CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

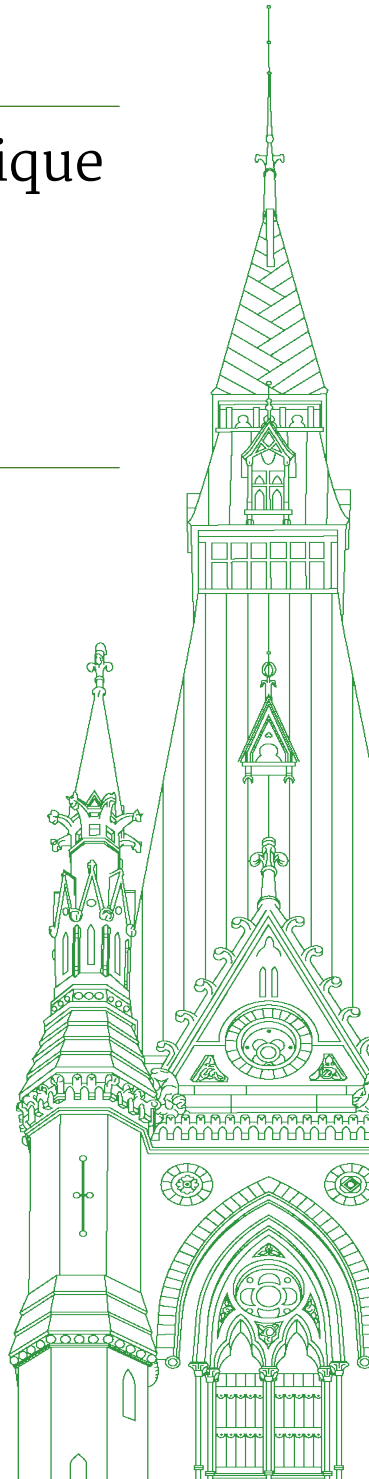
43e LÉGISLATURE, 2e SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 012

Le mercredi 9 décembre 2020



Président : L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 9 décembre 2020

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Je constate que nous avons le quorum. La séance est donc ouverte. Nous en sommes à la 12e séance du Comité permanent de la sécurité publique et nationale de la Chambre des communes.

Nous accueillons aujourd'hui M. Scott Jones, qui est dirigeant principal du Centre canadien pour la cybersécurité et qui a témoigné devant notre comité à maintes reprises, je dirais.

Avant de vous demander de faire votre déclaration préliminaire, je voudrais simplement vous féliciter pour votre rapport. Si la qualité d'un rapport tient à son accessibilité, je pense que celui que vous avez produit est en fait très accessible, surtout pour des gens comme nous qui n'ont pas une connaissance vraiment spécialisée du domaine. Je tiens donc à vous en remercier.

J'aimerais également signaler que ce rapport fait écho à celui du Comité des parlementaires sur la sécurité nationale et le renseignement, déposé par M. McGuinty, et il y avait une lettre qui, je l'espère, a été distribuée aux députés après la dernière réunion.

Sur ce, j'invite M. Jones à prendre la parole pour sept minutes et je le remercie à nouveau de sa disponibilité.

M. Scott Jones (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Merci beaucoup, monsieur le président.

Bonjour, mesdames et messieurs les membres du Comité.

Je vous remercie de m'avoir invité à témoigner devant vous aujourd'hui pour discuter de cybersécurité et, plus particulièrement, du rapport intitulé *Évaluation des cybermenaces nationales 2020*, publié le 18 novembre.

En tant que dirigeant principal du Centre canadien pour la cybersécurité, qui relève du Centre de la sécurité des télécommunications, ou CST, je suis très heureux d'être ici. Le CST est l'organisme canadien du renseignement étranger et le principal organisme technique et opérationnel pour la cybersécurité. Comme vous venez de l'entendre, j'ai témoigné devant votre comité à plusieurs reprises.

Créé en 2018, le Centre canadien pour la cybersécurité est une source unifiée de conseils d'experts, d'orientation et de soutien sur les questions opérationnelles liées à la cybersécurité. Nous travaillons en étroite collaboration avec les autres ministères du gouvernement, nos partenaires de l'industrie et le public en vue de renforcer la sécurité des Canadiens en ligne et d'assurer la résilience du Canada face aux cybermenaces.

L'objectif de l'évaluation des cybermenaces nationales n'est pas d'effrayer les Canadiens ou de les décourager, mais plutôt de les informer des menaces auxquelles ils pourraient être confrontés au cours des prochaines années. J'espère que la lecture de cette évaluation incitera plusieurs d'entre nous à prendre des mesures simples pour assurer notre protection. Comme nous avons pu le constater, la prise de mesures simples et faciles peut grandement renforcer notre sécurité personnelle.

Le Canada est l'un des pays les plus connectés au monde, et la pandémie de COVID-19 n'a fait qu'accroître cette dépendance à Internet. Notre vie se passe de plus en plus en ligne. En même temps, les auteurs de menace continuent de chercher de nouvelles façons d'utiliser Internet à des fins malveillantes. Bien que l'évaluation ne fournisse aucun conseil en matière d'atténuation, on peut trouver de l'orientation et des pratiques exemplaires sur le site Web du Centre canadien pour la cybersécurité et sur celui de la campagne de sensibilisation du public, intitulée « Pensez cybersécurité ». Comme je l'ai déjà dit, grâce à de simples mesures, tous les Canadiens peuvent aider à renforcer et à assurer la cyberrésilience du Canada.

Les Canadiens qui aimeraient en apprendre plus à ce sujet peuvent également consulter la version mise à jour de l'*Introduction à l'environnement de cybermenace*, qui explique plusieurs des termes et des techniques propres à la cybersécurité.

L'évaluation analyse les tendances inhérentes à la cybersécurité depuis 2018 et tire avantage de la perspective unique de l'environnement de cybermenace dont dispose le Centre canadien pour la cybersécurité pour prédire ces tendances jusqu'en 2022. Elle met également en lumière les cybermenaces les plus pertinentes pour les entreprises et les citoyens canadiens.

Avant de discuter plus en détail des menaces, j'aimerais souligner que les constats formulés dans l'évaluation sont basés sur des rapports tirés de plusieurs sources classifiées et non classifiées, dont ceux découlant du mandat de renseignement étranger du CST. Nous avons tenté de fournir aux lecteurs le plus d'information possible, accompagnée de notes de bas de page, même si le Centre canadien pour la cybersécurité est tenu de protéger les sources et méthodes classifiées.

Je présenterai maintenant un bref résumé des principales conclusions tirées par le Centre canadien pour la cybersécurité concernant l'environnement de cybermenace. De manière générale, il est possible de regrouper ces conclusions sous trois catégories que nous aborderons aujourd'hui.

L'*Évaluation des cybermenaces nationales 2020* fait mention de plusieurs observations clés.

Dans un premier temps, la cybercriminalité est la menace la plus susceptible de cibler les Canadiens à l'heure actuelle et au cours des années à venir, puisque les cybercriminels réussissent souvent à exploiter les habitudes sociales et les comportements humains de leurs victimes.

Dans un deuxième temps, les activités malveillantes dirigées contre le Canada continueront fort probablement à cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles.

Enfin, bien que la cybercriminalité demeure la principale menace, les cyberprogrammes parrainés par la Chine, la Russie, la Corée du Nord et l'Iran sont les plus grandes menaces stratégiques ciblant le Canada.

D'abord, nous estimons que la cybercriminalité demeure la menace la plus susceptible de viser les Canadiens. Comme c'est déjà le cas, dans les années à venir, la population et les organisations du Canada continueront de faire face à de la fraude en ligne et à des tentatives de vol de renseignements personnels, financiers et organisationnels. Les cybercriminels réussissent habituellement à atteindre leurs objectifs en exploitant des comportements humains et des pratiques sociales profondément enracinés, ainsi que les vulnérabilités des technologies. Malheureusement, c'est aussi pour ces raisons que les Canadiens sont encore plus à risque d'être victimes d'un cybercrime. Les risques sont d'autant plus grands en pleine pandémie de COVID-19.

Les auteurs de cybermenaces profitent de la peur qu'éprouvent les gens pour les berner et les encourager à visiter des sites Web frauduleux, à ouvrir les pièces jointes dans les courriels et à cliquer sur des liens qui contiennent des maliciels. Il est fréquent que ces sites Web, courriels et liens personnifient le gouvernement du Canada ou des organismes du domaine de la santé. Pour protéger les Canadiens contre ces menaces, il faut s'attaquer autant aux éléments techniques qu'aux éléments sociaux des cybermenaces.

Aussi, la sécurité des Canadiens dépend d'infrastructures essentielles, de même que de biens médicaux et de consommation, qui sont de plus en plus offerts sur le Web. Malheureusement, une fois en ligne, ces infrastructures et ces biens sont sujets à des cybermenaces, et les protéger exige des investissements que les fabricants et les propriétaires pourraient avoir de la difficulté à maintenir.

Nous estimons que les rançongiciels dirigés contre le Canada continueront de cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles. Comme ces entités ne peuvent pas se permettre de subir des perturbations importantes, elles sont prêtes à verser jusqu'à plusieurs millions de dollars pour rétablir rapidement leurs activités. Il est probable que beaucoup de victimes canadiennes continueront de consentir à payer les rançons demandées pour éviter d'éponger d'importantes pertes, des coûts de remise sur pied de leurs réseaux ou encore les conséquences auxquelles elles devront faire face si elles refusent de payer. La protection de ces entreprises et de ces réseaux est essentielle pour assurer la productivité et la compétitivité des entreprises canadiennes, et c'est d'une importance capitale pour la défense nationale du pays.

Enfin, des auteurs de cybermenace parrainés par des États cherchent vraisemblablement à développer des moyens de perturber les infrastructures essentielles du Canada pour atteindre leurs buts. Nous croyons toutefois qu'il est fort improbable que des auteurs de cybermenace tentent de perturber volontairement les infrastructures essentielles du Canada et de causer de sérieux dommages ou des pertes de vie s'il n'y a aucun climat d'hostilité à l'échelle internationale. Néanmoins, les auteurs de cybermenace pourraient cibler des organisations canadiennes dans l'objectif de recueillir des données, de se prépositionner en vue d'activités ultérieures ou de les intimider.

● (1535)

Bien que la cybercriminalité représente la menace la plus importante pour le Canadien moyen, les cyberprogrammes parrainés par la Chine, la Russie, la Corée du Nord et l'Iran posent les plus graves menaces stratégiques pour le Canada. Nous estimons que les auteurs de menace parrainés par des États continueront fort certainement de mener des activités visant à voler la propriété intellectuelle et l'information exclusive du Canada, ainsi que, dans le contexte actuel, l'information relative à la COVID-19.

Nous sommes aussi d'avis que les campagnes d'influence étrangère en ligne ne se limitent plus à des événements politiques importants, comme des élections. Elles font maintenant partie de la nouvelle réalité. Les adversaires tentent de maintenir leur influence sur divers débats publics qui revêtent, pour eux, une valeur stratégique. Bien que les Canadiens ne soient généralement pas des cibles prioritaires des activités d'influence étrangère en ligne, l'écosystème des médias du Canada est étroitement lié à celui des États-Unis et d'autres alliés. Cela signifie que lorsque les populations de ces derniers sont ciblées, les Canadiens s'exposent aussi indirectement à de l'influence en ligne.

Je tiens à vous rassurer que le CST et le Centre canadien pour la cybersécurité travaillent d'arrache-pied pour atténuer plusieurs de ces menaces et protéger les Canadiens et leurs intérêts en offrant des avis et des conseils ciblés. Le CST remplit tous les volets de son mandat et contribue ainsi à assurer la protection du Canada contre ces menaces. L'*Évaluation des cybermenaces nationales* ne vise pas uniquement à informer les Canadiens; elle a également pour objet d'établir les priorités d'action du Centre canadien pour la cybersécurité. Elle dicte les mesures que nous prenons pour nous attaquer aux menaces qui guettent chacun de nous, mesures qui sont souvent prises en collaboration avec des partenaires du secteur privé disposés à prêter main-forte.

L'initiative du Bouclier canadien de l'Autorité canadienne pour les enregistrements Internet, l'ACEI, est un bon exemple de ce type de partenariat. Le Bouclier canadien est un service DNS protégé offert gratuitement par l'ACEI qui bloque la connexion aux sites malveillants qui risquent d'infecter votre appareil et de voler vos renseignements personnels. Ce service est fourni par l'Autorité canadienne pour les enregistrements Internet, un organisme à but non lucratif qui gère le nom de domaine « .ca ». Ce service fait appel au renseignement sur les menaces recueilli par le Centre canadien pour la cybersécurité. En d'autres mots, si un utilisateur du Bouclier canadien clique sur un lien que l'on sait malveillant, l'accès au site en question sera bloqué.

L'ACEI a constaté qu'un certain nombre de Canadiens se sont déjà mis à utiliser cet outil, même si nous aurions certes voulu que la participation se fasse à un rythme plus accéléré. Nous venons de franchir le jalon de six mois. Nous recommandons à tous les Canadiens de profiter de ce service gratuit conçu par des Canadiens pour des Canadiens et visant à protéger leur vie privée.

Grâce à la publication de conseils et de consignes spécialement conçus, le Centre canadien pour la cybersécurité permet de renforcer la protection des ressources électroniques des Canadiens. Le Centre s'engage à faire avancer la cybersécurité et à accroître la confiance des Canadiens dans les systèmes qu'ils utilisent au quotidien. Nous espérons que ce rapport aidera à élever la barre en matière de sensibilisation aux cybermenaces actuelles. J'encourage les Canadiens à la recherche de conseils faciles sur la cybersécurité — notamment grâce à notre guide sur les achats des Fêtes —, à visiter notre site Web, pensezcybersecurite.ca.

Il est également possible de trouver toutes les publications du Centre canadien pour la cybersécurité, dont certaines destinées aux entreprises et aux grandes sociétés, à l'adresse cyber.gc.ca.

Je vous remercie encore une fois de m'avoir donné l'occasion de comparaître virtuellement devant le Comité aujourd'hui. Je me ferai un plaisir de répondre à vos questions.

● (1540)

Le président: Merci, monsieur Jones.

Pour la première série d'interventions de six minutes chacune, nous allons entendre Mme Stubbs, M. Lightbound, Mme Michaud et M. Harris. Ce sera dans cet ordre.

Madame Stubbs, je vous cède la parole. Vous avez six minutes.

Mme Shannon Stubbs (Lakeland, PCC): Merci, monsieur le président.

Je remercie le témoin de sa présence et de son temps, ainsi que du rapport qu'il a présenté et de tout le travail qu'il a accompli. C'est révélateur et profondément inquiétant. Je pense donc que nous sommes tous heureux que vous soyez là.

Dans vos observations et votre rapport, vous avez parlé brièvement du coût que représente le piratage informatique de l'étranger pour les entreprises et les gouvernements des pays de l'Ouest. En effet, selon les statistiques du Centre antifraude du Canada, en 2019, les Canadiens ont perdu plus de 43 millions de dollars à la suite de fraudes liées à la cybercriminalité.

Pouvez-vous nous expliquer à combien s'élèvent les coûts entraînés par les criminels et les auteurs de cybermenace parrainés par des États étrangers qui s'ingèrent dans notre démocratie et notre société? Je me demande si vous avez des observations à faire sur la relative impunité avec laquelle ils semblent agir, sans vraiment risquer d'avoir à assumer les coûts de leurs actes.

M. Scott Jones: Je vous remercie de la question, monsieur le président, et merci aussi pour les commentaires au sujet du rapport.

À mon avis, plusieurs facteurs entrent en ligne de compte. Les cybercriminels évoluent, en grande partie, dans un écosystème extrêmement développé qui repose notamment sur des transactions financières anonymes, comme Bitcoin et tout le reste. L'utilisation de devises numériques en ligne facilite vraiment les choses.

En ce qui concerne le risque, j'aurais aimé qu'un de mes collègues de la GRC soit ici pour en parler du point de vue des poursuites intentées. Quoi qu'il en soit, comme il s'agit d'un environnement difficile à gérer, il est possible de commettre des fraudes contre les Canadiens à partir de pays éloignés. Comme nous le soulignons dans le rapport, il existe de nombreux pays où les cybercriminels ne subiront pas les conséquences des autorités locales, car tant qu'ils ne viseront pas leurs concitoyens, ils ne feront l'objet d'aucune poursuite. Le principe du donnant-donnant semble donc être au rendez-vous, et ce constat a assurément été mis en évidence dans certains travaux de recherche.

Pour ce qui est des coûts, nous essayons d'en imposer quelques-uns. Le gouvernement a fait un certain nombre de déclarations pour dénoncer les activités menées par des États qui, à notre avis, dépassent les limites. Au début de l'année, nous avons dénoncé les activités menées par la Russie contre les entreprises de recherche sur les vaccins. Nous nous sommes certainement joints à nos alliés à plusieurs reprises pour le faire. Ainsi, nous avons uni nos efforts à ceux du Royaume-Uni et des États-Unis, surtout parce que nos régions étaient visées. Bref, nous n'avons pas manqué de dénoncer, parfois en collaboration avec nos alliés, le comportement de chacun des quatre pays que j'ai mentionnés.

Mme Shannon Stubbs: Pouvez-vous nous expliquer l'importance de dénoncer et d'exposer leur intention? Par ailleurs, avez-vous des observations à faire sur d'autres options de riposte, comme des sanctions ou d'autres outils?

M. Scott Jones: L'utilité de la dénonciation est assez variable. Le rôle de défenseur de la cybersécurité permet surtout de pousser les autres à agir. Lorsque nous faisons une dénonciation, les organismes ont tendance à prendre au sérieux les alertes que nous lançons. Lorsque nous disons qu'il est important d'appliquer tel ou tel correctif, les gens répondent à l'appel. Lorsque nous leur conseillons d'installer un correctif parce qu'un pays X cible un secteur donné, les gens font attention et ils prennent des mesures en conséquence. Cela finit par avoir un effet à l'échelle nationale, car les victimes éventuelles sont amenées à prendre la situation au sérieux et à agir.

Sur la scène internationale, nous n'avons certainement pas constaté de changement important dans le comportement des auteurs de cybermenace, mais ces efforts permettent de créer des normes. C'est peut-être un sujet qui relève davantage de mes collègues des Affaires mondiales, et ils sont probablement mieux placés pour aborder des questions comme les sanctions et d'autres aspects liés à la politique étrangère. J'essaie, pour ma part, de m'en tenir aux éléments techniques et aux questions de cybersécurité.

Mme Shannon Stubbs: D'accord. Je vous remercie.

À la page 23 de votre rapport et dans les observations que vous avez formulées — et vous avez déjà donné l'exemple du Bouclier canadien —, vous avez fait remarquer que les rançongiciels ciblent souvent les organisations de santé et que les attaques se sont multipliées pendant la pandémie de COVID-19. En page 25, vous avez parlé de la vulnérabilité de la chaîne d'approvisionnement. Je me demande si vous pouvez parler de la campagne de vaccination massive contre la COVID-19 que le gouvernement fédéral est en train d'organiser et des mesures qui sont prises, qui pourraient être prises ou qui seront prises pour assurer la protection de la chaîne d'approvisionnement contre les cyberacteurs malintentionnés. De plus, considérez-vous que les fournisseurs, les responsables de la logistique et les cliniques médicales ont instauré des mesures de cybersécurité suffisamment solides?

● (1545)

M. Scott Jones: Je vous remercie de vos questions. Il y a beaucoup de matière à couvrir.

Depuis le début, nous nous employons à renforcer la résilience du secteur des soins de santé. Nous nous sommes notamment associés aux provinces et aux territoires — qui ont manifestement un rôle très important à jouer à cet égard en fournissant des conseils et de l'orientation — afin d'offrir des séances d'information ciblées, destinées particulièrement au secteur des soins de santé afin d'en renforcer la résilience au fil du temps. Sachant qu'un vaccin serait mis en marché à un moment donné, nous avons renforcé la résilience et nous nous sommes assurés que l'information circule bien pour être certains que les acteurs disposent des renseignements dont ils ont besoin pour prendre des mesures proactives afin de se protéger. À cette fin, nous avons publié d'autres évaluations de la menace s'adressant expressément au secteur de la santé. Avec ces documents, nous effectuons des appels hebdomadaires réguliers pour passer en revue les menaces que nous décelons et cherchons à voir comment elles pourraient cibler le secteur de la santé afin de déterminer ce que nous pourrions faire à ce sujet. Nous tentons de renforcer la résilience avant que quelque chose n'arrive.

Pour ce qui est de la campagne de vaccination, nous collaborons évidemment avec nos collègues de l'Agence de la santé publique et l'ensemble du groupe de travail pour nous assurer que les organisations qui participent à la campagne disposent de l'information nécessaire pour être certains d'agir en amont. Forts de notre mandat de renseignement étranger, nous voyons aussi ce qu'il se passe à l'extérieur du pays ou au sein de notre groupe d'alliés du monde entier, et pas seulement parmi le Groupe des cinq. Nous comptons de nombreux alliés dans le domaine de la cybersécurité, et nous examinons et échangeons tous des renseignements très rapidement pour en assurer la diffusion. Notre objectif n'est pas d'observer le problème, mais bien de fournir à quelqu'un, à toute victime potentielle, quelque chose qu'elle peut utiliser pour se protéger. Tel est notre objectif réel.

Nous restons à l'affût de nouvelles manières qui nous permettraient de renforcer notre cyberrésilience à cet égard [*Inaudible*].

Le président: Je vous remercie, madame Stubbs.

Monsieur Lightbound, vous avez la parole pour six minutes.

[*Français*]

M. Joël Lightbound (Louis-Hébert, Lib.): Merci beaucoup, monsieur le président.

Je vous remercie, monsieur Jones, de votre présence au Comité, aujourd'hui. Je vous remercie aussi de ce rapport, qui est assez troublant, mais qui est relativement simple pour quelqu'un qui n'est pas nécessairement versé dans le domaine comme vous l'êtes.

Ma première question concerne les infrastructures critiques dont vous faites état dans votre rapport. J'aimerais connaître votre jugement par rapport à la situation au Canada sur la conscience de nos gestionnaires d'infrastructures critiques, d'un bout à l'autre du pays, des risques en matière de cybersécurité.

Qu'est-ce que fait le Centre pour s'assurer que ce degré de sensibilité à ses questions augmente?

[*Traduction*]

M. Scott Jones: Monsieur le président, c'est là une excellente question. Je me réjouis d'avoir l'occasion d'y répondre.

Nous collaborons avec les fournisseurs d'infrastructures essentielles du Canada depuis un certain temps. Nous devons maintenant nous concentrer sur les infrastructures les plus exposées au risque. Ainsi, le secteur de l'électricité dont nous parlons dans notre rapport est un acteur avec lequel nous travaillons afin d'établir une relation dont nous avons besoin à l'échelle du pays et avec des fournisseurs d'énergie comme l'Association canadienne de l'électricité pour nous assurer de contrer les cybermenaces de manière proactive.

Il y a plus d'un an, j'ai participé à la table ronde pour simuler ce qu'il se passerait advenant un incident de cybersécurité, juste pour m'assurer que nous étions prêts, que nous avions examiné la question de fond en comble et que le processus ne comportait aucune lacune. Nous cherchons sans cesse à nous améliorer à cet égard.

Dans ce domaine, le secteur est très au fait de l'évolution de la technologie. Très résilient, il comprend ce qu'il en est et est habitué à composer avec des facteurs comme les grands phénomènes météorologiques. La cybersécurité peut être considérée comme une autre source d'impacts du même genre. Les organisations du secteur comprennent la résilience au risque et nos échanges sont très faciles. Nous collaborons étroitement avec elles et nous cherchons à contrer les menaces. Nous essayons de voir comment nous pouvons élargir nos activités non seulement au chapitre de la cybersécurité proactive, mais aussi sur le plan de la détection des menaces avant qu'elles ne se manifestent sur le réseau. Nous cherchons enfin à mener des projets conjoints.

Au Centre canadien pour la cybersécurité, nous aimons réellement nous concentrer sur l'innovation. Nous le faisons toutefois en collaboration, tendant la main aux partenaires du secteur de l'énergie et à leurs fournisseurs pour leur demander si nous pouvons nous attaquer aux problèmes ensemble. S'il s'agit de la convergence de la technologie opérationnelle, nous leur demandons comment nous pouvons travailler avec eux et avec d'autres chefs de file de l'industrie, et comment nous pouvons voir quand une menace se présente ou quand quelqu'un les cible afin de contrer la menace de manière proactive.

Notre objectif consiste entre autres à nous assurer que les incidents sont signalés dans l'ensemble du secteur, aux quatre coins du pays et parmi tous les fournisseurs pour que la chose se sache rapidement. Si l'un d'eux est victime d'une attaque, nous ne voulons pas qu'il y en ait un deuxième. L'échange de renseignements est crucial ici aussi quand une attaque survient, car cela permet d'inoculer les autres contre la menace.

● (1550)

[*Français*]

M. Joël Lightbound: Je vous remercie, c'est un bon élément de réponse. Je pense que, bien qu'il soit récent, le Centre est assez utile à ce chapitre-là, justement pour bâtir cette relation avec les fournisseurs d'infrastructure critique.

Vous avez mentionné, dans votre présentation, le Bouclier canadien — j'aime bien le nom. Pourriez-vous faire état de l'utilisation faite par le grand public du Bouclier? Avez-vous des chiffres à cet égard?

[*Traduction*]

M. Scott Jones: Je peux vous répondre. Il s'agit en fait d'un projet de l'Autorité canadienne pour les enregistrements Internet, et j'espère ne pas lui voler sa primeur en disant qu'elle nous a avisés plus tôt cette semaine que 100 000 Canadiens utilisent maintenant ce service. C'est un bon nombre, même si, honnêtement, il n'est pas aussi élevé que je le voudrais, car cet outil renforce considérablement la protection des renseignements personnels.

Sachez que lorsque nous avons réfléchi à la question et collaboré avec l'Autorité canadienne pour les enregistrements Internet à la mise en œuvre de ce service, nous souhaitions qu'il fonctionne indépendamment du gouvernement, car nous ne voulions pas donner l'impression que nous pouvions potentiellement recueillir des données sur les Canadiens. Cela ne fait pas partie de notre mandat et cela ne s'inscrit certainement pas dans la loi qui nous régit. Une évaluation de la protection des renseignements personnels va toutefois de pair avec le projet.

J'espère que lorsque les Canadiens s'intéressent à la question, ils verront les solutions qui s'offrent à eux. Nous avons reçu des commentaires d'experts de la protection des renseignements personnels de l'industrie qui ont parlé de ce programme et de la manière dont il a été conçu. J'espère qu'à mesure qu'ils apprennent l'existence de ce programme, les Canadiens seront plus nombreux à s'en prévaloir, car il permet à tous les Canadiens de faire quelque chose pour se protéger grâce à un outil silencieux et discret.

Pour ma part, voici comment je décrirais le programme. Nous craignons tous de commettre une erreur et de cliquer sur un lien dans un courriel, déclenchant ainsi des conséquences catastrophiques. Le Bouclier canadien et nos démarches visent à faire en sorte que si on clique sur un lien, il n'y aura pas de conséquences, car le lien sera bloqué. Voilà, en quelque sorte, ce que fait le Bouclier.

[*Français*]

M. Joël Lightbound: Dans votre rapport, vous nommez spécifiquement quatre pays comme étant des risques, dont la Corée du Nord et la Chine.

Quels sont les facteurs qui entrent en ligne de compte pour nommer ces pays plutôt que d'autres?

[*Traduction*]

M. Scott Jones: Voilà une excellente question que j'espérais ardemment que quelqu'un me pose.

Il n'a pas été facile de décider de nommer des pays, car cela détourne immédiatement l'attention de tous les autres aspects du rapport pour la diriger vers ces quatre pays. Cependant, le fait est que le gouvernement du Canada a interpelé... À un certain moment, nous avons attribué certaines cyberactivités malintentionnées à l'un de ces quatre pays ou nous nous sommes joints à nos alliés pour le faire. Il s'agissait donc des quatre choix logiques. Ce sont aussi les quatre acteurs qui ont démontré qu'ils possédaient les capacités qui présentent un risque pour le Canada dont nous avons parlé. D'un côté, nous avons pensé que le fait de les nommer détournerait l'attention de certaines choses dont nous voudrions parler, comme le fait qu'un cinquième ou un sixième pays pourrait très facilement s'ajouter à la liste. Par contre, nous devons admettre le fait que ces quatre pays sont là et présentent un risque stratégique important pour le Canada en raison de leurs capacités et de ce qu'ils sont en mesure de faire.

Nous avons donc discuté de la question, mais sachez que la décision de nommer les pays vient plus du point de vue de la cybersécurité. Nous appuyons certainement cette décision, mais elle relève en fait des politiques et des affaires étrangères.

Le président: Nous allons devoir en rester là, monsieur Lightbound.

[*Français*]

Madame Michaud, vous disposez de six minutes.

Mme Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Merci, monsieur le président.

Monsieur Jones, je vous remercie de votre présence et de la publication de votre rapport. C'est en effet très intéressant et inquiétant à la fois. Je pense que la population en générale n'est pas tout à fait consciente du danger que la cybersécurité présente ou des cybermenaces dont vous faites état dans votre rapport.

Vous nous avez parlé du vol de données personnelles, par exemple, et du danger physique pour les Canadiens et les Québécois. J'aimerais que vous nous disiez de quelle façon la population générale devrait se protéger à cet égard.

Y a-t-il un certain devoir d'éducation des différents paliers de gouvernement?

Ce domaine évolue assez rapidement, vous l'avez évoqué. On est de plus en plus connecté et dépendant de toute cette technologie, notamment depuis la pandémie de la COVID-19 et le télétravail.

De quelle façon devrait-on mieux conscientiser les gens et de quelle façon ceux-ci pourraient-ils mieux se protéger?

● (1555)

[*Traduction*]

M. Scott Jones: Je pense qu'il y a certaines choses qui me préoccupent légèrement. Le rapport a pour but d'informer; nous espérons ne pas susciter la peur, car selon nous, elle n'incitera pas les Canadiens à prendre des mesures dans la plupart des cas. Nous espérons toutefois pouvoir proposer quelques mesures simples aux Canadiens pour qu'ils puissent se protéger en ligne. Le site Pensez cybersécurité est une excellente source à cet égard, qu'il s'agisse du compte Twitter ou du compte en ligne. Il propose certaines mesures très faciles que nous voudrions demander aux Canadiens de prendre.

L'une d'elles concerne les mots de passe. Nous avons constaté que le mot de passe le plus utilisé au Canada reste « mot de passe », le second étant « 123456 ». Cette situation, dénoncée dans un rapport, est assez courante un peu partout dans le monde. Ce choix ouvre la porte aux acteurs malintentionnés et leur facilite la tâche. Je sais que les mots de passe constituent un cauchemar pour tout le monde, mais le fait d'agir sur un élément aussi simple peut réellement renforcer la cybersécurité.

L'autre mesure simple que les gens peuvent prendre consiste à activer les mises à jour automatiques. Plutôt que d'effectuer les mises à jour manuellement sur son téléphone ou son ordinateur, il suffit d'activer la mise à jour automatique. Voilà qui rehausse aussi la cybersécurité d'un cran. Nous constatons que ces dernières années, ce sont les systèmes de base désuets qui sont à l'origine de la plupart des atteintes à la cybersécurité. Ce sont là deux mesures simples à prendre.

En ce qui concerne votre question, nous avons tenté de préparer à l'intention des petites et moyennes entreprises un guide comprenant des mesures simples et sans tracas qu'elles peuvent prendre, car elles n'ont pas besoin d'être expertes en cybersécurité, pas plus qu'elles ne devraient l'être, d'ailleurs. C'est ainsi que nous guidons les petites et moyennes entreprises. Nous avons élaboré ce guide expressément pour que 20 % des efforts que nous déploierions dans le cadre d'un programme de cybersécurité pour entreprise donnent 80 % des bénéfices.

Nous tentons de prendre des mesures pratiques et pragmatiques, auxquelles s'ajoutent des initiatives amusantes, comme le guide de cadeaux des Fêtes et d'autres outils appropriés à ce temps-ci de l'année, espérant ainsi aider les Canadiens à effectuer de bons choix au chapitre de la sécurité en ligne.

[*Français*]

Mme Kristina Michaud: Je vous remercie, monsieur Jones.

Je vais certainement partager ce guide de cadeau des Fêtes. Il semble très bien, notamment pour informer nos concitoyens.

Je reviendrai maintenant sur les petites entreprises, les grandes entreprises et toutes celles qui pourraient être menacées de cyberattaque. Nous avons vu de petites entreprises victimes de demandes de rançon hésiter à consulter des avocats et payer afin de récupérer leur propriété ou leurs données personnelles. Plusieurs articles dans les médias ont indiqué que de petites entreprises ont été victimes de cela.

Les compagnies d'assurance pourraient peut-être jouer un plus grand rôle et les avocats pourraient être plus informés à ce sujet. Je me tourne vers le gouvernement fédéral. Quel rôle peut-il jouer dans ce cas?

Nous pouvons effectivement jouer un rôle d'informateur, mais y a-t-il des programmes gouvernementaux ou des changements législatifs qui pourraient être mis en place?

Tout cela évolue très rapidement, alors quel pourrait être le rôle du gouvernement fédéral dans tout cela?

[*Traduction*]

M. Scott Jones: Je pense qu'un certain nombre de facteurs entrent en ligne de compte.

L'embarras, la honte et la crainte d'une perte potentielle de clients empêchent certainement les organisations de signaler les incidents. Dans le domaine de la cybersécurité, les citoyens tendent malheureusement à punir la victime plutôt que l'auteur. Ils tendent à tourner le dos à l'organisation, qui est ainsi incitée à ne pas admettre qu'elle est victime d'un incident de cybersécurité.

Il faut également tenir compte de l'embarras, puisque la situation découle souvent d'une erreur. Parfois, ce n'est pas parce qu'un correctif n'a pas été appliqué, mais parce que les gens ont cliqué quelque chose sur lequel ils n'auraient pas dû cliquer. Nous devons donc déstigmatiser cela et conscientiser les gens. On peut tomber dans le panneau. Certains des cybercriminels sont si habiles que ce n'est qu'une question de temps avant que je ne clique sur quelque chose, car les courriels sont très bien conçus.

Ainsi, si je sais que c'est le cas avec le travail que je fais, personne d'autre ne devrait avoir honte de se faire prendre. Je serai probablement embarrassé quand je cliquerai sur le lien, mais je m'en remettrai.

Sachez enfin que nous avons appris que les compagnies d'assurance conseillent aux organisations de ne pas signaler les incidents et de ne pas s'adresser à la police. Il est donc difficile de réagir au problème et d'obtenir des statistiques justes à ce sujet afin de savoir où affecter nos ressources pour contrer des menaces précises. Si nous voulons commencer à nous attaquer à une forme donnée de cybercriminalité, par où commencer si nous ne savons pas ce qui frappe les Canadiens?

La cybercriminalité constitue malheureusement un problème mondial, mais nous devrions nous concentrer sur les menaces qui ciblent les Canadiens, et c'est un défi pour nous et la GRC, car les organisations canadiennes ne signalent tout simplement pas les incidents pour un éventail de raisons, que ce soit parce qu'elles sont embarrassées ou parce qu'on leur conseille de ne pas les signaler et de payer la rançon pour pouvoir reprendre leurs activités en ligne.

● (1600)

Le président: Je vous remercie, monsieur Jones.

Monsieur Harris, vous disposez de six minutes.

M. Jack Harris (St. John's-Est, NPD): Je vous remercie, monsieur le président.

Je vous remercie de témoigner devant nous aujourd'hui, monsieur Jones.

C'est un rapport qui donne beaucoup à réfléchir. Il est encourageant de savoir que nous pouvons faire quelque chose nous-mêmes. Je voudrais d'abord vous interroger sur le Bouclier canadien de l'Autorité canadienne pour les enregistrements Internet, que vous qualifiez de « service DNS protégé offert gratuitement par l'ACEI qui bloque la connexion aux sites malveillants ».

Sachez tout d'abord qu'étant néophyte en la matière, j'entends parler du sujet pour la première fois aujourd'hui. Je vous remercie donc de nous informer.

Premièrement, qu'est-ce qu'un service DNS, et deuxièmement, protégez-vous vous-mêmes tous vos appareils personnels connectés à l'aide du Bouclier canadien de l'ACEI?

M. Scott Jones: Je le fais certainement. Je répondrai avec plaisir à vos questions.

En ce qui concerne tout d'abord le service DNS, Internet fonctionne grâce à des séries de chiffres. Nous nous rendons à www.website.com, mais Internet ne comprend pas ces caractères. Le service DNS les traduit en adresse Internet appelée adresse IP, laquelle indique à Internet le chemin à suivre pour se rendre à destination.

Les cybercriminels exploitent cette fonction en créant, par exemple, un domaine ou un site Web appelé « cyber.gcca » s'ils tentent de se faire passer pour le Centre. Quand les gens cliquent sur le lien, ils peuvent ne pas remarquer qu'il manque un point. Les Canadiens tombent ainsi les yeux fermés dans le piège de la fausse erreur de frappe et se retrouvent sur un site qui ressemble à celui du Centre, sauf qu'ils téléchargent un maliciel quand ils y arrivent.

Le pare-feu DNS fait en sorte que le site est accidentellement bloqué parce qu'il est illégitime, et quand les gens cliquent sur le lien, ils ne sont pas redirigés vers le site. Le service protège les gens des conséquences causées par une adresse mal écrite ou une tentative délibérée...

J'utilise certainement ce service. Je l'ai installé sur mes appareils personnels, car à dire vrai, cela me confère un degré de protection. J'admets que ce n'est qu'une question de temps avant que quelque chose n'arrive et que je clique sur un lien. Je veux donc m'assurer d'être aussi protégé que possible à tous les égards.

M. Jack Harris: Je vous remercie. Si cet outil est assez bon pour vous, il l'est pour moi. Je pense aussi qu'il le serait pour bien gens et qu'ils devraient s'en prévaloir. Je vous remercie de ces explications. J'ai fait un pas de plus vers la sécurité.

Permettez-moi de vous poser une question sur les rançongiciels. Vous affirmez que ces rançongiciels continueront de constituer une menace. Si on fait abstraction de la question de la rançon, la capacité d'empêcher quelqu'un d'accéder à Internet m'apparaît en soi comme une menace. Un individu, un criminel ou un État qui a accès à cette capacité et qui en dispose dans son arsenal pour s'en servir dans le cadre d'hostilités doit être considéré comme une menace dont doit se prémunir tout gouvernement ou tout pays qui souhaite se défendre, comme nous nous défendrions au moyen de capacités antiaériennes.

Le Canada est-il protégé contre ce genre de menace qui pèse non seulement sur les infrastructures essentielles comme les réseaux électriques, mais aussi sur les banques, les hôpitaux, l'accès aux renseignements médicaux dont on peut avoir besoin pour soigner des patients ou des éléments qui pourraient mettre à l'arrêt non seulement l'économie, mais l'activité en général?

M. Scott Jones: Je pense que plusieurs éléments entrent en jeu sur le plan de la sécurité. Il y a la confidentialité — soit la protection de l'information comme telle —, puis la disponibilité et l'intégrité de l'information transmise pour qu'elle ne soit pas modifiée en cours de route.

Vous parlez en fait de la disponibilité, et je pense qu'il s'agit d'une question importante. Plusieurs techniques pourraient être utilisées à cet égard.

Si vous vouliez bloquer mon accès Internet en ce moment même, vous pourriez lancer une attaque de déni de service distribué et submerger ma connexion Internet de manière à ce qu'elle ne sache plus ce qui constitue une bonne ou une mauvaise donnée. Des mesures d'atténuation très solides sont en place à ce chapitre. Les entreprises de télécommunications canadiennes peuvent se défendre contre de telles attaques depuis des années. Ces attaques surviennent constamment à notre insu sur Internet, car les entreprises s'en défendent très bien.

D'autres attaques cibleront des éléments précis des infrastructures en y exploitant habituellement une vulnérabilité. Elles pourraient prendre la forme d'un acheminement par inondation qui submergerait...

M. Jack Harris: Est-ce que nous pourrions nous centrer sur la capacité relative aux rançongiciels?

M. Scott Jones: Oui.

M. Jack Harris: On bloque l'accès. C'est donc une capacité particulière, sans égard à la rançon. Est-ce qu'il est possible pour un pays ou une opération de le faire en bloc? Est-ce que toute la nation est vulnérable? Si oui, est-ce que nous avons un moyen de défense à cet égard?

● (1605)

M. Scott Jones: En règle générale, les rançongiciels ne fonctionnent pas de cette façon. Ils servent habituellement à cibler une chose précise pour la tenir en otage ensuite, qu'il s'agisse de vos données ou de votre système. Les pirates menacent ensuite de diffuser l'information ou de la chiffrer afin qu'elle vous soit inaccessible, si vous ne les payez pas. Ils visent habituellement une organisation à la fois.

En ce qui concerne les attaques en bloc, nous avons vu certains rançongiciels se propager. Par exemple, l'entreprise Maersk Shipping a été la cible d'un rançongiciel, tout comme le National Health Service, au Royaume-Uni, qui a vu le rançongiciel se propager et devenir hors de contrôle.

Pour se défendre contre cela, il faut bloquer les systèmes infectés et utiliser un modèle de confinement. Il faut en même temps partager l'information et immuniser le système. Nous pouvons réagir et mettre en place des mesures pour protéger le système. La communauté mondiale est habile pour gérer ce genre de situation, ce qui ne signifie pas pour autant que ces processus ne feront pas de victimes.

M. Jack Harris: Croyez-vous qu'on pourrait utiliser ce genre de logiciel de façon organisée et coordonnée ou massive pour attaquer un pays ou ses institutions, qu'il s'agisse d'un hôpital ou...

Le président: Nous allons devoir en rester là. M. Harris a dépassé son temps de parole.

La parole est maintenant à M. Motz. Vous disposez de cinq minutes.

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

Merci, monsieur Jones, d'être avec nous à nouveau. Votre expertise dans le domaine nous est très utile. Nous vous remercions pour l'excellent service du Centre de la sécurité des télécommunications.

Monsieur Jones, vous avez déjà témoigné devant le Comité au sujet de votre approche relative à la protection des systèmes et réseaux mobiles et de télécommunications, par l'entremise d'un système semblable à celui du Royaume-Uni qui vise une inspection préalable à toute installation. Comme vous le savez, le Royaume-Uni n'utilise plus ce modèle et a même infirmé sa décision d'accepter Huawei à la suite de problèmes de sécurité soulevés par l'équipe de sécurité du gouvernement.

Nous savons tous que Huawei est une société contrôlée par l'État chinois, et que les lois du pays en matière de sécurité ne peuvent être appliquées de façon sécuritaire au Canada selon divers experts indépendants... En fait, tous les experts que j'ai entendus.

Est-ce que votre équipe travaille toujours à une recommandation pour le ministre ou l'avez-vous déjà informé à ce sujet et conseillé sur la meilleure façon de procéder?

M. Scott Jones: Je crois qu'il est important de souligner que mon rôle est d'émettre des conseils au sujet des politiques. Les décisions sont ensuite prises par le gouvernement et les élus. Je dois faire attention de ne pas... Mon objectif n'est pas... Je ne suis pas élu, alors je respecte vraiment...

M. Glen Motz: Je vous remercie, monsieur Jones. Selon votre réponse, je suppose que vous avez déjà présenté ce document au ministre. Si c'est le cas, je vous en remercie. Je suis certain qu'il sera très utile en vue de prendre une décision.

Votre rapport souligne de nombreuses façons les attaques indirectes visant à obtenir l'accès à certains systèmes, par l'entremise des fournisseurs, des partenaires d'affaires, des clients et des gouvernements... Tout cela pour atteindre une cible précise. Nous savons aussi que la Chine a été ciblée par divers organismes de sécurité de notre pays et d'autres également. Il serait contre-productif de voir un système qui transfère tous nos renseignements — à savoir, Internet — être contrôlé par une entreprise qui relève d'un pays qui se consacre au vol, à la mésinformation, à l'espionnage et aux perturbations.

Pouvez-vous m'aider, et aider les Canadiens, à comprendre pourquoi nous n'avons toujours pas de réponse à propos de Huawei?

Le président: Monsieur Motz, vous avez demandé deux fois à un représentant du gouvernement de commenter une décision du cabinet. Je crois que M. Jones a refusé de répondre à la question la première fois. Il devra probablement refuser d'y répondre une deuxième fois.

M. Glen Motz: Je vous remercie pour votre intervention, monsieur le président. J'aimerais que vous retiriez ce temps de parole des cinq minutes qui me sont accordées. J'en serais très heureux.

Monsieur Jones, avant...

Le président: Vous savez que je suis toujours généreux avec vous, monsieur Motz.

● (1610)

M. Glen Motz: Pas autant que vous l'êtes avec M. Harris, mais espérons qu'aujourd'hui sera une bonne journée.

Le président: Il s'en tire très bien, je dois l'admettre.

M. Glen Motz: Monsieur Jones, vous avez déjà dit que vous étudiez la façon de gérer les produits de sécurité — et c'est la clé — au sein de la chaîne d'approvisionnement mondiale. Vous avez aussi parlé des mises à jour des logiciels. C'est l'objectif que vous visiez lorsque vous avez comparu devant nous il y a quelque temps. C'était en septembre 2018. Cela fait maintenant deux ans. Avez-vous réussi à sécuriser l'équipement et les logiciels qui pourraient être en cause?

M. Scott Jones: C'est une question assez complexe, mais je vais tenter d'y répondre.

Je crois qu'elle comporte plusieurs éléments. De façon générale, puisque les technologies et Internet font partie d'une chaîne d'approvisionnement mondiale, les logiciels sont vulnérables à de nombreux égards. Nous visons quelques objectifs à cette fin.

Le premier consiste à renforcer la sécurité et à poursuivre notre travail avec diverses industries. Dans le contexte des infrastructures électriques du Canada, nous voulons intégrer la sécurité, mais pas seulement dans les produits en soi. Nous adoptons une approche similaire à celle que nous aurions utilisée dans le monde de la sécurité pour l'équipement. Nous voulons surveiller cet équipement pour veiller à ce qu'il fonctionne comme prévu. Il faut qu'il soit le plus sécuritaire possible, même s'il y aura probablement des faiblesses. Ensuite, il faut trouver une façon de le surveiller pour veiller à ce qu'il fonctionne comme prévu et pour intervenir rapidement au besoin. Il faut accroître notre capacité d'intervention également. Dans l'industrie, on parle de la gestion de la détection et de l'intervention, mais il faut surtout savoir et comprendre que rien n'est intouchable de nos jours. Tous les systèmes ont des faiblesses, peu importe l'endroit où ils ont été fabriqués et...

M. Glen Motz: Il serait donc juste de dire que nous ne pouvons garantir la sécurité, et qu'il s'agit d'une lutte continue. Il faut faire preuve de vigilance pour l'avenir. Il serait donc logique de vouloir utiliser les produits des pays de confiance uniquement. Ce serait sensé.

J'ai une question. Vous avez témoigné devant le CPSNR. Comme vous le savez, nous avons récemment présenté un rapport qui explique en détail nos préoccupations relatives à l'interférence et à l'influence étrangères au Canada, et aussi la façon dont la Chine joue un rôle à cet égard.

Notre pays a été désigné à titre de cible attrayante et permissive, selon ce rapport. D'après vous...

Le président: Monsieur Motz, j'arrête l'horloge.

M. Glen Motz: Ma question vise à savoir ce que nous pouvons faire pour changer cela.

Le président: D'accord. Je veux être prudent quant aux questions, réponses et délibérations associées au CPSNR. Il s'agit d'un comité de parlementaires dont les membres sont assujettis à un niveau de confidentialité très élevé, tout comme vous.

M. Glen Motz: Oui.

Le président: Je voulais simplement m'assurer que vous respectiez ces limites. Nous savons qu'elles sont importantes de nos jours.

M. Glen Motz: Oui, je sais qu'elles sont très importantes. Je ne veux pas aller en prison pour cela. Ces éléments font partie du rapport du CPSNR et sont déjà d'ordre public.

Le président: D'accord.

M. Glen Motz: Monsieur Jones, vous avez lu le rapport. Que devons-nous faire, en tant que pays, pour ne plus être une cible aussi facile? Nous sommes une cible attrayante et permissive. Que devons-nous faire différemment?

M. Scott Jones: Je crois que c'est un défi. Mon objectif, c'est la cybersécurité. Donc, pour rehausser la cybersécurité dans cet espace, nous encourageons tous les Canadiens à prendre certaines mesures de base, des mesures faciles qui peuvent nous aider. J'en ai parlé plus tôt: une hygiène de base et l'application de correctifs auraient une incidence énorme sur notre industrie et sur la cybersécurité. Nous serions immédiatement mieux protégés contre les activités et l'exploitation externes.

L'important aussi, c'est de ne pas se fier uniquement au coût pour le choix des applications et des technologies. Le produit le moins cher n'est pas nécessairement le meilleur. Il faut déterminer ce qui est important sur le plan de la sécurité et trouver des façons de le mesurer, ce qui est un défi pour tous. Je sais que nous voulons tous faire de bonnes affaires — surtout à l'approche du temps des Fêtes, avec les cadeaux— , mais souvent, les technologies peu coûteuses sont désuètes; elles ne sont pas à jour et n'ont pas reçu les derniers correctifs.

● (1615)

Le président: Nous devons nous arrêter là, malheureusement, monsieur Motz. Vous avez largement dépassé votre temps de parole.

Madame Khera, vous disposez de cinq minutes.

Mme Kamal Khera (Brampton-Ouest, Lib.): Merci, monsieur le président.

Merci, monsieur Jones, de témoigner devant nous. Merci aussi pour votre rapport et pour votre travail exceptionnel.

Je vais poursuivre là où s'est arrêtée ma collègue, Mme Michaud. Dans votre rapport, vous soulignez qu'au Canada, la majorité des cyberincidents pourraient être évités si l'on suivait quelques règles de base en matière de cybersécurité. Ces événements sont tout à fait évitables. Quelles mesures le Centre peut-il prendre pour accroître la sensibilisation et la conformité, afin de veiller à ce que les Canadiens fassent le nécessaire pour se protéger? Que peuvent faire les gens de ma circonscription? Quelle est la part de responsabilité des entreprises, des particuliers et du gouvernement?

M. Scott Jones: C'est une excellente question.

Je ne veux pas qu'on pense que nous blâmons les Canadiens ou les entreprises, parce que la situation n'est pas facile. Le problème avec le monde des technologies, c'est que nous avons rendu la tâche trop difficile pour les entreprises. Elles n'arrivent pas à se tenir à jour. Les propriétaires de petites entreprises n'ont pas à être des experts en matière de pare-feu ou de réseaux. Nous pourrions prendre certaines mesures pour leur faciliter la tâche.

Il y a toutefois certaines mesures faciles à prendre. Nos lignes directrices à l'intention des petites et moyennes entreprises présentent des étapes faciles à suivre, qui ont été rédigées de façon accessible. J'ai beaucoup aimé vos commentaires au sujet de l'accessibilité du rapport. Nous voulons que tous les Canadiens puissent s'en servir.

Nous publions des conseils à l'intention des particuliers. Nous voulons présenter des mesures simples à prendre pour sécuriser votre environnement. Vous pouvez, par exemple, créer un mot de passe unique pour votre compte bancaire. Ainsi, si le mot de passe n'est pas utilisé à d'autres fins — si vous n'utilisez jamais ce mot de passe —, alors vous montez la barre pour votre banque. L'authentification multifactorielle est plus difficile. Si elle est activée, personne d'autre ne peut se connecter en utilisant vos renseignements. Même si cette personne a votre mot de passe, elle doit passer par une autre étape de vérification, ce qui complique les choses. Ainsi, le pirate informatique passera à une autre personne. Ce que nous proposons, c'est de mettre des bâtons dans les roues des criminels. Ainsi, au lieu de s'acharner, ils passeront à la prochaine cible, qui n'a pas dressé les mêmes obstacles. Cette stratégie fonctionne seulement pour les particuliers.

Toutefois, les entreprises, et surtout les grandes organisations, en valent parfois la peine. Ainsi, les criminels investissent dans le développement de capacités uniques pour les attaquer. C'est ce qu'on appelle « la chasse au gros gibier », que pratiquent les pirates informatiques. Ils savent que les grandes organisations ont d'importants budgets et plus de ressources en matière de cybersécurité, et qu'elles peuvent faire appel à un fournisseur qualifié pour les aider.

Mme Kamal Khera: Merci.

Nous avons aussi entendu parler des conséquences de la COVID-19 sur l'interférence étrangère et des attaques informatiques pendant la pandémie, puisque nous vivons maintenant dans un univers virtuel. Ce sera peut-être le cas lorsque les vaccins seront offerts et que d'autres éléments seront mis en place. Quelles mesures supplémentaires le Centre a-t-il prises depuis le début de la pandémie? Je pense notamment au Centre antifraude du Canada, géré par la GRC.

M. Scott Jones: Dès le début de la pandémie, nous avons notamment travaillé avec les fournisseurs — partenaires du monde entier, fournisseurs commerciaux — pour fermer tous les sites qui se faisaient passer pour le gouvernement du Canada. Je pense que nous avons tous reçu des appels de gens qui disent représenter un organisme gouvernemental. La même chose se produit sur Internet, avec les courriels qu'on reçoit, etc. Nous en avons démantelé plus de 4 000 depuis le mois de mars. Voilà ce que nous avons fait pour tenter de réduire le nombre de fraudes.

Deuxièmement, nous avons essayé de sensibiliser les gens. Nous avons mené des campagnes de sensibilisation du public en collaboration avec la GRC et le Centre antifraude du Canada afin d'informer les Canadiens en leur disant de prendre garde à certaines choses que nous avons observées. Nous avons vraiment intensifié les campagnes de sensibilisation au pays. Nous tenons à diffuser l'information rapidement afin qu'elle se rende aux Canadiens, pour qu'ils aient tous les renseignements nécessaires sur les nouveaux types de fraudes.

Troisièmement, nous avons travaillé en collaboration avec les entreprises de télécommunications à mesure que les Canadiens signalaient les pourriels reçus. Nous avons réussi à mettre en place des mesures proactives pour toute mesure liée au gouvernement du Canada. Par exemple, pour les programmes mis en place par le gouvernement, notamment la PCU ou d'autres prestations d'urgence, nous nous sommes assurés d'en connaître la présentation d'avance de façon à mettre en place des mesures de détection des fraudes. Ainsi, nous avions des fournisseurs commerciaux qui cherchaient activement à déceler de faux sites de la PCU afin de les supprimer avant qu'ils ne fassent des victimes parmi les Canadiens.

Nous essayons vraiment d'avoir une longueur d'avance. Par conséquent, nous nous sommes appuyés sur les ministères responsables de la diffusion des renseignements.

Enfin, nous invitons tout le monde à chercher des informations à la source. Si vous recherchez des faits, consultez la source pour obtenir les faits réels. Pour moi, en temps de pandémie, ces sources de faits sont Santé publique Ottawa, Santé publique Ontario et l'Agence de la santé publique du Canada. Évidemment, cela varie selon l'endroit où l'on habite.

● (1620)

Le président: Merci, madame Khera.

Mme Kamal Khera: Merci.

Le président: Nous passons à Mme Michaud pour deux minutes et demie.

[*Français*]

Mme Kristina Michaud: Je vous remercie, monsieur le président.

J'aurais bien aimé en savoir en peu plus, comme mon collègue M. Motz, sur tout ce qui touche à la 5G et à la gestion du gouvernement. Je ne veux pas entrer là, mais quand même, dans le désir d'informer les citoyens, encore une fois, je suis certaine que mes collègues ont reçu autant de courriels que moi de la part de la population sur la 5G, qui est inquiétante. Je crois qu'elle divise aussi. Il y a beaucoup d'incompréhension. J'aimerais que vous nous en parliez.

Vous disiez plus tôt que la population ne devait pas avoir peur ni être inquiète, mais il y a quand même un devoir d'information.

[*Traduction*]

M. Scott Jones: Je ne suis pas certain de comprendre la question. Je suis désolé.

[*Français*]

Mme Kristina Michaud: Je peux la reformuler.

Comment se traduisent les menaces de la 5G pour les Canadiens et pour les Québécois?

Nous recevons beaucoup de courriels de la part de nos concitoyens, qui s'inquiètent de ce que cela peut représenter pour leur santé physique ou intellectuelle. Dans le but de les rassurer, peut-être, j'aimerais vous entendre sur ce que cela représente en ce moment.

[*Traduction*]

M. Scott Jones: Merci. Je suis désolé d'avoir eu de la difficulté à comprendre.

Je voudrais souligner quelques aspects. Je pense que lorsque nous examinons une nouvelle technologie ou un nouveau développement sur le marché... Il y a de la désinformation au sujet de la 5G, mais je vais laisser cela de côté pour me concentrer sur les aspects de sécurité. Il faut savoir qu'il s'agit d'un réseau qui peut supporter beaucoup plus d'appareils, de sorte que les communications sont beaucoup plus rapides. Il offre une bande passante beaucoup plus large, est beaucoup plus rapide, peut supporter beaucoup plus d'appareils connectés, et est pratiquement en temps réel. Donc, avec ce type de réseau, on peut faire des choses comme envoyer des commandes à des voitures autonomes. Il est conçu pour ce type d'environnement.

Nous cherchons en général des menaces liées à la confidentialité, à l'intégrité et à la disponibilité de certaines choses, comme le réseau. Concernant le réseau lui-même, puis-je communiquer? C'est la disponibilité. On cherche à connaître la robustesse de l'équipement. Y a-t-il plusieurs fournisseurs, de façon à pouvoir remplacer son équipement, au besoin, si un fournisseur devient moins fiable? C'est lié à la disponibilité.

Nous examinons ensuite l'intégrité. Si j'envoie un message par l'intermédiaire de ce réseau, arrivera-t-il tel quel? C'est là que le cryptage entre en jeu: c'est la pièce maîtresse de l'intégrité. Si je veux qu'un message soit livré clairement, je devrai l'envoyer de manière à ce qu'il ne puisse être modifié. Voilà l'utilité du cryptage: l'intégrité. Il peut s'agir de choses comme les signatures numériques, etc. Cela signifie que le message ne peut pas être modifié. C'est ce que permet la cryptographie.

Le dernier...

Le président: Je dois malheureusement vous interrompre.

Monsieur Harris, vous avez deux minutes et demie.

M. Jack Harris: Merci, monsieur le président.

Je décèle dans certaines observations et suggestions liées à certains de vos travaux un certain reproche à l'égard des victimes. Il va sans dire que les gens ne sont pas des spécialistes dans l'utilisation de ces équipements.

Invitez-vous les gens à apporter certains correctifs à nos systèmes? Le gouvernement peut-il exiger l'élimination de certaines étapes, même simples, par l'intermédiaire des fournisseurs de systèmes, des fournisseurs Internet ou des groupes de fabricants, afin d'améliorer la sécurité des gens?

M. Scott Jones: Nous ne voulons certainement pas jeter le blâme sur les victimes à cet égard. Je suis conscient qu'il est difficile de rester à jour pour tout cela.

La première chose que nous disons aux entreprises et aux particuliers, c'est d'activer les mises à jour automatiques; sur les téléphones, il suffit de glisser le bouton pour les activer. Cependant, l'industrie doit faciliter les choses, ce qui est souvent le cas, maintenant. Les mises à jour de nos portables et ordinateurs personnels se font par défaut, et il faut modifier les réglages manuellement pour empêcher les mises à jour automatiques, pour qu'elles soient en mode manuel.

C'est un bon progrès, mais il faut faire mieux.

Le vrai défi, ce sont les entreprises dont l'équipement n'est pas mis à jour automatiquement. Un administrateur système doit alors télécharger un correctif ou une mise à jour, l'installer directement sur l'appareil et faire des essais, ce qui peut fonctionner ou non, car l'appareil pourrait ne pas être convivial. L'industrie doit vraiment commencer à renforcer la cybersécurité à cet égard afin d'aider les PME à rester à jour plus facilement.

Cependant, il y a de l'espoir. Le nuage offre certains avantages à ces entreprises grâce aux mises à jour automatiques. Une des choses que nous avons faites lors de la création du Centre canadien pour la cybersécurité a été de transférer nos opérations dans le nuage, car nous voulions fonctionner comme toutes les entreprises canadiennes, à ce moment-là et à l'avenir. Nous voulions suivre nos propres conseils. Ce que nous faisons, c'est... Je reçois des mises à jour. En fait, je viens de voir — mon ordinateur vient de me l'indiquer — que j'ai reçu une mise à jour pour l'environnement Microsoft Teams que nous utilisons. Donc oui, nous recevons les mises à jour. Vous les recevez dès qu'elles sont offertes par le fournisseur.

Cela facilite les choses. Cela allège le fardeau pour les petites et moyennes entreprises, car procéder ainsi signifie qu'on n'a pas à s'en occuper soi-même. Vous n'avez pas à télécharger les correctifs ni à les installer, car c'est inclus.

Voilà l'aspect qui doit être plus facile pour les utilisateurs. Il ne s'agit pas de leur faire porter le blâme.

● (1625)

Le président: Très bien.

Merci, monsieur Harris.

Monsieur Van Popta, vous avez cinq minutes.

M. Tako Van Popta (Langley—Aldergrove, PCC): Excellent.

Monsieur Jones, je vous remercie d'être avec nous aujourd'hui. Merci de votre témoignage très instructif.

J'ai une question sur les universités et les cybermenaces liées au vol de la propriété intellectuelle. J'aimerais avoir vos commentaires à ce sujet, dans le contexte, bien sûr, des partenariats qu'établissent certaines universités de recherche avec des entreprises étrangères pour aider au financement de leurs recherches.

M. Scott Jones: Je pense qu'un des aspects pour lesquels nous avons fait un important travail de sensibilisation, avec nos collègues du Service canadien du renseignement de sécurité, a été d'aider à informer les universités des menaces qui pèsent sur elles et de leur donner des conseils pratiques. Elles œuvrent dans le secteur de la recherche ouverte, ce qui comporte des défis particuliers en matière de cybersécurité.

Nous avons aussi travaillé avec ce qu'on appelle CANARIE, le réseau canadien pour la recherche et l'innovation. C'est un organisme à but non lucratif. Nous avons travaillé avec le réseau pour en améliorer la cybersécurité et nous avons l'aussi appuyé dans ses efforts pour renforcer la cybersécurité dans toutes les universités canadiennes. Nous essayons de prendre des mesures pratiques pour faciliter la protection de la propriété intellectuelle.

En fin de compte, les organismes doivent en arriver à un équilibre, et je m'en remettrais à mes collègues du SCRS à cet égard. Souvent, dans leur enthousiasme à l'égard de leurs travaux, les gens sont simplement heureux de parler des recherches en cours et de les diffuser. Je vous invite à poser la question au Service canadien du renseignement de sécurité pour obtenir son expertise à ce sujet.

De notre point de vue, cependant, la menace interne... Nous essayons de renforcer la cybersécurité, et nous le faisons en partenariat. CANARIE est un exemple pour l'accès à la recherche. Nous communiquons aussi avec les universités canadiennes pour leur offrir des conseils et des informations concrètes sur les menaces possibles à la cybersécurité afin qu'elles renforcent leurs mesures.

M. Tako Van Popta: Quelle est l'importance de la menace sur le plan économique? Quelle est la valeur de la propriété intellectuelle volée aux universités? Quelle est l'ampleur du problème?

M. Scott Jones: J'aimerais bien avoir une réponse à cette question. Je ne sais pas.

Notre mandat ne comprend pas la collecte de renseignements au Canada. Nous nous appuyons sur des statistiques, comme celles de Statistique Canada ou les données publiées par d'autres organismes. Je n'ai pas vu de données chiffrant les pertes des établissements canadiens, que ce soit à court et à long terme.

Je suis désolé.

M. Tako Van Popta: Très bien.

La solution la plus simple serait-elle que les universités cessent de s'associer avec des acteurs étrangers?

M. Scott Jones: Je ne suis pas un expert. Il vaudrait peut-être mieux poser la question à des intervenants plus au fait des partenariats universitaires.

Un aspect qui ressort de nos rencontres avec certains organismes, c'est que la recherche est mondiale et que les partenariats sont vraiment importants. Tous les partenaires étrangers... Je ne suis pas certain que les universités se diraient capables de maintenir ces activités.

Nous avons l'habitude de conseiller aux organismes d'être pleinement conscients des menaces et de leurs objectifs. La relation est-elle mutuellement avantageuse? S'agit-il plutôt d'un moyen de diffuser l'information? Voilà l'essence de notre intervention de proximité avec le service. Nous espérons améliorer cet aspect pour les universités canadiennes.

M. Tako Van Popta: Évidemment, ces commentaires sur les universités vaudraient aussi pour les entreprises. Pendant que vous parliez, j'ai pensé à la récente question de CanSino, alors qu'il semble qu'une partie de la propriété intellectuelle relative au vaccin contre la COVID-19 soit sortie du pays par la porte arrière au profit d'un autre pays.

J'ai une petite question. C'est une petite question dont je ne connais pas la réponse.

Concernant la cybercriminalité, la meilleure et la plus efficace répartition des risques... Je pense, par exemple, à ma relation avec mon institution bancaire. Pour moi, il est très simple de modifier mon mot de passe. Donc, si on me vole de l'argent de mon compte, c'est moi et non la banque qui devrait en assumer pleinement le risque. Il conviendrait peut-être d'attribuer le risque à la société de logiciels qui fournit cette interface.

Avez-vous un commentaire à faire sur cette répartition des risques?

● (1630)

M. Scott Jones: C'est une question très fondamentale.

Au sujet de la répartition des risques, je pense que les banques sont un excellent exemple. Elles n'ont pas seulement des mesures de cybersécurité, mais elles ont aussi de nombreuses mesures antifraude. Donc, toute activité inhabituelle déclenchera les mesures antifraude. Cela m'a toujours beaucoup impressionné.

Je pense que nous avons tous été victimes, un moment donné, de choses comme le clonage d'une carte de débit, etc. J'espère que ce n'est pas votre cas, mais ma carte a été clonée une fois. Je pense qu'il y a là certains éléments.

Sur la question du risque, il s'agit essentiellement de le minimiser. Quant au transfert du risque, je ne suis pas certain de ce qu'il en est. C'est une question difficile. Je pense, dans ce cas, que la question serait de savoir si vous agissez de façon totalement négligente ou non.

Encore une fois, vaut mieux laisser la question à un avocat, probablement, plutôt qu'à un ingénieur en cybersécurité. C'est une chose pour laquelle...

Le président: Merci, monsieur Van Popta.

En fait, M. Van Popta m'a devancé. C'était la question que je voulais poser. Nous pourrons peut-être y revenir vers la fin, car je pense qu'il s'agit d'un sujet d'actualité.

Cela dit, nous passons à M. Iacono, pour cinq minutes.

[*Français*]

M. Angelo Iacono (Alfred-Pellan, Lib.): Merci, monsieur le président.

Je vous remercie, monsieur Jones, d'être avec nous et de nous informer de ce qui se passe dans le monde de la technologie.

La collecte de données partielles est un sujet de préoccupation de mes concitoyens d'Alfred—Pellan, ainsi que de l'ensemble des Canadiens. L'inquiétude est liée aux cyberattaques et à l'utilisation des données par les entreprises commerciales pour faire de la publicité ciblée. C'est évidemment inacceptable pour un grand nombre de personnes.

Pouvez-vous nous dire comment nous pouvons apprendre aux citoyens à bien protéger leurs données personnelles?

[*Traduction*]

M. Scott Jones: Je vous remercie de la question. Je pense qu'elle est au cœur de certaines questions dont nous avons parlé dans l'*Évaluation des cybermenaces nationales*.

La quantité de données sur chacun de nous dans le cyberespace est assez importante. Il a été souligné que souvent, dans toute cyberattaque, les auteurs n'ont pas seulement des choses comme vos noms d'utilisateur et vos mots de passe qu'ils ont volés ailleurs, mais aussi les réponses à vos questions de sécurité, comme le nom de jeune fille de votre mère, le nom de votre premier animal de compagnie, l'école que vous avez fréquentée, etc. Les choses qui constituaient en quelque sorte une deuxième barrière de sécurité sont maintenant l'équivalent de mots de passe. C'est fondamental.

Pour protéger mes renseignements, je me demande toujours pourquoi quelqu'un en aurait besoin, et même s'il est légal de demander ces informations. Si on me demande mon numéro d'assurance sociale pour un achat en ligne, ce qui n'est pas nécessaire, je laisse faire. Ils doivent commencer à collecter le moins de renseignements possible. Deuxièmement, je pense au risque que je cours. J'achète en ligne, évidemment, et pas seulement en raison de la pandémie, mais aussi parce que c'est pratique. Où l'information va-t-elle? Qui est à l'origine du service? Utilise-t-on un système de paiement d'une tierce partie? Cela peut vous protéger sur le plan financier. Cela dit, en réalité, les cartes de crédit ont de bonnes mesures de protection.

Fondamentalement, la question est de savoir s'ils en ont vraiment besoin. La collecte excessive d'informations est sans contredit un problème que nous suivons de près. Nous avons même pris cela en compte lors de la création du Centre canadien pour la cybersécurité. Nous avons créé une ligne téléphonique pour les gens qui voulaient obtenir de l'aide. Nous nous sommes demandé quels renseignements nous étaient absolument nécessaires pour répondre et aider la personne, puis nous avons fait une évaluation de la protection des renseignements personnels afin de les protéger. Toutes les entreprises devraient se demander si elles ont réellement besoin de savoir tout cela, si elle a vraiment besoin de conserver l'historique d'achats du client. Elles le font peut-être. Il pourrait y avoir des motifs légitimes. Je pense que les commissaires à la protection de la vie privée auraient des conseils à donner à ce sujet.

Du point de vue de la cybersécurité, plus nous diffusons des renseignements et plus nous en diffusons sur nos comptes de médias sociaux, plus nous nous rendons vulnérables. Très franchement, nous leur donnons les renseignements dont ils ont besoin pour nous cibler.

● (1635)

[*Français*]

M. Angelo Iacono: Je vous remercie.

Depuis plusieurs années, nous avons connaissance des activités et des transactions illégales qui ont lieu sur le Web profond. Il y a par exemple, du trafic de drogue, de la prostitution, du trafic d'armes et même des assassinats commandités.

Pouvez-vous nous dire si nous sommes parvenus à mettre en place des moyens afin de réduire ces activités préoccupantes et retracer les criminels en question?

[*Traduction*]

M. Scott Jones: Je pense que les enquêteurs de la GRC, ou peut-être de la Sûreté du Québec, par exemple, seraient sans doute mieux placés pour répondre à des questions sur l'étape de l'enquête.

L'un des risques que nous voyons, c'est que le Web caché aide certainement les cybercriminels et les outils de cybercriminalité. Il existe tout un écosystème où l'on peut dire: « Je veux un outil qui me permettra de faire ceci. » Admettons que vous voulez cibler ce type d'organisation, ou même une organisation précise. Ces gens vous feront des offres et vous diront ce qu'il vous en coûtera. Vous pouvez payer pour une assistance 24 heures sur 24, sept jours sur sept, ou pour un outil personnalisé qui sera conçu pour vous permettre d'atteindre vos objectifs.

Le crime organisé est derrière toutes ces activités. C'est une grande entreprise. Elle est facilitée par le Web caché et les systèmes de paiement anonymes comme Bitcoin et les devises en ligne. L'un des principaux défis, c'est que l'ensemble du système est conçu de manière à être anonyme et à ne pas avoir d'attribution.

[*Français*]

M. Angelo Iacono: D'accord

En ce qui concerne spécifiquement les outils de cyberattaque, étant donné qu'il s'agit de matériaux technologiques perfectionnés, il est raisonnable de penser que leur fabrication n'est pas à portée de la main.

Êtes-vous en mesure de nous dire, aujourd'hui, qui sont ces fabricants? Sommes-nous en mesure de les empêcher de vendre le matériel sur le sol canadien? Plus important encore, sommes-nous capables de saisir tout ce qui existe sur le marché qui peut venir nous faire mal?

[*Traduction*]

Le président: Malheureusement, M. Iacono a dépassé ses cinq minutes. C'est une question importante. Vous pourrez peut-être y revenir dans une autre réponse.

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

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup, monsieur le président.

Merci, monsieur Jones. C'est très instructif. C'est certainement un sujet important, surtout dans les circonstances dans lesquelles nous sommes avec la COVID. J'espère pouvoir répondre à quelques questions.

Y a-t-il des domaines où le Canada est plus à risque, ou plus vulnérable, en raison de l'évolution de l'utilisation d'Internet depuis le début de la pandémie de COVID-19 et de l'explosion de la capacité en ligne requise pour faire face à la pandémie?

M. Scott Jones: Il y a quelques domaines où nous dirions que nous devons faire preuve d'une grande prudence à l'égard des risques accrus. Le fait que nous sommes très nombreux à travailler de la maison a changé notre environnement technologique. Nous travaillons principalement en dehors du périmètre de notre organisation, si bien qu'en ce qui a trait à de nombreux mécanismes de défense sur lesquels nous comptions, de nombreux Canadiens travaillent maintenant de la maison et se connectent directement à Internet.

Il existe des moyens pour essayer de minimiser et d'atténuer ces risques. Ce sont certaines des mesures que nous avons publiées, mais c'est probablement l'un des plus grands risques: le fait que nous sommes maintenant en dehors du périmètre de défense qui a été mis en place. Dans certains cas, nous ne le sommes pas. Par exemple, je ne quitte jamais notre périmètre de défense en raison de la façon dont nous avons mis en place notre accès à distance. Nous l'avons conçu pour qu'il fonctionne à distance afin que je puisse travailler de la maison et être protégé par notre ensemble complet de cyberdéfenses. C'est le cas pour la majorité des employés du gouvernement.

Pour beaucoup d'organisations, cependant, nous les encourageons entre autres à s'assurer d'avoir un mécanisme similaire à celui que nous avons pour le gouvernement ou d'y ajouter d'autres défenses existantes.

Ce serait l'un des principaux risques, mais il y a aussi que nous conservons davantage de données à la maison, et nous tenons des conversations comme celle-ci, bien que ce soit une tribune publique ici. Il y a des secteurs comme celui-ci où nous devons simplement être conscients de ce que nous faisons.

M. Damien Kurek: Merci beaucoup de ces remarques.

De toute évidence, les infrastructures en santé sont au premier plan des préoccupations de tout le monde avec la pandémie de COVID qui sévit depuis une dizaine de mois. Avons-nous constaté une hausse des menaces qui pèsent sur notre système de soins de santé?

Comment votre organisation peut-elle contribuer à veiller à ce que les renseignements ne soient pas uniquement communiqués au gouvernement fédéral, mais qu'ils soient également acheminés sur le terrain dans les hôpitaux locaux, dans les cliniques locales et aux médecins qui travaillent à domicile — et, dans bien des cas, les Canadiens qui sont en vidéoconférence avec leur médecin —, tout en assurant la protection de l'ensemble du système?

● (1640)

M. Scott Jones: Cette question touche en quelque sorte l'essence même de ce que nous faisons. L'objectif est de ne pas laisser ces renseignements au sein du gouvernement fédéral, mais de les transmettre à d'autres. Je l'ai déjà mentionné lorsque j'ai parlé de notre appel hebdomadaire avec le secteur de la santé. Cela inclut nos collègues provinciaux et territoriaux, mais aussi toutes les organisations qui viennent à la table. Le nombre augmente chaque semaine à mesure que de plus en plus de personnes s'inscrivent, et nous sommes heureux de passer en revue ce que nous voyons sur la cybersécurité, y compris les conseils et les directives.

Mais en général, quand nous voyons aussi... C'est là où nous avons un effet de levier par rapport à ce que notre mandat en matière de renseignement étranger peut nous dire sur le ciblage. Nous nous sommes adressés à des organisations précises où nous voyons des situations, et nous leur avons donné des conseils sur mesure parce que c'est un système important pour le gouvernement. En réalité, il s'agit de mettre ces renseignements entre les mains de quelqu'un... notre objectif est de les obtenir avant que les gens deviennent des victimes afin qu'ils puissent prendre des mesures proactives pour se protéger. C'est ce que nous faisons chaque semaine, et nous le faisons systématiquement.

Ensuite, bien entendu, nous publions un certain nombre de mises en garde et d'avis qui sont transmis aux secteurs. Nous avons publié l'évaluation des menaces pour le secteur de la santé, et nous l'avons rendue publique. Nous l'avons également envoyée à l'avance au secteur de la santé pour lui faire savoir ce que nous allions dire sur les questions dont il devait être au courant. Notre objectif est d'encourager les gens à échanger les pratiques exemplaires au sein du secteur...

M. Damien Kurek: Je m'excuse. Il me reste environ une minute, et j'espère pouvoir poser une dernière question. Je ne veux pas vous couper la parole.

Nous sommes dans ce qui est considéré comme étant une « infodémie ». Il y a des tonnes de renseignements, beaucoup de désinformation, puis il y a énormément d'éléments d'information quelque part au milieu, et je pense que c'est ce qui rend les théories du complot crédibles, car il y a toujours une petite part de vérité dans tout.

Plus précisément, en ce qui concerne l'intégrité de la démocratie canadienne, je voudrais vous demander de commenter les menaces qui pèsent sur la démocratie canadienne, les élections ou toute infrastructure connexe.

M. Scott Jones: C'est énorme.

Nous parlons vraiment de certaines des choses que nous avons mises en évidence dans notre premier et deuxième rapports, *Cybermenaces contre le processus démocratique canadien*, que nous avons publiés afin de faire ressortir certains de ces éléments d'information. Cela demeure un problème.

Maintenant, je pense que la réponse n'est pas forcément une réponse en matière de cybersécurité. Vous verrez qu'Élections Canada intervient à propos de la désinformation. Vous êtes confrontés à ce problème en tant que députés et candidats à un moment donné, entre autres choses, et la façon de lutter contre... C'est l'un de ces secteurs où, du point de vue de la cybersécurité, nous sommes très limités dans ce que nous pouvons faire, parce que ce ne sont que des renseignements erronés qui sont affichés quelque part, bien franchement, et nous ne sommes pas les détenteurs ultimes de la vérité.

C'est toutefois un sujet où nous nous demandons toujours, dans un premier temps, comment nous pouvons renforcer notre cybersécurité. Le but du rapport en soi était de démystifier certaines des menaces et certaines des faussetés pouvant être diffusées et de soutenir que ce n'est pas ainsi que les démocraties fonctionnent. On ne peut pas aller en ligne et simplement changer le résultat du vote, car des procédures sont en place, etc.

Le président: Nous allons devoir en rester là, malgré les nombreux efforts déployés au sud de la frontière pour modifier le résultat du vote.

Madame Damoff, vous avez cinq minutes, s'il vous plaît.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Merci, monsieur le président.

C'est merveilleux de vous avoir ici, monsieur Jones.

Merci de votre travail et de votre rapport. C'est très utile. Vous le présentez de manière à ce que les Canadiens puissent le comprendre. Une grande partie de ce document dépasse de loin nos connaissances. Il est important de le simplifier pour que nous sachions de quoi nous parlons.

En 2018, vous disiez être « convaincu que des mesures de protection suffisantes existent pour faire face aux risques de piratage ou d'espionnage des télécommunications par la Chine », mais vous reconnaissez que le risque pourrait augmenter avec l'introduction de la technologie 5G.

Cette semaine, le Citizen Lab a publié un rapport. Je ne sais pas si vous l'avez vu, mais il fait état que la stratégie en matière de technologie 5G du Canada ne devrait pas « être conçue pour résoudre un problème qui vise Huawei », mais elle devrait régler un problème lié à la technologie 5G « pour assurer la résilience, la sécurité ».

Je me demande si vous pouvez nous en dire un peu plus à ce sujet et sur le type de stratégie que nous devrions envisager à mesure que nous avançons et que les entreprises passent à la technologie 5G.

M. Scott Jones: Je vais devoir être prudent car la décision politique n'a pas encore été prise.

En général, ce que nous constatons lorsque nous examinons un système qui s'apparente un tant soit peu à un réseau 5G, c'est que le système doit être sécurisé en plusieurs couches, depuis sa maintenance à ceux qui y ont accès, en passant par la variété de l'équipement. Il y a aussi la question de savoir si le logiciel utilisé est en libre accès, s'il peut être soumis à l'examen du public ou s'il est en circuit fermé, ce qui signifie qu'il provient d'un fournisseur particulier, et il y a également la façon dont nous tirons parti du logiciel. C'est l'un des aspects où les télécommunications modernes offrent un avantage considérable à l'heure actuelle.

Nous comptions sur le réseau pour la sécurité et la façon dont vous transmettiez les données, car le chiffrement ne pouvait pas être utilisé. C'était trop cher. Nos appareils n'étaient pas assez rapides pour le faire. C'est un défi, dans le contexte de l'application de la loi.

Le chiffrement offre une protection des renseignements personnels que vous transmettez. C'est difficile à observer. Le chiffrement est maintenant de plus en plus activé par défaut sur nos appareils. Tous les sites Web du gouvernement du Canada exigent qu'ils soient chiffrés. Le chiffrement protège la confidentialité et la capacité de savoir ce que je dis ou ce qui se passe.

Le deuxième aspect est l'intégrité, sachant que lorsque j'envoie un message, personne ne le modifie. C'est l'un des domaines où nous devons réfléchir du début à la fin. Par exemple, si la ville facilite l'arrivée d'une ambulance à l'hôpital et qu'elle change les feux de circulation, vous voulez vous assurer qu'elle ne les change pas systématiquement au vert, là où des piétons vont traverser, notamment. C'est l'intégrité du message, c'est-à-dire que le message que vous voulez envoyer arrive exactement comme prévu. On utilise le chiffrement pour cela. On ne se soucie pas vraiment de savoir si quelqu'un voit le message; on se soucie seulement qu'il ne peut pas le modifier.

Il y a ensuite la disponibilité: nous avons besoin que les réseaux soient là. C'est là où nous envisageons vraiment une stratégie solide, qui consiste à faire en sorte que les fournisseurs construisent de meilleurs équipements et de meilleurs logiciels. Comment le réseau est-il testé? Il est de portée internationale pour s'assurer qu'il réponde aux normes minimales, mais il y a aussi de nombreux fournisseurs. Nous voulons une stratégie qui inclut de nombreux fournisseurs. Nous voulons une diversité sur le marché. Nous voulons ces éléments dans chaque section, quel que soit le type de réseau ou le type d'équipement. C'est toujours préférable que d'avoir un monopole.

Nous voulons vraiment tirer parti de toutes ces choses. C'est là où, je pense, le rapport du Citizen Lab voulait en venir. Il a fait valoir qu'il y a de multiples facettes. Il n'y a pas de solution unique au défi auquel nous sommes confrontés; on doit appliquer de multiples aspects différents de la sécurité. C'est certainement ce que nous essayons d'intégrer dans tout programme de sécurité que nous mettons en place. Ce n'est pas propre au réseau mobile de nouvelle génération par rapport à un réseau fixe ou à tout ce qui est... Par exemple, nous utilisons le même modèle de sécurité pour le réseau incroyablement rapide que j'ai chez moi en ce moment.

● (1645)

Mme Pam Damoff: Je serai brève car il ne me reste qu'une minute.

Les Canadiens avaient exprimé des inquiétudes concernant l'application Alerte COVID et la divulgation de leurs renseignements personnels, ce qui n'est pas le cas, nous le savons. Pourtant, ces mêmes personnes téléchargent une photo d'elles-mêmes sur une application qui vieillit automatiquement leur visage, sans même penser que toutes ces données sont destinées à une société russe. Comment surmonter cela? On le voit tout le temps sur les médias sociaux, où les gens donnent accès à des photos et à des renseignements personnels. On communique des renseignements personnels qui finissent par être utilisés pour des questions de sécurité, et on y répond ouvertement sur Facebook. Comment éduquer les Canadiens à ce sujet?

M. Scott Jones: C'est certainement un défi, et j'aimerais avoir une réponse à cette question. C'est certainement l'un des défis que nous devons relever.

L'application Alerte COVID a été une expérience frustrante en raison de cette préoccupation précise. De mon point de vue, l'application a été conçue en accès libre. Nous l'avons testée avec des fournisseurs commerciaux pour nous assurer que nous avions fait tout ce que nous pouvions pour tester les vulnérabilités ou simplement les erreurs de codage. Elle était en accès libre. Les commissaires à la protection de la vie privée l'ont examinée, mais le problème persiste. On dit simplement, « Eh bien, c'est le gouvernement ».

J'ai vu un dessin animé. Il se déroulait dans les années 1950. On pouvait y lire: « Je ne peux pas parler; le gouvernement pourrait écouter au téléphone. » Et maintenant, on dit, « Hé, dispositif d'écoute », qui est l'un de ces haut-parleurs que nous avons à la maison, « Dites-moi ce que je fais ». C'est cette dichotomie qui existe, où les gens sont...

J'aimerais avoir une excellente réponse.

Le président: Qui savait que Siri existait dans les années 1950?

Madame Michaud, vous disposez de deux minutes et demie, s'il vous plaît.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Je remercie ma collègue Mme Damoff de son intéressante question. D'ailleurs, la réponse était tout aussi intéressante.

Je m'intéresse particulièrement au groupe de travail qui avait été créé et auquel le Centre a participé pour protéger les élections fédérales de 2019 contre l'ingérence étrangère, particulièrement avec des élections qui pourraient arriver plus tôt que prévu. C'est inquiétant.

Je ne peux pas m'empêcher de penser à tout ce qu'on a vu à la télévision, par exemple *The Great Hack* et *The Social Dilemma*. Je ne sais pas si mes collègues les ont vus, mais il y a certainement quelque chose d'inquiétant là-dedans.

Quelles mesures spécifiques sont ressorties de ce groupe de travail pour contrer les campagnes de désinformation ou l'ingérence étrangère dans les élections fédérales ou provinciales?

Y a-t-il des mesures précises ou des recommandations qui ont été émises par ce groupe de travail?

● (1650)

[*Traduction*]

M. Scott Jones: Je vais supposer que vous parlez du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections que le CST a présidé au nom de la communauté.

Nous prenons quelques initiatives. Nous avons travaillé avec Élections Canada pour les soutenir globalement en matière de cybersécurité. Je pourrais entrer dans les détails, mais le directeur général des élections et son équipe pourraient le faire aussi.

L'un des aspects pour nous était également de nous assurer que chaque parti politique enregistré qui le souhaitait puisse bénéficier de séances d'information régulières sur la cybersécurité. Mon équipe l'a fait de manière continue tout au long de la campagne pour veiller à ce que nous communiquions toutes les cybermenaces que nous voyions. Nous avons également mis en contexte ce qui était vraiment important et ce qu'ils pouvaient s'attendre à voir. Cela a été fait avec les responsables du parti.

Nous avons également mis en place une ligne téléphonique où les partis politiques pouvaient appeler s'ils avaient besoin d'aide avec un problème, comme de faux comptes sur les médias sociaux, etc. La plupart des fournisseurs de médias sociaux étaient assez réceptifs à ce genre de choses. Nous tentions de faire en sorte que des connexions soient établies.

Cela demeure un défi. C'est l'un des domaines dans lesquels nous cherchons toujours des moyens de nous connecter.

Par ailleurs, l'une des choses qui m'ont été répétées à maintes reprises est que si, par exemple, quelqu'un usurpe votre identité sur les médias sociaux, je ne peux pas déposer une plainte en votre nom. Vous devez le faire. Les entreprises de médias sociaux sont très catégoriques à ce sujet. C'est l'un des domaines où, si quelque chose comme cela se produit, nous essayons de faciliter et, espérons-le, d'accélérer l'obtention d'une résolution. Nous avons vu des incidents de ce genre où les parties ont demandé un certain soutien.

Puis, bien sûr, dans les rapports — le premier et le deuxième —, ont fait mention des menaces qui pèsent sur les processus démocratiques du Canada, où nous essayons vraiment de jeter les bases pour les cybermenaces que nous nous attendons voir peser sur les institutions démocratiques du Canada.

[*Français*]

Le président: Merci, madame Michaud.

[*Traduction*]

Monsieur Harris, vous avez deux minutes et demie.

M. Jack Harris: Merci, monsieur le président.

Monsieur Jones, pourriez-vous nous expliquer quelle est la différence entre la cyberdéfense et la cybersécurité?

Nous savons que votre agence relève du ministre de la Défense. D'après mes souvenirs en tant que porte-parole en matière de défense, je ne pense pas que vous faites partie du ministère. L'armée, bien sûr, doit protéger sa propre infrastructure, son équipement, ses communications et tout le reste.

Votre agence participe-t-elle d'une manière ou d'une autre à la planification de la défense? Vous avez parlé d'exercices de simulation avec les gens du réseau électrique. Participez-vous à ce genre d'exercices avec les militaires en matière de planification de la défense ou de planification de scénarios pour les activités militaires?

M. Scott Jones: Nous faisons partie du ministère de la Défense et nous relevons du ministre. Nous rendons compte au ministre, mais nous sommes une agence distincte rattachée au ministère de la Défense. J'ai failli revenir sept ans en arrière pendant une seconde.

Avec la « cyberdéfense », nous parlons vraiment des cas où nous prenons des mesures actives pour prévenir un incident de cybersécurité. Nous faisons un blocage. Nous sommes les cyberdéfenseurs du gouvernement du Canada. Nous prenons plus de deux milliards de mesures par jour, en plus des mesures que fournissent les outils commerciaux, pour protéger le gouvernement du Canada. Notre programme comporte un volet de cyberdéfense.

« Cybersécurité » est le terme générique que nous utilisons. C'est aussi une question de mesures proactives. Il ne s'agit pas seulement d'agir au point de compromis, mais de construire les défenses et de les renforcer pour qu'elles soient sûres dès le départ. C'est la sécurité intégrée à la conception. C'est vraiment, dans mon esprit, ce qui différencie la cybersécurité de la cyberdéfense. La cyberdéfense concerne en fait les mesures de protection que vous prenez.

En ce qui concerne notre travail avec le ministère de la Défense, il est évident que celui-ci est responsable de la défense de ses systèmes. Ce sont les experts en matière d'équipement militaire, mais nous fournissons un certain nombre de services. L'un d'eux est la cartographie et les systèmes de cryptage qu'ils utilisent pour protéger toutes les opérations des Forces canadiennes. Nous travaillons avec eux à ce genre de choses depuis 70 ans. Bien sûr, nous collaborons avec la Défense pour toute activité de planification d'exercices.

Nous le ferions également avec toute autre organisation pour dire comment nous réagissons à tout incident de cybersécurité. Nous recherchons vraiment les possibilités de hausser la barre de manière proactive. Nous le ferions dans le cadre de notre mandat.

Le président: Merci, monsieur Harris.

Je suis désolé de vous avoir interrompu, monsieur Jones. Voulez-vous finir votre phrase?

M. Scott Jones: Oui, je veux juste dire enfin qu'une partie de la Loi sur le CST vise les cyberopérations défensives et les cyberopérations étrangères, la possibilité de réagir lorsque le Canada est menacé, et la possibilité de dire, avec l'autorisation ou la reconnaissance du ministre des Affaires étrangères et du ministre de la Défense, que nous devons prendre des mesures à l'étranger pour protéger le Canada également. Cela fait partie de la Loi sur le CST que le Parlement a adoptée.

● (1655)

Le président: Merci, monsieur Harris.

Précédemment, dans votre réponse, je pensais que vous aviez dit qu'il y avait à peu près deux milliards d'attaques par jour.

M. Scott Jones: Nous prenons deux milliards de mesures par jour pour prévenir certaines activités malveillantes, dont certaines consistent à analyser le gouvernement pour trouver des vulnérabilités, et d'autres sont des logiciels malveillants qui tentent de se faire télécharger.

Le président: Vraiment? Il me semble que cela fait beaucoup d'attaques.

M. Scott Jones: Eh bien, dans certains cas, il s'agit d'un balayage en masse. C'est comme si quelqu'un se rend sur tous les ordinateurs du gouvernement comme il le ferait avec un bâtiment dont il essayerait toutes les portes et les fenêtres pour voir si rien n'est resté déverrouillé. Nous mettons donc un frein à cela. Si vous ne pouvez pas voir nos vulnérabilités, vous ne pouvez pas les exploiter.

Le président: D'accord. Merci.

Monsieur Kurek, c'est à vous pour six minutes.

M. Damien Kurek: Merci beaucoup, monsieur le président.

Ce sujet a fait l'objet d'un certain débat dans les milieux politiques canadiens, récemment, dans le sillage d'un éditorial assez explosif du New York Times concernant MindGeek et les vidéos abusives du site Pornhub, entre autres. Je me demande simplement si vous avez des commentaires sur ce qui peut être fait pour les victimes de certains de ces crimes terribles, comme la pornographie juvénile ou le viol. J'aimerais entendre les solutions pratiques, les recommandations que vous auriez pour qu'on puisse éliminer ce fléau.

M. Scott Jones: C'est une question troublante juste à cause du contenu, mais c'est aussi une question de fond. Je pense que la réponse plus générale, la meilleure position, viendrait de mes collègues de Sécurité publique Canada qui examinent vraiment l'aspect des préjudices en ligne afin de trouver des moyens de les atténuer.

Certains des éléments de la cybersécurité — les techniques et les outils — sur lesquels nous mettons l'accent visent à empêcher les gens de se retrouver dans des situations où ils pourraient être exploités de cette manière ou à empêcher leurs enfants d'être exploités de cette manière. C'est l'un des grands défis à relever.

Mais je pense que l'un des autres aspects qui posent un grand défi est que ces plateformes sont conçues pour être accessibles dans de nombreux cas. Comme le dit un des mèmes célèbres d'Internet, toujours du *New York Times*, « Sur Internet, personne ne sait que tu es un chien ». Comme les gens sont tellement anonymes, vous n'avez aucune idée de la personne qui se cache derrière. C'est l'une des choses qui font du tort en ligne. Comment concilier cette réalité avec la question de savoir qui interagit avec les enfants, ou qui interagit avec moi en ligne, etc. Vous pouvez être anonyme, et cela facilite beaucoup de choses. Mais la réponse plus générale à certaines de ces questions devrait probablement venir de Sécurité publique Canada. Du point de vue de la cybersécurité, nous pouvons continuer de donner des conseils et, nous l'espérons, d'aider les gens à assurer la sécurité de leurs enfants et leur propre sécurité en ligne.

M. Damien Kurek: Je comprends. Il y a bien sûr la prévention, puis la question de la cybercriminalité et tout un tas d'autres aspects qui doivent être abordés.

L'une des préoccupations — et cela revient à la discussion sur l'information et la désinformation — concerne les éditoriaux et les publireportages dirigés par des États étrangers, et la menace ou l'influence de groupes culturels ou autres, au Canada, avec des acteurs d'États étrangers qui se servent d'une présence en ligne pour essayer d'exercer une influence directe au Canada. Je me demande si vous pouvez nous parler de cela et de tout ce qui pourrait être fait pour garantir l'intégrité sur ce plan.

M. Scott Jones: J'aimerais vraiment que mes collègues du Service canadien du renseignement de sécurité soient là pour vous répondre. Dans l'univers de la cybersécurité, notre défi est vraiment d'essayer d'informer les gens, par l'intermédiaire d'une évaluation nationale de la cybermenace, et de dire: « recherchez les faits ». L'Internet est conçu pour être ouvert et libre et pour permettre ce type de communication. De notre point de vue, en tant qu'agence de cybersécurité, le conseil que nous avons est vraiment de faire preuve de vigilance et de ne pas se fier uniquement à ce que l'on trouve en ligne. D'un autre côté, je pense que Sécurité publique Canada est probablement mieux placée pour parler de certaines des mesures qui peuvent être prises. À mon avis, il semble que ce soit un trafic Internet légitime et c'est le cas. Je ne cherche pas à le légitimer, mais j'essaie de dire qu'il ne semble pas s'agir d'une cyberactivité malveillante. Ce n'est pas un logiciel malveillant ou quelque autre activité comme celle qui consiste à exploiter les aspects techniques de la cybersécurité.

● (1700)

M. Damien Kurek: C'est juste.

Enfin, nous parlons beaucoup du nuage et de la façon dont il offre un certain niveau de sécurité qui n'aurait pas été accessible auparavant parce qu'il n'est pas nécessaire d'avoir des serveurs, une porte à verrouiller et les différentes couches de cybersécurité pour garantir la sécurité. Avec le nuage, c'est évidemment la responsabilité de quelqu'un d'autre. L'un des défis supplémentaires que cela représente est que vous avez un système énorme qui contient une quantité incroyable de données. Bien qu'il y ait un niveau de sécurité plus élevé, il y a des risques associés à cette situation à une échelle beaucoup plus grande, bien qu'il soit beaucoup plus difficile de s'y infiltrer.

Je me demande si vous pouvez nous dire comment ces risques sont atténués, car cela touche particulièrement les petites et moyennes entreprises qui achètent une option de stockage dans le nuage pour 20 $ ou 50 $ par mois, ce qui leur donne accès aux services. Cependant, les problèmes d'échelle existent également dans ce domaine.

Le président: Malheureusement, M. Kurek a largement dépassé le temps qui lui était accordé. Si vous pouvez intégrer votre réponse d'une autre manière...

Madame Lambropoulos, êtes-vous prête pour les cinq minutes dont vous disposez?

Mme Emmanuella Lambropoulos (Saint-Laurent, Lib.): Oui. Merci, monsieur le président.

[*Français*]

Je vous remercie beaucoup, monsieur Jones, d'être avec nous et de répondre à nos questions.

J'ai deux questions à vous poser.

Compte tenu de tous les accords commerciaux que nous avons signés au cours des cinq dernières années, de plus en plus d'entreprises canadiennes font des affaires sur des marchés mondiaux, comme vous le savez. C'est excellent pour l'économie canadienne, en plus d'être pratique et avantageux pour les entreprises.

Dans l'évaluation des cybermenaces nationales, vous avez indiqué que la menace de l'espionnage en ligne est certainement beaucoup plus élevée pour les entreprises canadiennes qui font des affaires à l'étranger ou qui travaillent directement avec des sociétés détenues par des États étrangers.

Vous avez déjà abordé le sujet et vous avez donné des suggestions quant à la façon dont les Canadiens, les Canadiennes et les entreprises peuvent se protéger. J'aimerais savoir si vous avez des conseils à donner aux entreprises qui sont en lien direct avec des acteurs qui sont possiblement parrainés par des États étrangers pouvant menacer la cybersécurité.

[*Traduction*]

M. Scott Jones: Excellent. Je vous remercie de cette question. Il y a des risques, et cela dépend du pays que nous examinons. Rappelez-vous en particulier que nous avons parlé des entreprises d'État et des partenariats avec celles-ci.

Dans ce domaine, en fonction de l'entreprise canadienne, il est possible d'obtenir de nombreux conseils. Il s'agit de comprendre quel est l'objectif de l'accord de partenariat. Est-ce un accord de transfert de technologie qui vise vraiment à transférer la technologie pour construire, ou bien un accord de fabrication qui vise à externaliser quelque chose?

Savoir ce qui est important pour vous en tant qu'entreprise est la première étape. Qu'est-ce qui distingue mes renseignements des autres? S'agit-il de propriété intellectuelle, d'un procédé de fabrication unique, de la conception d'une technique d'outillage, ou bien de ma clientèle et de la façon dont j'interagis avec elle, dont je fais la promotion et ainsi de suite? En sachant ce qui vous rend spécial et unique, vous savez ce que vous devez protéger — c'est l'objectif que vous devez protéger.

Ensuite, vous gardez les yeux grands ouverts. Qu'est-ce qui m'intéresse? S'agit-il d'une relation mutuellement bénéfique? Lorsque vous commencez à évaluer cette relation, elle vous dicte où vous devez placer vos cyberdéfenses, ce qui, en fin de compte, aboutit à ce dont je suis responsable. Positionnez-vous votre entreprise en vue d'une prise de contrôle? Dans ce cas, vous pouvez vous attendre à ce qu'une entreprise cherche à obtenir des renseignements sur vos finances. Quelles sont vos principales vulnérabilités, qui sont vos fournisseurs, qui est votre conseiller juridique, etc.? Vous pourriez voir cela comme une offre publique d'achat.

S'il est question d'une technologie unique, vous devez la protéger. Comment puis-je la protéger et m'assurer qu'elle ne se répand pas et qu'elle ne m'échappe pas? Réfléchissez vraiment à cela. Vous réfléchissez aux menaces et ensuite vous tirez parti des conseils qui existent.

Mme Emmanuella Lambropoulos: Parfait. Merci beaucoup.

Dans un autre ordre d'idées, j'aimerais remercier mon collègue, M. Kurek, d'avoir évoqué MindGeek, qui se trouve à environ 15 minutes de route de chez moi. Cela me touche de près, ce qui se passe et le fait que ces vidéos soient publiées depuis un endroit si proche de chez moi.

Quelles recommandations feriez-vous au gouvernement du Canada pour garantir que les enfants ne sont pas exploités comme ils le sont déjà? Je sais que vous avez dit que la Sécurité publique travaille déjà à ce dossier, mais pouvez-vous nous donner un aperçu de ce qui peut être fait et de ce que le gouvernement peut exiger?

● (1705)

M. Scott Jones: Je pense que le défi auquel je suis confronté concerne en fait la cybersécurité. Je recommanderais surtout aux victimes potentielles des moyens de protéger les choses, de se protéger elles-mêmes et d'essayer de ne pas se retrouver dans une telle situation, et de vraiment réfléchir avant de fournir de l'information. Une fois que l'information est sur Internet, elle y est pour toujours. Comment partagez-vous cette information? Quelles sont les applications que vous utilisez? On a donné l'exemple des applications qui utilisent une photo du visage pour estimer l'âge d'une personne, mais il y a aussi le partage de photos, et la nécessité de ne pas se mettre dans une position où l'on est vulnérable à ce type de préjudice.

Il s'agirait ensuite d'amener les Canadiens à réfléchir à la manière dont ils utilisent la base technologique et à se demander s'ils comprennent vraiment les préjudices qu'ils peuvent s'infliger en étant peu à peu happés par tout cela. Il faut alors minimiser les dommages et les gérer.

Je ne suis tout simplement pas bien placé pour parler des différents outils, parce que cela ne fait pas partie de ce que nous ferions du point de vue de la cybersécurité.

En tant que citoyen, j'aimerais bien sûr que cette question soit réglée avec fermeté et rapidité, mais nous ne sommes pas en mesure de vraiment en parler du point de vue de la cybersécurité.

Le président: Merci, madame Lambropoulos.

Nous avons effectué trois tours, chers collègues. Il nous reste encore 20 minutes. Je crois que les conservateurs veulent que Mme Stubbs soit la prochaine à prendre la parole, mais avant d'en arriver à ce tour, j'ai quelques questions à poser. Les libéraux pourraient indiquer au greffier le nom de la personne qu'ils souhaitent voir intervenir. Je propose cinq minutes pour les conservateurs et les libéraux et deux minutes et demie pour le NPD et le Bloc, ce qui nous laisserait encore cinq minutes, dont deux minutes pour les libéraux et deux pour les conservateurs. Veuillez m'indiquer les personnes que vous souhaitez désigner pour poser les questions.

Je voudrais revenir sur la question de M. Van Popta concernant la répartition des risques.

Il y a deux ans, les représentants de Desjardins sont venus nous parler d'une fuite de données attribuable à un employé qu'ils ont qualifié de « malveillant ». Ce que je n'ai pas compris, c'est comment un client de Desjardins peut courir un risque important de voir ses données se retrouver sur le Web invisible sans que Desjardins soit apparemment responsable d'un quelconque préjudice qui pourrait arriver à l'un de ses clients. Je me demande simplement si cela a fait l'objet de discussions dans le contexte de votre centre de cybersécurité et, dans l'affirmative, la direction que ces discussions prennent selon vous.

M. Scott Jones: C'est une question intéressante.

Je pense que nous devons faire face au fait qu'une menace d'initié, qui est vraiment ce dont nous parlons, comporte différentes facettes. La première est que la personne se trouve dans une position de confiance et qu'elle a accès à certains types de données et de renseignements, surtout si cet accès est lié à sa fonction. Quels sont alors les contrôles mis en place du point de vue de la sécurité de l'information? Il s'agit de comprendre un des éléments de nos dix priorités, à savoir segmenter et séparer l'information.

Il y a des choses au CST que je n'ai tout simplement pas besoin de savoir. Oui, je suis l'un des cadres supérieurs, mais cela ne veut pas dire que je dois tout savoir. Je n'ai pas accès aux dossiers de sécurité pour les habilitations de sécurité. Je n'ai pas besoin de savoir; je n'ai pas besoin d'y accéder. Nous segmentons l'information et nous la protégeons. C'est pour des raisons de protection de la vie privée, mais aussi pour des raisons de sécurité.

Même au centre pour la cybersécurité, il y a des choses pour lesquelles un groupe limité de personnes est exposé à certains renseignements. Nous le faisons délibérément pour en assurer la protection.

Ce sont là certains des éléments de cybersécurité qui, selon nous, font partie de nos conseils et orientations en général, mais vous devez d'abord savoir ce qui doit être protégé. C'est l'un des éléments, ainsi que ce contre quoi cette information pourrait être utilisée. Souvent, ce que je dis aux entreprises, c'est de ne pas penser au préjudice qu'elles pourraient subir, mais plutôt au préjudice que quelqu'un pourrait leur causer avec leur propre information. À qui cette information pourrait-elle être donnée et ainsi vous causer du tort?

Le président: Monsieur Jones, la responsabilité ne devrait-elle pas incomber à l'institution financière? L'institution financière dispose de beaucoup plus de ressources pour me protéger que j'en ai pour me protéger moi-même. Ce que je ne comprends pas, c'est pourquoi la responsabilité ne devrait pas incomber au fournisseur de services financiers.

M. Scott Jones: Je crains que cette question ne m'amène en terrain juridique, et je ne suis absolument pas qualifié pour cela.

Le président: Eh bien, je vous invitais ni plus ni moins à vous jeter du haut de la falaise…

Des voix: Ha, ha!

Le président: ... mais c'est quelque chose qui m'irrite depuis un bon moment déjà.

Ma deuxième question porte sur les mots de passe, et vous avez raison de plaider pour les mots de passe. Ce que je ne comprends pas, c'est pourquoi tous les Canadiens, lorsqu'ils accèdent à leurs comptes bancaires, ne disposent pas simplement d'une technologie de reconnaissance faciale. N'est-ce pas le moyen de protection ultime pour les mots de passe?

● (1710)

M. Scott Jones: C'est une excellente question, car c'est un enjeu récurrent au gouvernement. Tout se résume à l'accessibilité. Est-ce que chaque Canadien possède la technologie nécessaire pour avoir accès à la reconnaissance faciale?

Ce n'est pas infaillible. La technologie fait partie des facteurs. Nous disons toujours qu'il y en a trois. Le premier se rapporte à une chose que vous connaissez, et un mot de passe correspond à cette définition. Le deuxième est quelque chose qui vous est propre, comme la reconnaissance faciale, ou même d'une empreinte digitale. Enfin, le troisième facteur touche une chose que vous possédez.

Quand j'entre dans l'édifice du Centre de la sécurité des télécommunications, je me dis toujours que la chose que je connais est mon code d'identification qui me permet d'entrer; la chose que je possède est mon badge; et la chose qui m'est propre est ma photo et mon visage que nos gardiens de sécurité vérifient lorsque je traverse les différentes portes. Ce sont là des exemples de ces facteurs dans le monde réel.

Ce serait donc un facteur de plus. Les mots de passe sont une chose que vous connaissez. Des jetons matériels pourraient être une chose que vous possédez, mais il s'agit là encore d'une question d'accessibilité. Il faut vraiment trouver l'équilibre. Il y aurait un facteur d'authentification de plus, et il est important…

Le président: Dans l'échelle de la sécurité, j'ose croire qu'utiliser la technologie de reconnaissance faciale ou d'empreinte digitale est beaucoup plus sécuritaire que de se souvenir si son mot de passe est « 123 » ou « 321 ».

M. Scott Jones: Tout à fait. C'est un obstacle beaucoup plus important à franchir que si vous avez un mot de passe simple et facile à deviner et que vous le réutilisez.

Le président: Bien.

Pour ma dernière question — je mets vraiment la patience de mes collègues à rude épreuve, mais peu importe —...

Des voix: Ah, ah!

Le président: ... je citerai l'exemple d'un de mes amis qui a fait une remarque à propos de plusieurs des pays que vous avez nommés. Il a une crainte légitime des menaces, qu'elles soient cybernétiques ou autres. Il est membre d'une diaspora.

Lorsqu'il a signalé une menace au service de police local, on lui a répondu que c'était à la GRC de s'en occuper. Lorsqu'il s'est ensuite adressé à la GRC, on lui a dit que l'affaire relevait plutôt du Service canadien du renseignement de sécurité. Et quand il a enfin essayé de s'adresser au SCRS, on lui a répondu par un silence total.

Je pense qu'une des raisons pour lesquelles les membres d'une diaspora ne signalent pas toutes les menaces, c'est qu'il n'existe pas de mécanisme clair à cette fin. Avez-vous des conseils à donner à mon ami, ou aux Canadiens en général qui reçoivent des menaces de la part d'acteurs d'États étrangers, tant sur le plan cybernétique qu'en personne?

M. Scott Jones: Je vais devoir m'en tenir au conseil sur le plan cybernétique, qui est notre expertise.

Tout d'abord, si vous voyez une chose, que ce soit un message texte ou un courriel qui semble être indésirable, il faut le signaler. Il y a différentes façons de le faire auprès de vos fournisseurs de services. Si vous envoyez vos messages textes indésirables au 7726, qui épelle « SPAM » sur votre téléphone, ils seront examinés. Dans certains cas, l'information est partagée.

Chose certaine, si des personnes sont témoins de courriels malveillants ou menaçants, ou de courriels accompagnés de logiciels malveillants et qui semblent douteux, il existe des moyens de les signaler en toute sécurité. Les gens n'ont pas tendance à le faire, mais il y a des façons de procéder.

Veillez à ce que vos systèmes soient toujours à jour si vous pensez être la cible d'une menace sur le plan de la cybersécurité. Le plus gros point faible, c'est l'obsolescence du système — ou un système qui n'a pas fait l'objet d'un correctif, pour employer un jargon technique.

Le président: Je vous remercie, monsieur Jones. Je vais devoir m'arrêter ici, sans quoi je serai destitué par mes collègues.

[*Difficultés techniques*]

Le président: Oh, il est agréable d'entendre de la musique.

Il y a un manquement à notre propre sécurité.

● (1715)

M. Glen Motz: Monsieur le président, je vote pour la destitution.

Des députés: Ah, ah!

Le président: Nous allons maintenant laisser la parole à Mme Stubbs, qui a cinq minutes.

Mme Shannon Stubbs: Je vous remercie, monsieur le président. En fait, votre question précédente était extrêmement importante.

Mes questions portent sur deux sujets. S'il me reste du temps et que vous êtes d'accord, j'aimerais si possible partager mon temps de parole avec mon collègue, M. Van Popta, qui aura peut-être une interrogation.

Le président: C'est possible.

Mme Shannon Stubbs: Bien. Je vous remercie, monsieur le président.

Monsieur Jones, vous avez dit que la Chine, la Russie, la Corée du Nord et l'Iran représentent des menaces pour le Canada. Vous savez probablement que des chercheurs israéliens et américains ont récemment découvert que la Chine détourne le trafic Internet au moyen de services contrôlés par l'État.

Si possible, pourriez-vous nous dire s'il s'agit selon vous d'espionnage ou de vol de propriété intellectuelle? Quel en est l'objectif? Le Centre de la sécurité des télécommunications a-t-il agi? Quelle mesure a-t-il prise pour empêcher la Chine de détourner le trafic Internet canadien?

M. Scott Jones: La question peut se rapporter à des enjeux classifiés, mais je vais tout de même en parler, en espérant y répondre pleinement.

Quelques éléments entrent en ligne de compte. À vrai dire, Internet est conçu de façon à emprunter la route la moins chère, qui est généralement la plus rapide. Or, il est possible de prétendre être la route la moins chère et la plus rapide, ce qui oblige Internet à la traverser. La technique en question s'appelle le « piratage du protocole BGP », mais je ne me perdrai pas dans les dédales techniques.

C'est une des choses sur lesquelles nous travaillons en partenariat avec les entreprises de télécommunications. J'ai déjà parlé d'innovation, et nous cherchons des façons d'innover et de travailler avec nos entreprises de télécommunications pour déceler ce genre d'activité. Nous leur demandons aussi quels moyens de défense nous pouvons employer pour empêcher un tel piratage.

Ce n'est pas courant, mais c'est une menace possible que nous surveillons. Nous cherchons des façons d'atténuer le risque et de nous en prémunir, sans pour autant réduire la fiabilité d'Internet.

Puisqu'il y a d'importants changements à ce chapitre, la situation est un peu préoccupante. À vrai dire, il faut pouvoir regrouper toutes les données qui vont du point A au point B, et le chiffrement constitue un excellent moyen de défense.

Du côté de nos applications, par exemple, nous utilisons en ce moment un canal Zoom chiffré. Il n'est pas possible pour le public d'y accéder; il faut s'y inscrire, et ainsi de suite. Il y a donc un chiffrement. Lorsque j'envoie un message par n'importe quelle application de messagerie, c'est chiffré.

Désormais, nos sites Web et ceux du gouvernement sont tous chiffrés, et il est à espérer qu'un nombre grandissant de sites commerciaux le seront entièrement. Cet outil empêche immédiatement une personne d'utiliser l'information à une fin quelconque; elle se retrouve avec une foule de données chiffrées et ne peut rien en faire.

Ce sont là quelques-uns des mécanismes de défense.

Mme Shannon Stubbs: Je vous remercie.

À propos d'un sujet que nous avons abordé plus tôt, je constate que la stratégie de notre gouvernement sur les infrastructures essentielles n'a pas été mise à jour depuis 2009. J'aimerais parler de la possibilité qu'un rançongiciel cible les grandes entreprises et les infrastructures essentielles. Je voudrais avoir plus de précisions et de détails sur la nature ou la profondeur des relations que vous avez établies avec les exploitants d'infrastructures essentielles du secteur privé. Avez-vous noué des liens avec ceux qui sont au pouvoir et qui peuvent prendre des décisions officielles?

M. Scott Jones: Tout à fait. Nous avons commencé par le secteur des télécommunications, qui est à l'origine de bien des choses sur le plan de la cybersécurité. Nous nous sommes ensuite attardés au secteur de l'énergie, et plus particulièrement à celui de l'électricité d'un océan à l'autre. Par conséquent, nous collaborons bel et bien avec des partenaires, et nous avons en effet communiqué avec les cadres supérieurs de ces entreprises. Nous cherchons toujours à renforcer ces partenariats. Je viens de décrire le travail que nous avons réalisé avec les entreprises de télécommunications. Nous envisageons de faire de même avec les entreprises d'électricité dans le but de contrer les menaces qui planent sur la recherche et le développement — il s'agirait d'une amélioration conjointe où les entreprises investiraient avec nous pour trouver une façon de parer à la menace. Il y a un critère à respecter: lorsque nous apprenons des choses, il faut les mettre en commun avec tous les intervenants du secteur.

Si nous travaillons avec une entreprise donnée, nous faisons bien attention de ne jamais lui faire bénéficier d'un avantage concurrentiel. Nous voulons nous assurer que ce soit profitable pour l'ensemble du secteur. Nous sommes le gouvernement; notre objectif est de faire en sorte que les solutions s'appliquent du nord au sud et d'est en ouest, et qu'elles soient mises en commun ouvertement afin que chacun puisse en profiter, où qu'il soit. Il y a de grandes entreprises au Canada qui disposent de plus de ressources. Nous les avons vues assumer leurs responsabilités. Nous avons vu leurs cadres supérieurs intensifier les efforts. Nous travaillons avec elles. Par exemple, je rencontre assez régulièrement les cadres supérieurs des sociétés énergétiques, et aussi des entreprises de télécommunications, simplement pour m'assurer que nous sommes sur la bonne voie et que nous nous attaquons aux menaces les plus criantes. Ces gens ont une très bonne compréhension des risques. Les efforts se multiplient, mais on peut encore faire mieux.

Pour répondre à votre question, les infrastructures essentielles représentent un vaste secteur. Il y a un certain nombre de fournisseurs très dispersés au pays. Nous sommes à la recherche de chefs de file, mais aussi d'organisations comme les associations industrielles qui peuvent réunir tous leurs membres à la table et les représenter auprès de nous.

● (1720)

Le président: Nous allons devoir en rester là, madame Stubbs.

Qui est le prochain intervenant pour les libéraux?

Allez-y, madame Khera.

Mme Kamal Khera: Je vous remercie, monsieur le président.

Merci, monsieur Jones.

Je représente la circonscription de Brampton-Ouest, et vous savez peut-être qu'en 2019, nous avons travaillé en très étroite collaboration avec l'Université Ryerson pour qu'elle devienne un catalyseur en cybersécurité. Une partie de l'initiative a aussi été financée par le gouvernement canadien. Il y a donc un centre national de la cybersécurité et de l'innovation situé à Brampton. Le catalyseur favorise la collaboration dans le but de donner plus de moyens d'action aux entreprises et de s'attarder à ce dont vous parlez, c'est-à-dire l'innovation, afin que les entreprises s'attaquent aux problèmes.

Connaissez-vous ce centre? Y a-t-il des occasions de partenariat ou de collaboration avec ce catalyseur?

M. Scott Jones: Nous connaissons certainement le centre. Il est toujours agréable de voir une organisation prendre position. Nous n'avons jamais prétendu avoir le monopole de l'innovation ou de la résolution du problème. Nous essayons d'arriver à la table en toute humilité avec nos connaissances, mais nous savons que d'autres ont des compétences et aborderont le problème sous un angle différent.

Il y a toujours des occasions à saisir. Nous essayons de divulguer certains de nos défis, notamment sur le plan de la recherche, que le Centre de la sécurité des télécommunications a publiés. Nous avons collaboré avec le Conseil national de recherches pour divulguer certains de nos défis qui se rapportent plus à la recherche qu'au développement. Ensuite, nous avons également organisé des événements, comme la GeekWeek, qui a lieu en octobre. Les organisations peuvent poser leur candidature. L'activité était bien sûr virtuelle cette année, mais elle est habituellement en personne. Plus de 200 professionnels de la cybersécurité du Canada, des universités, de l'industrie, du gouvernement et du monde entier se réunissent pour commencer à s'attaquer ensemble à ces problèmes. Voilà un autre volet qui nous permettrait de contribuer et de collaborer à des projets de recherche.

Enfin, nous sommes toujours ouverts aux bonnes idées. Je fais partie d'un collectif qui cherche des endroits où nous pouvons travailler ensemble à des solutions comme une initiative conjointe de cyberdéfense. Nous sommes toujours à la recherche de bonnes idées et nous écoutons ce que les gens ont à dire.

Mme Kamal Khera: C'est excellent. Je vous remercie de votre réponse.

Peut-être pouvez-vous nous dire quelques mots sur le fait que votre organisme est relativement jeune, puisqu'il a été créé en 2018. Pouvez-vous nous expliquer brièvement la méthode qui était employée avant cette date pour contrer les cybermenaces et sensibiliser les gens à leur sujet? Cette méthode avait-elle des limites dans la prévention et la lutte contre les cyberattaques?

M. Scott Jones: Je vais avoir l'air de me vanter. Toutes ces organisations existaient déjà. Sécurité publique Canada, par exemple, avait déjà lancé la campagne Pensez cybersécurité. Au Centre de la sécurité des télécommunications, nous avions la Direction de la sécurité des TI depuis la fin des années 1940 ou le début des années 1950, qui s'occupait principalement du chiffrement, mais qui s'orientait de plus en plus vers la cybersécurité. Bien sûr, Services partagés Canada avaient aussi des opérations de sécurité. Nous avons donc réuni tous ces secteurs, car nous devions commencer à nous occuper de cette menace qui touche l'ensemble de l'économie.

En ce qui concerne les mesures que nous avons prises, il y a vraiment eu une approche axée sur la collaboration avec l'industrie et des partenaires. Nous ne voulions pas imposer notre aide sous prétexte que nous représentons le gouvernement fédéral, mais plutôt proposer une collaboration, en reconnaissant que les autres joueurs ont eux aussi des connaissances et une expertise.

En deuxième lieu, nous avons essayé de donner des conseils et des lignes directrices pratiques. En fait, tous nos conseils ont été reformulés, et pas seulement ceux à l'intention des petites et des moyennes entreprises, de façon à dire ce qu'un simple citoyen devrait faire de manière réaliste, et non un informaticien titulaire d'un doctorat. Nos conseils et lignes directrices étaient pratiquement inaccessibles, et ils sont désormais intelligibles. Je suis très heureux d'entendre tous les commentaires à propos du rapport. Je suis vraiment ravi que les gens le trouvent facile à comprendre. Il a été formulé pour que chacun d'entre nous puisse le lire.

Troisièmement, nous nous sommes beaucoup attardés aux initiatives conjointes de cyberdéfense. Nous avons travaillé avec des partenaires industriels pour résoudre le problème ensemble. Nous avons une certaine expertise. Le gouvernement du Canada a mis en place de très bonnes défenses au cours de la dernière décennie. Comment pouvons-nous mettre en application ces leçons? Le Bouclier canadien de l'Autorité canadienne pour les enregistrements Internet en est un exemple. Nous travaillons en collaboration avec nos entreprises de télécommunications, les exploitants d'infrastructures essentielles et, bien sûr, les provinces et les territoires. C'est un secteur où nous sommes encore en train d'établir des relations, mais nous avons certainement vu différentes provinces venir à la table des négociations pour nous demander de travailler ensemble. Nous avons en ce moment des relations avec la totalité des provinces et des territoires. Un des objectifs est d'adopter une approche pancanadienne.

● (1725)

Mme Kamal Khera: Je vous remercie.

Me reste-t-il du temps, monsieur le président?

Le président: Vous avez 30 secondes.

Mme Kamal Khera: Je vais céder mon temps à mon amie, Mme Damoff.

Mme Pam Damoff: Je vous remercie, madame Khera.

Ma question est fort simple: l'application COVID est-elle sécuritaire? Vous pouvez répondre par oui ou non.

M. Scott Jones: Oui.

Mme Pam Damoff: C'est très bien.

Le président: Vous avez encore 15 secondes.

Mme Pam Damoff: Je vous remercie, monsieur le président.

Le président: Madame Michaud.

[*Français*]

Madame Michaud, vous disposez de deux minutes et demie.

Mme Kristina Michaud: Je vous remercie, monsieur le président.

Je vais terminer par une question moins simple. Je vous laisserai tout le temps pour y répondre.

Si, à l'heure qu'il l'est, le gouvernement ne prend pas de mesures précises pour contrer la cybermenace pour protéger la population, les entreprises et les infrastructures gouvernementales, selon vous, cela pourrait-il représenter un danger pour notre démocratie? Quelles mesures devraient être prises?

Il semble y avoir une certaine responsabilité partagée entre chacun des individus et les entreprises, mais aussi par les pouvoirs publics. J'aimerais vous entendre parler à ce sujet.

Quelles sont vos attentes concernant la publication de ce rapport?

Vous êtes une organisation assez récente. Y a-t-il des mesures qui devraient être prises en particulier?

[*Traduction*]

M. Scott Jones: Je pense que plusieurs éléments entrent en ligne de compte. Nous prenons pas mal de mesures pour essayer de relever la barre de la cybersécurité: certaines sont publiques alors que d'autres sont privées. Nous agissons. Nous avons des plans stratégiques d'atténuation, qui s'attaquent directement aux menaces mentionnées dans le rapport. Il y en a un sur la cybercriminalité et l'autre, sur la protection des infrastructures essentielles. Le premier portait sur la défense de la démocratie. Il y a aussi le plan des opérations qui est suivi des opérations à proprement parler, ce qui pourrait comprendre des cyberopérations défensives visant à protéger et à agir, au besoin. Il s'agit vraiment de tirer parti du mandat que le Parlement nous a confiés dans le cadre de la Loi sur le Centre de la sécurité des télécommunications, et de nous assurer de prendre des mesures globales.

En deuxième lieu, nous devons cependant nous assurer de divulguer les informations pratiques aux gens et de collaborer avec eux pour qu'ils puissent agir par eux-mêmes. Le rapport avait justement pour objectif de dire quelles sont les menaces qui se profilent. Si les Canadiens lisent le rapport, ce que j'espère — j'en serais ravi —, ils pourront prendre certaines mesures fondamentales. Ils peuvent suivre les directives de Pensez Cybersécurité. Les petites et moyennes organisations peuvent lire nos conseils et nos lignes directrices les concernant pour savoir si elles atténuent leurs risques cybernétiques. Il y a ensuite le programme CyberSécurité Canada, qui a été lancé par Innovation, Sciences et Développement économique Canada. Les entreprises pourront se servir de ces outils pour confirmer qu'elles ont pris des mesures et qu'elles peuvent cocher une case sur le plan de la cybersécurité. J'aimerais que nous puissions l'utiliser pour évaluer les entreprises canadiennes. Ce crochet serait une sorte davantage concurrentiel pour l'entreprise et indiquerait qu'elle a fait le travail.

Ce sont des choses qui pourraient être faites directement au moyen du rapport. Il faut comprendre la menace, savoir où l'entreprise s'expose au risque, puis prendre des mesures pour rectifier le tir. Nous avons beaucoup d'informations qui, nous l'espérons, permettront aux Canadiens de faire des choix semblables.

Le président: Vous verriez cela un peu comme la norme ISO pour une entreprise?

M. Scott Jones: C'est un programme qui est déjà en place. C'est une comparaison possible, sauf que ce serait un objectif vraiment atteignable pour une petite ou moyenne entreprise, alors que les normes ISO ne sont généralement accessibles qu'aux grandes organisations.

Le président: D'accord.

Monsieur Harris, vous avez deux minutes et demie.

M. Jack Harris: Merci.

C'est donc davantage comparable à un signe indiquant qu'un légume est biologique.

Des voix: Ha, ha!

M. Jack Harris: Monsieur Jones, j'ai une question qui découle d'une recommandation formulée par notre comité en 2019 à l'issue d'une étude sur la cybersécurité dans le système financier considérée comme un enjeu lié à la sécurité économique de notre pays.

Voici donc notre recommandation 9 :

> Le Comité recommande que le gouvernement du Canada explore de nouveaux moyens pour s'assurer que toutes les données sensibles qui circulent au Canada suivent un chemin de routage domestique et ne sont pas exposées à une infrastructure réseau étrangère.

Pourriez-vous nous dire ce que le Canada a fait au cours de la dernière année pour donner suite à cette recommandation? Vous avez mentionné le cryptage parmi les mesures de protection possibles. Y a-t-il d'autres moyens que notre pays devrait mettre en œuvre?

Je me pose la question dans le contexte de la vente récente d'une entreprise de ma circonscription, Verafin, qui a été acquise par Nasdaq Inc. pour la mirobolante somme de 2,75 milliards de dollars. Cette entreprise s'intéresse notamment au suivi des obligations des banques et des institutions financières au moyen du CANAFE.

Dans une situation semblable, comment pouvons-nous assurer que les données de nature délicate sont acheminées via un parcours intérieur pour ne pas être exposées à une infrastructure réseau étrangère?

● (1730)

M. Scott Jones: C'est une question qui m'intéresse au plus haut point. L'infrastructure de télécommunications du Canada — et mes collègues du ministère de l'Innovation, des Sciences et du Développement économique pourraient vous en dire plus long — se distingue notamment du fait qu'elle s'inscrit généralement dans une orientation nord-sud qui est attribuable au mode d'aménagement des réseaux Internet et autres interconnexions. La vaste majorité de nos connexions sont avec nos voisins du Sud, alors que les liens est-ouest sont plutôt rares. Il y a eu cependant certains investissements de ce côté-là.

Il est donc possible que l'on ne soit tout simplement pas capable d'acheminer des données en suivant un parcours uniquement canadien. Nous ne sommes pas nécessairement les mieux placés pour agir à ce niveau. Il faut par conséquent se demander comment on peut assurer la protection des données, peu importe l'itinéraire emprunté.

Il y a une chose qu'il faut absolument savoir au sujet d'Internet. Si je vous envoie un courriel à l'instant, il se peut qu'il fasse le tour du monde avant de parvenir à votre bureau de circonscription. Le mode de fonctionnement des connexions Internet fait en sorte qu'un tel message ne va pas nécessairement demeurer dans les limites du Canada. Il peut transiter par n'importe quel endroit au monde. C'est pour cette raison que nous préconisons des mesures de protection. Le cryptage est la meilleure qui soit. Il fait en sorte que la confidentialité n'est pas compromise.

En fait, il y a certaines caractéristiques de l'infrastructure Internet qui pourraient certes assurer une meilleure cybersécurité non seulement du point de vue de la souveraineté, mais aussi dans la perspective de la fiabilité. Nous souhaiterions assurément pouvoir miser davantage sur ces éléments, mais d'énormes investissements du secteur privé sont nécessaires à cette fin. Mes collègues d'Innovation, Sciences et Développement économique Canada seraient sans doute mieux à même de répondre à cette question.

Le président: Merci, monsieur Harris.

Il est passé 17 h 30, mais personne ne nous pousse dans le dos. Nous serions censés avoir encore deux intervenants, un pour les libéraux et un pour les conservateurs.

Souhaitez-vous que nous continuions ou voulez-vous que nous nous arrêtions maintenant?

Mme Pam Damoff: Je crois que nous pouvons nous arrêter, monsieur le président.

Le président: D'accord.

Monsieur Jones, je tiens à vous remercier au nom du Comité. Votre rapport et vos réponses sont formulés d'une manière tout à fait intelligible, ce qui est primordial pour un exercice semblable. Il faut que tous comprennent à quel point nous sommes vulnérables, aussi bien individuellement que collectivement en tant que nation, étant donné toutes les menaces qui nous guettent.

Votre analyse des enjeux de sécurité nous a été d'une grande utilité. Nous vous sommes reconnaissants pour votre comparution, et je m'attends à ce que nous vous invitions de nouveau.

Sur ce, je vous remercie également, chers collègues.

Avant que je ne lève la séance, je veux que vous sachiez que personne ne nous a rien dit pour l'instant quant à la possibilité que nous nous réunissions la semaine prochaine. C'est donc à suivre.

Merci encore une fois.

La séance est levée.