs. Ils font des choses formidables, dans bien des cas, manifestement, mais les gouvernements ont explicitement adopté une approche passive, et je pense que nous en payons maintenant le prix, notamment parce que les institutions publiques ont perdu de vue la forme que pourrait avoir une infrastructure orientée par le secteur public. Il s'agit à mon avis d'un problème structurel profond qui nécessite beaucoup d'information et de discussions. Je pense que cela aurait été une assez bonne protection.

Procédez plus lentement, mais de façon plus prudente et plus transparente afin d'accroître la reddition de comptes. Les améliorations urgentes et successives ont très souvent pour effet d'empirer les choses, car on se trouve à corriger des problèmes qui auraient mérité une meilleure réflexion.

● (1740)

M. Glen Motz: Cela m'amène à un commentaire auquel vous avez tous les deux fait allusion il y a quelques minutes par rapport à la chaîne d'approvisionnement. Que pouvons-nous faire à cet égard? Quelle est la meilleure façon d'assurer la sécurité de la chaîne d'approvisionnement dont nous parlons? Quelle est la meilleure façon d'y parvenir? Est-ce par l'intervention gouvernementale, comme vous l'avez suggéré, monsieur Clement, ou faut-il procéder autrement?

La question est pour vous deux.

M. David Masson: Je vais laisser le professeur commencer.

M. Andrew Clement: Allez-y.

M. David Masson: Très bien.

Je vous dirais d'accepter que les menaces se concrétiseront. En fait, acceptez que c'est déjà une réalité. C'est peut-être arrivé par l'intermédiaire de votre chaîne d'approvisionnement, par des fournisseurs tiers, etc. Attendez-vous à ce que cela arrive et mettez en place des systèmes pouvant les détecter, mais sans avoir une idée précise de la nature de la menace.

Il existe actuellement une multitude de règlements rigoureux. Je crois savoir que le CST publie beaucoup de règles qu'il faut respecter lorsqu'on obtient un contrat du gouvernement, mais en fin de compte, si quelqu'un réussit à introduire une puce à l'usine, comme un député l'a mentionné plus tôt, vous le découvrirez uniquement après avoir branché la puce et vu le résultat.

M. Andrew Clement: Il en existe, certes, mais je dirais que nous accusons un retard dans la conception de ces systèmes complexes. Je ferais preuve d'une grande prudence pour la conception de systèmes très intégrés, car lorsqu'un problème survient, les dommages peuvent se répandre rapidement. Il faut prévoir des zones tampons, ce qui n'est pas dans la nature des chaînes d'approvisionnement concurrentielles, où la rapidité est primordiale, mais dans une optique stratégique à plus long terme, il faut ralentir les choses quelque peu et accroître la vigilance.

M. Glen Motz: J'ai une dernière question pour vous deux.

Nous savons que les taux et l'incidence des cyberintrusions sont en hausse au pays et partout dans le monde. Le vol de données et de fonds semble presque inévitable. Je pense que les Canadiens semblent presque immunisés — même si cela arrivera de toute façon —, du moins jusqu'à ce que cela leur arrive. À ce moment-là, le problème est grave.

Je déteste être prophète de malheur, mais ne devrions-nous pas être prêts à ce que cela se produise fréquemment? Doit-on simplement se faire à l'idée qu'il est inévitable de se faire pirater ou voler lorsqu'on va sur Internet, ou y a-t-il de l'espoir?

Le président: Très brièvement, s'il vous plaît.

M. David Masson: Puis-je commencer? Je dirais qu'il y a de l'espoir si vous avez recours à l'intelligence artificielle. Vous comprenez? L'intelligence artificielle donne à celui qui se défend une longueur d'avance sur ceux qui l'attaquent.

Professeur.

M. Andrew Clement: Je dirais que nous n'acceptons pas ce genre d'approche pour d'autres aspects de nos infrastructures essentielles. Comme nous le faisons pour le développement d'autres infrastructures, ce qui est mis en place doit être examiné de façon beaucoup plus attentive et rigoureuse et doit être dans l'intérêt public. On empêche ainsi que des choses soient imposées au public et qu'on s'attende à ce qu'il s'y fasse. C'est ce qu'on voit actuellement, essentiellement.

● (1745)

Le président: Merci beaucoup, monsieur Motz.

Monsieur Picard, pour cinq minutes.

M. Michel Picard: On peut raisonnablement s'attendre à ce qu'un gouvernement qui s'interroge sur les mesures qu'il doit prendre pour accroître la cybersécurité n'ait aucun système en place. Je pense qu'il est juste de dire que mon système doit être plutôt bon, car je travaille avec divers organismes. J'ai des protections, des systèmes, des outils. Je vais simplement vous renvoyer la question. Quelles mesures devrais-je prendre pour me protéger, créer un mécanisme solide et améliorer la situation? Quelles sont les principales mesures?

Les représentants de l'Association des banquiers canadiens ont dit que la sensibilisation à la cybersécurité est la meilleure solution. À mon avis, j'aurais beaucoup de problèmes si je fondais mes mesures de cybersécurité sur la publicité. L'information et la sensibilisation ne suffisent pas. Quels sont les principaux facteurs à considérer pour m'assurer d'avoir au moins de bonnes infrastructures de base en matière de cybersécurité?

M. David Masson: Je vous laisse commencer, professeur.

M. Andrew Clement: Je pense qu'un examen par des experts indépendants est important. Ces experts de l'extérieur de l'organisme doivent pouvoir faire un véritable examen des mesures proposées et des menaces possibles, et fournir des conseils. Voilà ce qu'il en est de façon générale. Autrement, vous devrez préciser le type de système dont il est question.

M. David Masson: En ce qui concerne l'avenir, allons au-delà des acteurs malveillants qui utilisent l'intelligence artificielle, dont j'ai beaucoup parlé. Je conseillerais certainement au gouvernement d'accorder une grande attention aux attaques contre les infrastructures essentielles nationales, en particulier les attaques sur ce qu'on appelle les systèmes de technologie opérationnelle. Nous avons surtout parlé des systèmes de TI, mais je parle ici des systèmes de TO, les systèmes qui assurent le fonctionnement des robots dans les usines de voitures, par exemple. Il faut absolument accorder une grande importance à cela, en particulier pour les systèmes des infrastructures essentielles nationales.

M. Michel Picard: Une très vieille question que j'ai l'habitude de poser assez souvent — comme je l'ai fait au comité de l'éthique lorsque nous traitions d'un sujet semblable — est liée à un risque que je ne pourrai jamais contrôler: le facteur humain. Quelles solutions proposez-vous pour réduire ou tout simplement minimiser le risque lié aux ressources humaines? Je ne peux l'éliminer.

M. Andrew Clement: Eh bien, les risques ne peuvent jamais être éliminés; ils peuvent seulement être atténués et minimisés. Sur le plan des ressources humaines, il y a un principe général selon lequel il faut respecter les personnes qu'on embauche, qu'on forme et qu'on gère, et qu'elles doivent souscrire à la mission de l'organisation.

Les intérêts de l'organisation ne sont servis que si les gens font preuve de prudence et adoptent une vue d'ensemble. C'est un principe de base dans toute organisation.

M. David Masson: Oui, on dit toujours que l'humain est le maillon le plus faible, mais j'ai parfois l'impression que c'est une façon pour les grandes organisations de se soustraire à leurs responsabilités. Elles ont toujours tendance à mettre les gens en cause.

De toute évidence, il faut accroître l'information et la sensibilisation, mais aussi favoriser l'instauration d'une culture de sécurité adéquate au sein des organisations, pas seulement parmi la base. Tous doivent être empreints de cette culture de sécurité et veiller à l'appliquer de manière honnête. On ne parle pas de gens qui donnent des ordres, mais de chefs de file qui veulent promouvoir une culture de sécurité en faisant de cet enjeu une véritable priorité.

M. Michel Picard: Les représentants de la chambre de commerce ont indiqué que certaines petites entreprises se considèrent comme trop petites pour être piratées. Je pense plutôt qu'elles sont trop petites pour consacrer une part du budget à la sécurité. Ce sont des entreprises qui oeuvrent dans des domaines liés à Internet, aux services en ligne et au monde virtuel.

Sur le plan personnel, quelqu'un qui piraterait mon téléphone pourrait savoir si je suis à la maison ou non, parce que je contrôle mon système de chauffage avec mon téléphone. On pourrait voir que je ne respecte pas l'horaire habituel, parce que je maintiens une température plus basse lorsque je suis absent. Donc, mon téléphone est une vulnérabilité.

Il semble que mon réfrigérateur n'est pas sécuritaire, parce qu'il peut communiquer avec moi, comme pour tout appareil avec une puce à l'intérieur. Donc, personnellement, je dirais que la présentation que nous avons entendue était à glacer le sang. Désolé, je l'ai presque dit.

Est-il trop tard pour moi?

● (1750)

Le président: Probablement. Vos cinq minutes sont écoulées.

Nous allons laisser M. Picard dans l'anxiété.

Il nous reste environ cinq minutes et un certain nombre de questions. M. Motz a gracieusement accepté de partager son temps avec moi.

Monsieur Masson, pendant votre présentation, vous vous êtes dit très préoccupé par le maintien des données, du réseau et de la transmission au Canada. Essentiellement, vous avez adopté la recommandation de M. Clement.

Toutefois, l'Association des banquiers canadiens n'a pas semblé aussi préoccupée et a fait valoir que les données lui appartiennent toujours.

Que répondez-vous à l'Association des banquiers canadiens? La situation actuelle ne semble absolument pas lui poser problème. Cela pourrait signifier que les données passent de Toronto à Chicago puis à New York avant de revenir à Toronto pour y être conservées, ou encore qu'elles sont conservées à New York, par exemple. Que répondez-vous à cela?

M. Andrew Clement: Je crois avoir entendu cette discussion à la fin de leur partie. Ils ont dit pouvoir insister sur les modalités de leurs accords d'impartition avec des tiers indépendants, puis qu'ils seraient entièrement responsables de trouver des solutions pour les consommateurs. Je ne remets pas en question la capacité des institutions bancaires d'y parvenir dans des cas très précis, mais en cas de problème majeur, que feront-elles si leurs données sont à l'extérieur du pays? Poursuivront-elles le tiers? Elles seront dans une autre administration. Je ne pense pas que les accords d'impartition sont adéquats. Comme ils l'ont indiqué, ces accords n'ont aucune incidence sur les lois du pays où l'information est détenue. Ces lois s'appliquent et les tiers sont tenus de les respecter, même si cela signifie qu'ils enfreindront les termes de l'accord. Autrement, ils pourraient être pris dans un dilemme.

J'étais beaucoup moins rassuré par leur confiance quant à la possibilité d'externaliser simplement les données dans d'autres pays et de se fier aux contrats. Je pense que ces institutions seraient bien mieux placées si ces services relevaient de la compétence du Canada, en sol canadien. Je ne vois pas de raison importante pour laquelle elles ne pourraient atteindre cet objectif, du moins à long terme, soit avoir à la fois le beurre et l'argent du beurre, comme on dit.

Le président: La dernière question porte sur les cartes que vous nous avez gracieusement fournies. Cela m'a rappelé un voyage que j'ai fait sur une frégate canadienne l'été dernier. Nous sommes partis d'Iqaluit, avons descendu la baie Frobisher et sommes allés jusqu'au Groenland, où nous avons rencontré un général danois responsable de l'OTAN. Il y a évidemment eu des commentaires sur les intrusions russes dans les territoires de l'OTAN, etc. Il semble que les Russes ont une incroyable fascination pour les recherches scientifiques sur les câbles qui relient l'Europe et l'Amérique du Nord. Monsieur Clement, cela semble se rapporter à l'une de vos préoccupations, soit qu'une des façons de pirater facilement l'ensemble de ces réseaux serait d'attacher des dispositifs sur ces câbles d'une manière ou d'une autre.

Vous avez clairement démontré la vulnérabilité de l'ensemble de nos données.

● (1755)

M. Andrew Clement: Les câbles transocéaniques représentent en effet un point de vulnérabilité s'étendant sur des milliers de kilomètres. Je sais que les États-Unis ont la capacité de lever les câbles, de créer une épissure et d'intercepter les communications, et je ne serais pas surpris que les Russes et les Chinois l'aient aussi. Une des façons d'y remédier est de créer des redondances. Il s'agit de créer une surcapacité. Ainsi, en cas de défaillance d'un lien, les autres liens maintiennent la communication. C'est d'ailleurs le cas d'au moins un câble aboutissant en Nouvelle-Écosse, le câble Hibernia, qui est une sorte de boucle.

Je pense qu'il faut investir dans les systèmes redondants afin de minimiser le nombre de points de défaillance critiques. Ainsi, en cas d'attaque, une panne généralisée serait beaucoup moins probable, et il serait possible de rediriger le flux des données en cas de défaillance d'un système. Malheureusement, l'impératif d'efficacité et de vitesse et l'accent mis sur ces caractéristiques ont pour effet que nous avons très souvent tendance à mettre tous nos oeufs dans le même panier. Je dirais que la redondance et les dédoublements constituent une approche générale de la sécurité et que c'est là qu'il faut investir. Nous devons en être conscients et ne pas attendre une défaillance ou une panne généralisée pour le découvrir.

Le président: C'est malheureusement là-dessus que se termine notre discussion avec vous. C'était absolument fascinant. Nous vous sommes reconnaissants de votre contribution à notre étude. Bonne continuation à tous les deux.

La séance est levée.