CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

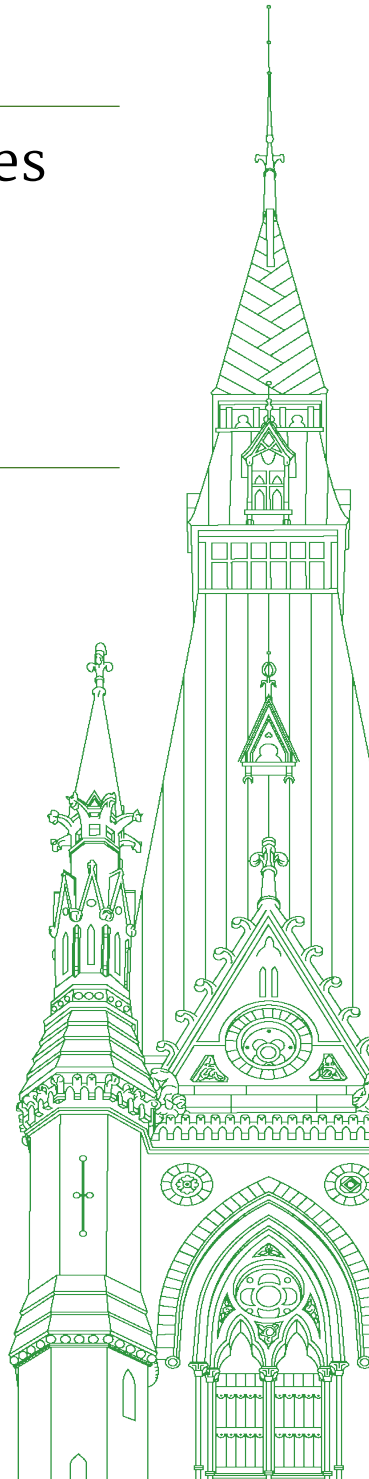
43e LÉGISLATURE, 1re SESSION

Comité permanent de l'industrie, des sciences et de la technologie

TÉMOIGNAGES

NUMÉRO 016

Le mercredi 20 mai 2020



Présidente : Mme Sherry Romanado

Comité permanent de l'industrie, des sciences et de la technologie

Le mercredi 20 mai 2020

● (1500)

[*Traduction*]

La présidente (Mme Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.)): Bonjour à tous. Je déclare maintenant la séance ouverte.

Bienvenue à la 16e séance du Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des communes. Conformément à l'ordre de renvoi du samedi 11 avril, le Comité se réunit pour recueillir des témoignages sur la réponse du gouvernement à la pandémie de la COVID-19.

La séance d'aujourd'hui se déroule par vidéoconférence, et les délibérations seront diffusées sur le site Web de la Chambre des communes.

Je rappelle aux membres et aux témoins d'attendre que je les désigne par leur nom avant de prendre la parole. Quand vous êtes prêts à parler, activez votre microphone, et désactivez-le quand vous avez terminé. Veuillez parler lentement et intelligiblement pour que les interprètes puissent accomplir leur travail, et formulez vos questions et vos observations par l'entremise de la présidente.

Comme je le fais habituellement, je brandirai le carton jaune quand il reste 30 secondes à votre intervention, et le carton rouge quand votre temps est écoulé.

Je vais maintenant accueillir nos témoins.

[*Français*]

De l'Autorité des marchés financiers, nous recevons M. Jean-François Fortin, directeur général du contrôle des marchés, ainsi que M. Christian Desjardins, directeur de l'évaluation et du renseignement.

[*Traduction*]

Nous recevons également M. Byron Holland, président et chef de la direction, M. Dave Chiswell, vice-président au Développement de produits, et M. Albert Chang, conseiller juridique, de l'Autorité canadienne pour les enregistrements Internet.

Nous entendrons aussi M. Scott Jones, dirigeant principal du Centre canadien pour la cybersécurité, du Centre de la sécurité des télécommunications.

M. Simon Marchand, examinateur de fraude certifié et administrateur agréé en Biométrie et sécurité, témoignera au nom de Nuance Communications.

Enfin, de la Gendarmerie royale du Canada, nous accueillons M. Eric Slinn, commissaire adjoint aux Opérations criminelles de la Police fédérale, ainsi que

[*Français*]

M. Guy Paul Larocque, officier responsable intérimaire, du Centre antifraude du Canada.

[*Traduction*]

Chaque témoin fera un exposé de cinq minutes, suivi par nos tours de questions.

Nous commencerons aujourd'hui par l'Autorité des marchés financiers. Vous disposez de cinq minutes.

[*Français*]

M. Jean-François Fortin (directeur général, Contrôle des marchés, Autorité des marchés financiers): Je vous remercie, madame la présidente.

Comme vous l'avez mentionné tout à l'heure, je suis le directeur général du contrôle des marchés. Je suis accompagné de mon collègue Christian Desjardins, directeur de l'évaluation et du renseignement.

L'Autorité des marchés financiers est le régulateur des marchés financiers au Québec et il a pour mission d'encadrer le secteur financier.

L'Autorité des marchés financiers assure en tout temps une vigie proactive des enjeux et problématiques liés à la fraude financière. Ces efforts de vigie se font de multiples façons au sein de plusieurs équipes de l'Autorité, ainsi que par nos participations actives au sein de comités québécois, canadiens ou internationaux.

Nous disposons d'équipes multisectorielles, qui travaillent de façon concertée pour assurer la surveillance des marchés, la cybersurveillance et la vigie des marchés. Nous déployons aussi d'importantes ressources financières pour mener des campagnes majeures de sensibilisation et des partenariats stratégiques.

Depuis le 16 mars, l'Autorité des marchés financiers est en mode télétravail. Nous avons su mettre en place rapidement les équipes nécessaires pour que les activités de mise en application des lois et de sensibilisation se poursuivent à distance. Tous les employés, à quelques exceptions près, sont pleinement fonctionnels en télétravail. Certaines activités, comme des entrevues ou des témoignages en personne, ont dû être ralenties, mais cela n'affecte pas nos activités. Les activités de collecte et d'analyse de l'information, de même que des entrevues en vidéoconférence, se poursuivent.

Dans le cadre de la pandémie de la COVID-19, l'Autorité a intensifié ses activités de surveillance sur le Web, notamment. Nous participons également à un groupe d'intervention sur les investissements frauduleux, qui regroupe des gens de l'ensemble des régulateurs en valeur mobilière au Canada, afin d'échanger de l'information sur les activités illégales observées en lien avec la COVID-19.

Nous participons également au groupe de travail qui a été mis sur pied par la North American Securities Administrators Association, une association qui regroupe des régulateurs en valeur mobilière du Canada et des États-Unis et qui vise à coordonner la mise au jour des fraudes potentielles en matière d'investissement liées à la COVID-19 de même qu'à coordonner les enquêtes connexes, et d'informer le public des dangers potentiels.

De plus, nous avons mis en place une stratégie de surveillance des marchés afin de cibler davantage les activités de manipulation de marchés et de délits d'initiés potentiels. À ce titre, nous avons surveillé de plus près les compagnies pharmaceutiques, notamment, en lien avec la fausse promotion de vaccins ou de solutions pharmaceutiques miracles, par exemple.

Nous faisons également des efforts particuliers et une surveillance plus adaptée en lien avec de potentiels délits d'initié dans le contexte du report de la divulgation des états financiers qui a été accordé par les régulateurs compte tenu de la pandémie. Ce report de divulgation d'information relative au marché accentue les risques de délits d'initiés, puisque les dirigeants ou d'autres personnes, comme des professionnels ou des conseillers, peuvent avoir accès plus longtemps à de l'information délicate inconnue du public.

Cela conclut le volet qui traite de la surveillance des marchés et de la mise en application des lois.

Nous avons aussi poursuivi de façon très proactive les interventions et les initiatives d'information visant le public. L'Autorité a cherché à sensibiliser le public en diffusant sur son site Web des alertes dédiées concernant la prévention de la fraude en lien avec la COVID-19. Nous avons également augmenté nos publications au sujet de la prévention de la fraude sur les médias sociaux, comme Facebook.

Nous avons également adressé des communications écrites aux principales associations d'aînés et aux associations de consommateurs du Québec pour rappeler le maintien de nos services d'assistance et pour les inviter à nous faire part des problèmes qu'elles peuvent observer, notamment les tentatives de fraude.

Enfin, nous avons aussi publié de multiples mises en garde, qui sont diffusées sur les médias sociaux et qui sont souvent relayées par nos partenaires.

J'aimerais aussi souligner un élément important. Dès le mois de mars, à la suite d'observations de tentatives de fraude liées à la COVID-19, nous avons investi dans une campagne majeure qui a été déployée du 6 avril au 5 mai à la télé, sur le Web et sur d'autres médias sociaux.

● (1505)

Je voudrais souligner qu'il y a eu plusieurs initiatives de sensibilisation diffusées à la télévision, dans les médias sociaux et par d'autres moyens de communication pour atteindre les personnes âgées et les personnes vulnérables.

L'Autorité des marchés financiers est l'un des régulateurs en matière financière au Canada. Il y a une collaboration constante avec l'ensemble des régulateurs canadiens en la matière et les régulateurs internationaux.

Merci.

La présidente: Je vous remercie beaucoup, monsieur Fortin.

[*Traduction*]

Nous entendrons maintenant l'Autorité canadienne pour les enregistrements Internet.

Monsieur Holland, vous disposez de cinq minutes.

M. Byron Holland (président et chef de la direction, Autorité canadienne pour les enregistrements Internet): Je vous remercie beaucoup, madame la présidente et distingués membres du Comité.

La plupart des gens savent que l'Autorité canadienne pour les enregistrements Internet, ou ACEI, est l'organisme qui gère le registre du domaine .ca. Notre mission première consiste à gérer un espace de domaine sécuritaire et stable.

L'ACEI est considérée comme un chef de file mondial dans l'industrie des noms de domaine. En fait, de nombreux pays s'inspirent de nos infrastructures, de nos services et de nos connaissances pour leurs propres registres de noms de domaine. Notre technologie est considérée comme la meilleure parmi nos pairs. Bref, l'ACEI est parfaitement équipée pour affronter la crise de la COVID-19. Nous avons confiance en notre capacité de protéger l'intégrité du domaine .ca.

À ce jour, nous avons détecté un peu plus de 2 000 noms de domaines comportant des mots-clés relatifs à la COVID-19. Pour mettre les choses en contexte, nous avons enregistré plus de 200 000 noms de domaines depuis janvier. Ce chiffre cadre avec ce que nous observons chez nos pairs de l'Europe et du reste du monde, où les noms de domaines relatifs à la COVID-19 composent moins de 1 % des enregistrements effectués jusqu'à maintenant cette année. Sachez toutefois qu'un grand nombre de ces noms de domaine sont parfaitement légitimes et même bénéfiques, comme conquercovid19.ca, une campagne de soutien aux premiers intervenants.

Nous examinons soigneusement tous les domaines relatifs à la COVID-19 pour nous assurer qu'ils sont conformes à nos règles, en ce qui concerne particulièrement les exigences relatives à la présence canadienne, et nous veillons à ce que tous les domaines restent canadiens. Nous collaborons aussi avec le milieu international des noms de domaines, notamment avec des organisations comme Council of European National Top-Level Domain Registries, pour nous assurer que nous appliquons les mêmes pratiques que nos pairs du reste du monde.

L'ACEI n'est toutefois par mandatée pour examiner ou authentifier le contenu des sites Web ayant un nom de domaine .ca. En outre, une telle authentification ne devrait pas être efficace, puisqu'Internet, et les menaces connexes sont d'envergure internationale. Même si les noms de domaines .ca sont assujettis à la loi canadienne, des milliers d'autres menaces viennent de l'étranger. Il existe des outils et des processus bien établis pour contrer la fraude en ligne et les cyberattaques. Si des Canadiens tombent sur un domaine dont ils soupçonnent qu'il est frauduleux ou malveillant, ils devraient communiquer avec le Centre antifraude du Canada ou le Centre canadien pour la cybersécurité, avec lesquels nous travaillons en étroite collaboration.

Au chapitre de la fraude sur Internet, il importe de se rappeler que les pirates adorent les crises. Même si les solutions techniques constituent une importante protection contre la fraude en ligne et les cybermenaces, le plus grand vecteur d'attaques est la faiblesse humaine. Les cybervoleurs exploitent l'anxiété, l'incertitude et la peur afin de s'en prendre aux Canadiens alors qu'ils sont à leur plus vulnérable. Malheureusement, l'actuelle pandémie de COVID-19 constitue un terreau fertile pour ces criminels.

C'est dans cet environnement que nous avons lancé le Bouclier canadien de l'ACEI, une solution gratuite de sécurité et de protection des renseignements personnels destinée aux citoyens canadiens et à leurs familles. En collaboration avec notre partenaire, le Centre canadien pour la cybersécurité, nous protégeons déjà plus de 50 000 Canadiens avec le Bouclier canadien quand ils travaillent, apprennent, enseignent et socialisent alors qu'ils sont confinés à la maison pendant la pandémie. Le Bouclier canadien s'inscrit dans l'engagement de l'ACEI à établir un Internet fiable pour les Canadiens. Nous nous réjouissons d'avoir l'occasion de protéger chaque Canadien avec ce service gratuit.

L'ACEI contribue à protéger les hôpitaux, les écoles, les universités et les municipalités du Canada grâce au service de cybersécurité d'entreprise du pare-feu DNS, un outil installé chez plus de 1,1 million d'utilisateurs, dont des étudiants, des enseignants, des médecins, des fonctionnaires municipaux et des premiers intervenants de toutes les régions du Canada.

● (1510)

La présidente: Excusez-moi un instant, monsieur Holland. Je pense que quelqu'un invoque le Règlement.

[*Français*]

M. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Madame la présidente, les interprètes nous ont signalé une espèce de sifflement il y a deux ou trois minutes. Nous n'entendons plus l'interprétation à cause de la mauvaise qualité du son. Ce serait dommage que les propos de M. Holland ne puissent pas être entendus par les francophones.

La présidente: D'accord.

Merci beaucoup, monsieur Lemire. Nous allons vérifier ce qu'il est possible de faire.

[*Traduction*]

Nous passerons au témoin suivant, question de voir si nous pouvons régler le problème de microphone de M. Holland et entendre le reste de son témoignage.

Sur ce, nous entendrons M. Jones, du Centre de la sécurité des télécommunications. Vous disposez de cinq minutes.

● (1515)

M. Scott Jones (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Bonjour, madame la présidente et distingués membres du Comité. Je vous remercie de m'avoir invité à témoigner depuis ma salle à manger aujourd'hui afin de traiter de la cyberfraude relative à la pandémie.

Je m'appelle Scott Jones et je suis à la tête du Centre canadien pour la cybersécurité, lequel relève du Centre de la sécurité des télécommunications, ou CST. La CST est un des organismes de renseignement clés du Canada et la principale autorité technique du pays en matière de cybersécurité. Lancé en octobre 2018, le Centre pour la cybersécurité est une organisation relativement nouvelle, mais forte d'une riche histoire et de plus de 70 ans d'expérience en cybersécurité, ayant auparavant fonctionné dans le cadre du mandat de sécurité des TI de longue date du CST. Le Centre pour la cybersécurité constitue une source unifiée de conseils, d'avis, de services et de soutien d'experts sur les questions opérationnelles de cybersécurité, et offre aux citoyens et aux entreprises du Canada une source fiable et transparente de conseils en matière de cybersécurité.

Le Centre pour la cybersécurité s'intéresse particulièrement à cinq principaux domaines. Nous informons d'abord le Canada et les Canadiens au sujet des questions de cybersécurité. En outre, nous protégeons les intérêts des Canadiens au chapitre de la cybersécurité grâce à des conseils, des avis, de l'aide concrète ciblés et de solides partenariats fondés sur la collaboration. De plus, nous mettons au point et partageons des technologies et des outils de cyberdéfense spécialisés, ce qui améliore la cybersécurité de tous les Canadiens. Nous défendons également les sybersystèmes, notamment ceux du gouvernement, en déployant des solutions de cyberdéfence perfectionnées. Enfin, nous agissons à titre de chef de file opérationnel et de porte-parole du gouvernement lorsque surviennent des incidents de cybersécurité.

Voilà qui m'amène à l'objet de la discussion d'aujourd'hui: la cybersécurité en temps de pandémie de la COVID-19. Comme nous l'avons fait remarquer dans l'évaluation nationale des cybermenaces en 2018, la cybercriminalité constitue la plus grande menace qui cible les Canadiens. J'aimerais faire le point sur le travail que le Centre pour la cybersécurité accomplit pour protéger les Canadiens des cyberfraudes entreprises avant, pendant et après la pandémie.

En ces temps incertains, les auteurs de cybermenaces tentent de profiter du degré accru d'inquiétude et de crainte des Canadiens au sujet de la COVID-19. De nombreux Canadiens se sentent naturellement craintifs et tendus, et ces réactions émotives peuvent être exploitées en ligne. Nous avons constaté une augmentation des signalements d'acteurs malveillants qui utilisent la COVID-19 dans des campagnes d'hameçonnage et des fraudes commises au moyen de maliciels.

La COVID offre aux cybercriminels et aux fraudeurs un appât efficace qui encourage les victimes à visiter de sites frauduleux, à ouvrir des pièces jointes à des courriels et à cliquer sur des liens dans des messages textes. Souvent, ces sites Web, ces courriels et ces liens adoptent les couleurs d'organisations sanitaires ou appartiennent prétendument au gouvernement fédéral, entre autres, et visent à propager un maliciel et à soutirer de l'argent ou des renseignements personnels aux Canadiens.

Le Centre pour la cybersécurité a évalué que la pandémie de la COVID-19 présente un degré élevé de risque pour la cybersécurité des organisations sanitaires canadiennes qui participent à la réponse nationale à la pandémie. Je tiens à vous assurer que le CST et le Centre pour la cybersécurité font des pieds et des mains pour atténuer ces menaces et pour protéger les Canadiens.

Je prendrai plaisir à vous expliquer les mesures que nous prenons pour tenter de protéger le gouvernement du Canada, les systèmes importants et tous les Canadiens contre les cyberfraudes pendant la pandémie. Nous continuons de tirer parti de toutes les facettes de notre mandat pour que le Canada soit protégé contre les menaces et que le gouvernement fédéral ait accès aux renseignements qui peuvent l'aider à prendre des décisions quant à l'approche à adopter à l'égard de la COVID-19. Le Centre pour la cybersécurité travaille sans relâche pour sensibiliser continuellement la population aux cybermenaces qui ciblent les organisations sanitaires canadiennes en lançant des alertes à la cybermenace de manière proactive et en fournissant des conseils et des avis personnalisés aux organisations sanitaires canadiennes, aux partenaires du gouvernement et aux parties prenantes de l'industrie.

Outre les conseils et les avis que nous offrons aux organisations canadiennes, nous continuons d'améliorer la campagne « Pensez cybersécurité » pour aider tous les Canadiens à prendre des mesures pour assurer leur propre sécurité en ligne. En collaboration avec des partenaires de l'industrie et le réseau international d'organisations de cybersécurité, le Centre pour la cybersécurité contribue à l'élimination de sites frauduleux et d'autres mécanismes utilisés pour arnaquer les Canadiens, y compris des sites appartenant faussement au gouvernement du Canada.

Pour soutenir les programmes importants pour le gouvernement, nous continuons aussi de surveiller les programmes du gouvernement fédéral, comme l'application Web de la Prestation canadienne d'urgence, et de les protéger contre les cybermenaces. [*Difficulté technique*]

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Madame la présidente, mon audio a coupé.

La présidente: Je pense que l'Internet du témoin a malheureusement figé.

M. Glen Motz: Il doit être à Ottawa.

M. Brian Masse (Windsor-Ouest, NPD): La communication sera bonne en 2030.

[*Français*]

M. Sébastien Lemire: Monsieur Masse, je sens qu'il y a un peu d'ironie dans votre commentaire.

[*Traduction*]

La présidente: Monsieur Jones, êtes-vous toujours avec nous?

Il semble que nous ayons perdu M. Jones; nous passerons donc au prochain témoin. Nous reviendrons à M. Jones dès que nous serons capables de rétablir la communication avec lui.

Notre prochain témoin représente Nuance Communications.

● (1520)

[*Français*]

Monsieur Marchand, vous avez la parole pour cinq minutes.

M. Simon Marchand (examinateur de fraude certifié et administrateur agréé, Biométrie et sécurité, Nuance Communications): Membres du Comité, bonjour. Je vous remercie de me recevoir aujourd'hui.

Je m'appelle Simon Marchand et j'occupe le poste de chef de la prévention de la fraude chez Nuance Communications Canada. Nuance est une entreprise américaine qui est très présente à Montréal. Elle développe des technologies liées à l'intelligence artificielle et à la biométrie vocale, qui sont appliquées notamment à la prévention de la fraude. Chez Nuance, je suis spécifiquement responsable d'appliquer ces technologies de biométrie vocale pour prévenir l'usurpation d'identité. Nuance est très présente au Canada en ce moment, ses technologies de biométrie étant déployées dans la majorité des grandes banques et des entreprises de télécommunication canadiennes. Nuance est aussi présente à l'international, dans les grandes banques américaines et dans la plupart des grandes entreprises de la planète. Nous développons également des technologies destinées aux organismes d'application de la loi et à certains services gouvernementaux pour leur permettre de recueillir des éléments de preuve ou d'identifier des citoyens.

Je suis ici aujourd'hui pour vous faire part de certaines de nos observations. Dans mon rôle, je suis évidemment au courant de toutes les grandes fraudes qui ont cours sur la planète. Je veux vous faire part de certaines observations que nous avons faites en lien avec la pandémie de la COVID-19 et vous faire part de certains des risques qui ont été relevés ou qu'il faut prévoir. Cela permettra d'assurer que la législation canadienne sera prête afin de traiter les problèmes de fraude qui risquent de survenir prochainement.

Je vais commencer par certains risques internes. À cause de la pandémie de la COVID-19, certaines entreprises ont rapidement réorganisé leurs activités pour permettre le télétravail. Il ne m'appartient pas de me prononcer sur les effets bénéfiques ou néfastes du travail à distance. Par contre, le télétravail comporte des risques avérés, surtout quand on parle de service à la clientèle. Tous les agents de service à la clientèle qui sont normalement dans des centres d'appels travaillent maintenant de chez eux, dans un environnement non supervisé. Ces agents disposent de peu de ressources, mais ont maintenant l'occasion d'avoir accès à de l'information de nature délicate sur des consommateurs, qu'il s'agisse de données sur leurs actifs ou d'information pouvant être utilisée par certaines personnes pour se faire passer pour quelqu'un d'autre.

La situation socioéconomique dans laquelle nous nous trouvons va certainement exercer de la pression sur beaucoup de ménages. En matière de fraude interne, nous savons que la pression et l'occasion sont les deux motifs fondamentaux qui vont pousser un employé à agir contre les intérêts de son employeur et à commettre une fraude. Cette fraude peut consister à voler de l'information appartenant à l'organisation, dont certaines recueillent des données de nature très délicate sur les citoyens canadiens.

Ces changements dans l'organisation du travail soulèvent pour l'avenir le risque que de l'information soit volée puis diffusée sur le Web clandestin. Cela va certainement faciliter le travail des fraudeurs spécialisés dans le vol d'identité.

D'autres témoins ont mentionné l'hameçonnage. Le problème est déjà documenté, mais les fraudeurs bien organisés se sont adaptés à la pandémie et utilisent la COVID-19 comme prétexte pour tenter de soutirer de l'information aux gens. Dans certaines régions, il y a une augmentation de 600 % des tentatives d'hameçonnage prétextant la COVID-19, au moyen de pièces jointes, de sites Web ou d'autres méthodes d'approche.

Cela va permettre à des fraudeurs d'accumuler une importante quantité d'information sur les consommateurs. Cette information sera utilisée, non pas dans les prochaines semaines, mais bien dans les 6 à 18 prochains mois pour ouvrir des comptes, obtenir des produits financiers ou se procurer des produits d'entreprises de télécommunication.

Puisque les banques et les entreprises de télécommunication sont de compétence fédérale, il est pertinent que le législateur soit au courant de ces risques. On parle beaucoup de la responsabilité des entreprises pour ce qui est de protéger les données qui leur sont confiées. Cependant, je pense qu'il faut plutôt s'interroger sur la responsabilité des entreprises, en matière de reddition de compte, concernant l'information qu'elles utilisent pour offrir leurs services. En effet, quand on parle d'une banque qui se fait voler de l'information, il faut s'interroger sur sa responsabilité, qui est de protéger cette information. Personne ne s'interroge sur ce qui va être fait avec cette information une fois qu'elle est recueillie. Il y a un grand manque sur le plan de la reddition de compte.

● (1525)

C'est avec plaisir que je répondrai à vos questions à ce sujet.

La présidente: Je vous remercie beaucoup, monsieur Marchand.

[*Traduction*]

Nous reviendrons à M. Jones, qui a pu se reconnecter avec nous.

Monsieur Jones, il restait environ une minute à votre témoignage. Je ne suis pas tout à fait sûre de l'endroit où vous vous êtes arrêté, mais nous vous laisserons poursuivre votre exposé.

M. Scott Jones: On m'a indiqué où j'étais rendu. Merci. Je suis désolé qu'il y ait eu un problème. La technologie a des répercussions sur nous tous.

En collaboration avec nos partenaires de l'industrie et dans le cadre du travail international d'organisations de cybersécurité, nous avons contribué à éliminer des sites frauduleux, et j'ai parlé de la protection de la Prestation canadienne d'urgence, ou PCU.

Les auteurs de cyberattaques cherchent désormais à exploiter les connexions établies pour le télétravail, étant donné que de nombreux travailleurs exécutent leurs tâches à l'extérieur du périmètre sécurisé normalement fourni par leurs organisations. En l'occurrence, le Centre pour la cybersécurité s'est associé à l'Autorité canadienne pour les enregistrements Internet — ou ACEI, comme vous l'avez entendu — dans le but de créer et de mettre en place le Bouclier canadien de l'ACEI. Ce bouclier consiste en un service gratuit de coupe-feu DNS qui vise à protéger la confidentialité en ligne et à garantir la sécurité des Canadiens. D'ailleurs, l'ACEI a fait montre d'un leadership remarquable en mettant au service des Canadiens un mécanisme de protection des activités en ligne. Je tiens donc à la remercier du travail accompli dans le cadre de notre partenariat.

Pour protéger encore plus les Canadiens, nous avons jugé important de les tenir au courant des questions de cybersécurité. Grâce à la publication de conseils et de consignes spécialement conçus, le Centre pour la cybersécurité permet de renforcer la protection des ressources électroniques des Canadiens. Nous avons diffusé, notamment, des conseils de cybersécurité sur les outils de vidéoconférence et de télétravail. De cette façon, nous tenons à informer et à sensibiliser les Canadiens relativement aux moyens de sécuriser les activités en ligne, particulièrement en cette période où nombre d'entre nous travaillent à domicile.

Le Centre pour la cybersécurité a élaboré tout un éventail de conseils et de consignes, dont un bon nombre sont maintenant plus pertinents que jamais. D'ailleurs, j'encourage les Canadiens à visiter notre site Web pour en apprendre davantage sur les directives et les pratiques exemplaires qu'il convient de mettre en pratique pour que chacun puisse se protéger contre les cybermenaces.

Il importe enfin de souligner que le gouvernement du Canada entretient des relations solides et précieuses avec ses partenaires internationaux de la cybersécurité. Nous échangeons régulièrement des renseignements, ce qui a des répercussions importantes sur le maintien de la sûreté et de la sécurité de nos pays respectifs. Le CST et le Centre pour la cybersécurité sont à l'œuvre pour contrer les cybermenaces qui pourraient peser sur les Canadiens en ces temps difficiles. Toutefois, la cybersécurité est la responsabilité de tous, et nous nous engageons à tirer parti de notre vaste expertise pour assurer la protection du Canada et des Canadiens.

Je vous remercie de nouveau de m'avoir offert l'occasion de témoigner devant vous aujourd'hui et d'avoir fait preuve de patience à l'égard de la technologie. Je me ferai un plaisir de répondre à vos questions.

La présidente: Merci beaucoup, monsieur Jones, d'avoir pu reprendre cet appel.

Nous entendrons maintenant la GRC, puis nous reviendrons à M. Holland.

J'accorde maintenant la parole à la GRC, qui dispose de cinq minutes.

Comm. adj. Eric Slinn (commissaire adjoint, Opérations criminelles de la Police fédérale, Gendarmerie royale du Canada): Bonjour.

[*Français*]

Je vous remercie, madame la présidente.

C'est avec plaisir que je prends la parole devant le Comité dans le cadre de son étude sur la réponse du Canada à la pandémie de la COVID-19.

Je suis accompagné aujourd'hui du sergent Guy Paul Larocque, qui joue un rôle de premier plan dans la gestion du Centre antifraude du Canada, ou CAFC.

[*Traduction*]

Dans le cadre de notre mandat consistant à protéger l'intégrité économique du Canada, la criminalité financière, y compris la fraude, est depuis longtemps une priorité de la Police fédérale à la GRC. Devant la pandémie de la COVID-19, le travail que nous accomplissons avec nos partenaires des secteurs public et privé au Canada et dans le monde pour combattre et prévenir la fraude s'avère encore plus important. Cette responsabilité partagée témoigne de la confiance que les Canadiens accordent à la GRC pour veiller à leur sécurité et assurer une réponse opportune et efficace à la pandémie de la COVID-19.

Alors que les mesures visant à juguler la crise se poursuivent, la pression sur les Canadiens et les institutions qui servent le pays ne fera que s'accentuer. Les criminels chercheront à exploiter les vulnérabilités du système et des Canadiens eux-mêmes, comme nous l'avons malheureusement constaté. Nous devons faire preuve de diligence pour lutter contre ceux et celles qui tentent d'escroquer les Canadiens les plus vulnérables en misant sur leurs peurs et leurs incertitudes face à la pandémie. En termes clairs, les criminels exploitent activement la peur, l'incertitude et le doute face à la pandémie de COVID-19. Nous le savons parce que le Centre antifraude du Canada, ou CAFC, a constaté une hausse considérable du nombre de signalements de fraude de janvier à avril par rapport à la même période l'an dernier.

Depuis mars 2020, nous avons dénombré près de 1 000 plaintes de fraude relativement à la COVID-19. Dans la plupart des cas, il s'agit de tentatives d'hameçonnage dans le cadre desquelles des criminels cherchent à obtenir des renseignements personnels au moyen de courriels ou de messages textes prétendument liés à des demandes de Prestation canadienne d'urgence, ou de tentatives d'installation d'un logiciel malveillant sur les appareils des victimes. Toutefois, les plus importantes pertes pécuniaires découlent de la vente frauduleuse de biens liés à la pandémie de COVID-19, comme des masques, du matériel de dépistage ou des remèdes miracles.

Bien que nous ayons reçu un grand nombre de signalements de fraude liée à la COVID-19, les criminels continuent à user de fraudes et d'escroqueries traditionnelles pour exploiter les Canadiens, qui en subissent de lourdes conséquences. Par exemple, les fraudes commises contre les aînés l'an dernier sont estimées à plus de 700 millions de dollars, et ces types de fraudes ont gagné du terrain pendant la pandémie à mesure que ces groupes criminels insensibles ont continué d'exploiter les vulnérabilités des gens et des institutions. Enfin, les groupes du crime organisé tentent d'escroquer le gouvernement et minent les efforts visant à offrir de l'aide financière aux personnes qui sont réellement dans le besoin. L'intensification des activités frauduleuses liées à la COVID-19 et des fraudes traditionnelles illustre vraiment la capacité des groupes criminels de s'adapter aux circonstances et de les exploiter pour en tirer des gains personnels.

En réaction directe aux fraudes commises relativement à la COVID-19, la GRC a intensifié ses efforts en matière de renseignement et d'application de la loi face à ces activités illégales. Plus que jamais, nous admettons que, à tous les échelons des services de police, la GRC a un important rôle à jouer. Pour coordonner l'intervention de la GRC, en mars, nous avons commencé à exécuter un programme axé sur les fraudes liées à la COVID-19. Des efforts de coordination sont déployés à la direction générale, tandis que le CAFC s'occupe de l'analyse du renseignement, de la collecte de statistiques et des activités de communication. Des membres des divisions se chargent de la perturbation des fraudes et de l'application de la loi, en plus d'avoir la responsabilité d'assurer la liaison avec les services de police compétents pour mieux coordonner les interventions à l'échelle locale.

En reconnaissance de la responsabilité partagée entre les organismes publics et privés dans la lutte contre la fraude, la GRC collabore avec ses principaux partenaires et intervenants, au pays comme à l'étranger, pour échanger des renseignements et coordonner les efforts d'application de loi relativement à la pandémie. Si l'objectif initial était les fraudes en ligne, il s'est rapidement élargi pour inclure tous les types de fraude et de crime liés à la COVID-19, pour que nous puissions mieux veiller à la sécurité publique.

La prévention est un élément fondamental de la lutte contre la fraude. En effet, ces fraudeurs sont si envahissants et insidieux, et leurs activités si lucratives, que la seule application de la loi ne suffit pas à lutter contre ce crime; ce serait comme arracher des mauvaises herbes. Comme ma grand-mère le répétait souvent, il vaut mieux prévenir que guérir. L'accroissement continu de la sensibilisation du public est un outil essentiel de la stratégie de prévention qui doit être maintenue. Comme nous l'avons mentionné lors de notre dernière comparution devant le Comité, la GRC gère le CAFC en partenariat avec le Bureau de la concurrence Canada et la Police provinciale de l'Ontario depuis 2005. Ce centre agit à titre de chef de file en matière d'initiatives de prévention, étant notamment très actif sur diverses plateformes médiatiques pour communiquer avec les Canadiens.

En plus d'administrer le CAFC, la GRC gère une unité de prévention et de mobilisation de la police fédérale. Ce groupe joue un rôle important pour coordonner des réunions avec de nombreux services de police, organismes du gouvernement du Canada, fournisseurs du secteur privé et institutions financières à l'échelle du Canada.

● (1530)

Cela dit, je vais m'arrêter ici. Je pourrais probablement poursuivre mon intervention, mais il y a d'autres personnes qui souhaitent s'exprimer.

Je suis impatient de répondre à vos questions.

[*Français*]

Je vous remercie beaucoup.

[*Traduction*]

La présidente: Merci beaucoup, monsieur Slinn.

Cela dit, nous allons retourner à M. Holland.

Je vais lui demander s'il pourrait recommencer son témoignage au début et approcher le microphone de ses lèvres, car on entend un sifflement en arrière-plan.

M. Byron Holland: J'ai changé mon micro et mes écouteurs. Avec un peu de chance, vous m'entendrez mieux.

Madame la présidente, je vous remercie de me donner encore une fois l'occasion de faire un exposé. Comme vous me l'avez demandé, je vais commencer au début afin de m'assurer que les gens qui n'étaient pas en mesure de m'entendre le peuvent maintenant.

Je m'appelle Byron Holland, et je suis président et chef de la direction de l'Autorité canadienne pour les enregistrements Internet, ou ACEI. Notre organisation a pour principale mission d'exploiter le registre des noms de domaine .CA, d'une façon sécuritaire, stable et sécurisée.

Dans notre domaine, l'Autorité est reconnue comme un chef de file à l'échelle mondiale. En fait, un grand nombre de pays tirent parti de notre infrastructure, de nos services et de nos connaissances pour gérer leurs propres registres de noms de domaine. Parmi nos pairs, notre technologie est considérée comme la meilleure en son genre. Bref, l'ACEI est parfaitement équipée pour gérer la crise de la COVID-19. Nous avons confiance en notre capacité de protéger l'intégrité du registre des noms de domaine .CA.

Jusqu'à maintenant, nous avons repéré un peu plus de 2 000 noms de domaine .CA dont les mots clés sont liés à la COVID-19. Pour replacer les choses dans leur contexte, je précise que nous avons ajouté plus 200 000 noms de domaine depuis le début de l'année. Cela cadre avec ce que nous ont fait observer nos pairs partout dans le monde, où les noms de domaine liés à la COVID représentent moins de 1 % de l'ensemble des enregistrements. Toutefois, il est important de noter que bon nombre de ces domaines sont parfaitement légitimes, et même positifs, comme le nom de domaine conquercovid.ca, qui est lié à une campagne visant à appuyer les premiers intervenants.

Nous examinons minutieusement tous les noms de domaine liés à la COVID-19 afin de nous assurer qu'ils respectent nos règles, en général, et nos exigences relatives à la présence canadienne, en particulier. Nous travaillons aussi en collaboration avec la communauté mondiale des noms de domaine, y compris des organisations comme le Council of European National Top-Level Domain Registries, afin de nous assurer que nos pratiques exemplaires coïncident avec celles appliquées à l'échelle mondiale.

Toutefois, il est important de noter que l'ACEI n'a pas pour mandat d'examiner ou d'authentifier le contenu des sites Web des domaines .CA et, de toute manière, une telle authentification serait inefficace, étant donné qu'Internet et les menaces qui s'y rattachent sont véritablement d'origine mondiale. Même si les domaines .CA sont assujettis aux lois canadiennes, il y a des milliers d'autres menaces qui proviennent de l'extérieur de nos frontières. Des outils et des processus bien établis ont été mis en place pour gérer la fraude en ligne et les cyberattaques. Si les Canadiens trouvent des noms de domaine qu'ils soupçonnent d'être utilisés à des fins frauduleuses ou malveillantes, ils peuvent communiquer avec le Centre antifraude du Canada ou, comme nous l'avons entendu, avec le Centre canadien pour la cybersécurité. Nous travaillons en étroite collaboration avec ces deux organisations.

En ce qui concerne la fraude sur Internet, il est important de se souvenir que les pirates informatiques aiment profiter d'une crise importante. Même si les solutions techniques forment un obstacle substantiel à la fraude en ligne, la fragilité humaine, que les cybercriminels exploitent, constitue le meilleur vecteur d'attaque. Malheureusement, la pandémie actuelle a fourni à ces criminels un climat d'anxiété accrue qui les aide à exercer leurs activités, et elle a simultanément forcé la plupart des Canadiens à travailler, à apprendre, à enseigner et à socialiser au moyen de leurs appareils personnels et de leur réseau résidentiel, lesquels ne sont pas protégés par une sécurité de catégorie commerciale.

C'est dans ce contexte que nous avons lancé le Bouclier canadien de l'ACEI, une solution de sécurité et de protection de la vie privée conçue à l'intention de tous les Canadiens et de leur famille. Comme vous l'avez entendu dire, nous avons élaboré cette solution en partenariat avec le Centre canadien pour la cybersécurité. À l'heure actuelle, nous protégeons plus de 50 000 Canadiens, et ce bassin d'utilisateurs s'agrandit. Le Bouclier canadien témoigne de l'engagement que l'ACEI a pris à l'égard de la création d'un Internet digne de confiance pour les Canadiens, et nous sommes impatients de donner à tous les Canadiens l'occasion de se protéger au moyen de ce service gratuit.

Nous contribuons aussi à protéger des hôpitaux, des écoles, des universités et des municipalités du Canada à l'aide de notre service de cybersécurité d'entreprise, c'est-à-dire DNS Firewall de l'ACEI. Notre clientèle compte plus de 1,1 million d'utilisateurs qui comprennent des étudiants, des enseignants, des médecins, des travailleurs municipaux et des premiers intervenants partout au Canada. Nous offrons ce service gratuitement à tous les établissements de soins de santé et les petites entreprises du Canada jusqu'en septembre, au moment où, avec un peu de chance, la crise commencera à s'atténuer.

Enfin, la connaissance est le facteur qui importe le plus lorsqu'il s'agit de protéger les Canadiens contre la fraude en ligne. Tout comme nos parents nous ont appris à regarder des deux côtés avant de traverser la rue, les Canadiens ont besoin d'acquérir un sens pratique sur Internet qui leur permettra de repérer les tentatives de fraude, les fausses nouvelles, la désinformation et les arnaques. La meilleure façon d'y parvenir consiste à les sensibiliser et à les éduquer.

À l'ACEI, nous faisons équipe avec Beauceron Security, un excellent exemple de réussite au Nouveau-Brunswick, afin de mettre en œuvre la formation sur la sensibilisation envers la cybersécurité de l'ACEI, c'est-à-dire une plateforme qui permet d'éduquer les employés, d'établir des points de référence et de mettre les employés continuellement à l'épreuve afin de s'assurer qu'ils ont acquis le sens pratique le plus récent en matière de cybersécurité. Nous avons aussi lancé un cours de cybersécurité gratuit, intitulé « Pratiques de cybersécurité pour les travailleurs à distance », afin d'aider des milliers de Canadiens qui travaillent maintenant à la maison à se protéger et à protéger leur organisation contre des cybermenaces.

● (1535)

Tout ce que j'ai mentionné jusqu'à maintenant représente des exemples d'innovation, de compétence et de leadership canadiens dans le domaine de la cybersécurité. Toutefois, au moment où le Canada et le monde entier entrent dans une ère où Internet s'avère être un canot de sauvetage pour l'économie mondiale, nous croyons que le Canada doit en faire davantage pour être un chef de file de la cybersécurité à l'échelle mondiale. Nous encourageons le gouvernement du Canada à consacrer encore plus de fonds à la recherche sur la cybersécurité et à l'élaboration de solutions et de plateformes pour protéger les Canadiens et assurer la sécurité de notre économie numérique. C'est seulement en investissant que nous pourrons faire en sorte que les Canadiens aient accès à de la formation, des outils et des plateformes pour se protéger et protéger leurs entreprises contre la fraude en ligne et des logiciels malveillants.

Il n'y a pas de solution miracle. Comme le portrait des menaces évolue constamment, notre sensibilisation et notre technologie doivent progresser au même rythme. À l'Autorité canadienne pour les enregistrements Internet, l'ACEI, nous sommes impatients de vous aider de toutes les façons possibles.

Je vous remercie d'avoir pris le temps de m'écouter.

● (1540)

La présidente: Merci beaucoup, monsieur Holland.

Cela dit, nous allons passer à nos séries de questions. Les interventions de la première série de questions dureront six minutes, et le premier député qui interviendra sera M. Motz.

Bienvenue à la séance du Comité de l'industrie, des sciences et de la technologie. Vous avez la parole pendant six minutes.

M. Glen Motz: Merci, madame la présidente.

Chers témoins, je vous remercie de l'excellente introduction du sujet que vous nous avez donnée aujourd'hui.

Pendant cette série de questions, je vais me préoccuper surtout de M. Jones et du Centre de la sécurité des télécommunications.

Si j'ai bien compris les observations que vous avez formulées au cours de votre déclaration préliminaire, comme vous donnez des conseils sur les cyberattaques et Ia cyberfraude, vous avez conseillé le gouvernement sur les attaques étrangères et sur les sujets de préoccupation liés au cyberespace tout au long de la pandémie de COVID-19.

M. Scott Jones: Oui, c'est tout à fait exact. Nous continuons de prodiguer des conseils sur tous les aspects, bien que la majorité des activités que nous avons observées soient liées à la cybercriminalité.

M. Glen Motz: Lorsqu'une cyberintrusion survient, savez-vous d'entrée de jeu s'il s'agit d'un cas de cyberfraude, d'un cas de cyberespionnage, d'un cas d'espionnage industriel, d'une attaque aléatoire ou d'une attaque à d'autres fins?

M. Scott Jones: Habituellement, lorsqu'une sorte d'atteinte est signalée, la première mesure que nous prenons consiste vraiment à examiner la façon dont nous pouvons limiter les effets de l'intrusion d'une manière ou d'une autre, au lieu de procéder à un genre d'attribution, c'est-à-dire chercher l'acteur responsable. Nous présumons toujours que l'acteur est le plus averti qui soit et qu'il cherche à extraire de l'information ou à appliquer une technique avancée d'un type ou d'un autre. Toutefois, le fait est que presque toutes les atteintes que nous avons observées et tous les incidents qui ont été signalés sont liés à la cybercriminalité pour le moment.

Nous cherchons d'abord à limiter les effets, puis à aider la victime afin de nous assurer qu'elle est en mesure de verrouiller ses moyens de défense, d'améliorer sa sécurité, de prendre des mesures pour empêcher le problème de se propager partout dans son réseau. Ensuite, nous récapitulons, et nous faisons appel aux organisations qui conviennent, comme les organismes d'application de la loi, nos partenaires du Service canadien du renseignement de sécurité, s'il s'agit d'un acteur étranger, et bien sûr les propres employés du CST qui sont responsables du renseignement étranger.

M. Glen Motz: Fort bien.

Les attaques contre nos travailleurs de la santé de première ligne pourraient être conçues pour voler de l'information, pour vendre des renseignements personnels ou pour faciliter les activités frauduleuses. Depuis le début de la pandémie, le CST a-t-il été appelé à gérer l'une ou l'autre de ces intrusions ou de ces attaques contre nos établissements de soins de santé et nos travailleurs de la santé de première ligne? Dans l'affirmative, combien de fois êtes-vous intervenus?

M. Scott Jones: Il y a eu des cas de cyberincidents dans des secteurs liés aux soins de santé et dans des organisations de recherche et développement. Nous sommes intervenus dans un petit nombre de cas en vue de gérer l'incident et de donner des conseils et des directives.

Cependant, la majeure partie de nos activités visent à tenter de fournir des renseignements à l'avance, de signaler les vulnérabilités, par exemple, qui se développent ou qui sont annoncées, afin que les établissements de soins de santé puissent prendre des mesures préventives. Nous essayons vraiment de transmettre l'information sur les activités d'un acteur, afin de protéger les organisations à l'avance. Nous nous efforçons réellement d'anticiper les événements pour prévenir toute atteinte.

M. Glen Motz: Très bien.

Le CST a-t-il été appelé à intervenir pour contrer des attaques contre les recherches de notre propre gouvernement afin de trouver un vaccin contre la COVID?

M. Scott Jones: La défense du gouvernement du Canada est intégrée à nos opérations courantes. Pour déployer les multiples outils de défense dont nous nous sommes dotés au cours des 10 dernières années, le gouvernement s'affaire proactivement à arrêter toute activité malicieuse. Il n'y a eu aucune atteinte aux activités du gouvernement, parce que nos outils de défense sont ainsi conçus que le gouvernement est très bien protégé.

M. Glen Motz: Pour répéter ce que vous venez de dire, il y a eu des attaques, mais aucune intrusion, ce qui est positif.

Quelle est l'intention de ces attaques? Visent-elles à voler notre propriété intellectuelle ou à en tirer un gain économique? Comment les évaluez-vous?

M. Scott Jones: Selon notre analyse de la cybercriminalité, le but est véritablement d'en tirer un gain financier. Les pirates cherchent à voir comment ils peuvent en profiter. Quand on regarde un peu ce que font les États-nations, on voit que tout le monde cherche à comprendre ce qui se passe dans le monde. Nous sommes alertes à cela, et il y a globalement une augmentation de l'intérêt des États-nations entourant ces enjeux.

M. Glen Motz: Très bien.

● (1545)

M. Scott Jones: Ensuite, bien sûr, nous constatons que la propriété intellectuelle de l'industrie canadienne est constamment ciblée.

M. Glen Motz: Vous avez dit qu'évidemment, il y a déjà eu des intrusions dans nos recherches. Vous rappelez-vous la cybermenace qui avait touché les systèmes du Conseil national de recherches du Canada en 2014? Il avait dû totalement désactiver son réseau et même, le remplacer de A à Z. On dit que cette intrusion nous a coûté plus de 100 millions de dollars. Croyez-vous qu'elle était motivée par la fraude ou par d'autres fins?

M. Scott Jones: Nous estimons que l'atteinte au Conseil national de recherches était surtout motivée par un vol de propriété intellectuelle.

M. Glen Motz: Vous avez participé à l'enquête. Avez-vous aussi contribué à sécuriser le nouveau réseau?

M. Scott Jones: Absolument, nous sommes intervenus sur les deux fronts.

M. Glen Motz: Très bien.

Le gouvernement de l'époque avait pointé du doigt des acteurs commandités par l'État chinois. Est-ce exact, selon votre évaluation?

M. Scott Jones: C'est ce qu'avait déclaré le gouvernement de l'époque.

M. Glen Motz: D'accord, donc maintenant, votre organisation, monsieur Jones, a-t-elle été consultée sur les questions de cybersécurité et de sécurité informatique concernant le nouveau partenariat entre le Conseil national de recherches, l'entreprise de propriété chinoise CanSino Biologics et l'Académie des sciences médicales militaires chinoise sur la mise au point d'un nouveau vaccin contre la COVID?

M. Scott Jones: Nous travaillons constamment avec des partenaires de recherche de partout, au gouvernement, y compris dans le secteur de la santé. Nous leur fournissons les conseils les plus d'actualité en matière de cybersécurité afin que nos défenses demeurent toujours à l'avant-garde.

M. Glen Motz: Très bien, donc vous êtes intervenus dans la conclusion de cet accord.

M. Scott Jones: Nous sommes mis à contribution dans tout ce qui concerne la cybersécurité en matière de recherche.

M. Glen Motz: Merci infiniment.

La présidente: Merci beaucoup.

C'est M. Jowhari qui posera la prochaine série de questions.

Vous avez six minutes.

M. Majid Jowhari (Richmond Hill, Lib.): Merci, madame la présidente.

Je remercie tous nos témoins d'être ici et de nous fournir ces renseignements utiles.

Je m'adresserai d'abord aux représentants de l'ACEI.

Monsieur Holland, vous avez indiqué qu'environ 2 000 noms de domaines .ca ont été enregistrés depuis l'arrivée de la COVID-19. Pouvez-vous nous donner quelques statistiques concernant les éléments suivants: combien d'entre eux ont été enregistrés au Canada? Est-il possible d'enregistrer un domaine de l'extérieur du Canada et le cas échéant, combien y en a-t-il qui ont été créés ainsi? De même, concernant ces 2 000 noms de domaines, vous avez mentionné que la plupart étaient tout à fait légitimes. Combien y en aurait-il qui ne le sont pas, selon vous?

M. Byron Holland: Il y a une politique importante qui est en place et qui mérite notre attention, pour répondre à votre question. Il s'agit du critère de la présence au Canada. Tous les noms de domaines .ca doivent appartenir à une personne ou une organisation légitimement liée au Canada, de sorte que chaque nom de domaine soit lié à la juridiction canadienne et au droit canadien.

Pour ce qui est des noms de domaines enregistrés qui contiennent des termes liés à la COVID — et nous faisons des recherches assez vastes quand nous faisons nos vérifications pour tous les trouver — comme je viens de le mentionner, nous en avons relevé un peu plus de 2 000.

Je demanderai à notre conseiller juridique, Albert Chang, qui est également ici, de vous parler plus en détail des vérifications que nous avons faites pour repérer les noms de domaines suspects.

Monsieur Chang, vous avez la parole.

M. Albert Chang (conseiller juridique, Autorité canadienne pour les enregistrements Internet): Comme M. Holland le mentionnait, nous vérifions tous les jours tous les nouveaux noms de domaines enregistrés liés à la COVID-19, et les termes précis que nous cherchons sont « COVID », « coronavirus » et « pandémie ». À ce jour, depuis janvier, nous en avons relevé 2 000. Nous faisons des vérifications chaque jour, et leur total s'élevait à 2 041 hier.

Sur ces 2 000 noms de domaines, nous n'en avons repéré que 20 qui n'étaient pas liés à une adresse au Canada. Selon une démarche automatisée qu'on appelle le processus de validation de l'information sur le titulaire, nous envoyons un courriel aux personnes titulaires d'un nom de domaine et leur demandons de confirmer leur identité. Ils doivent alors confirmer qu'ils répondent aux critères de la présence au Canada de l'ACEI. Quand...

M. Majid Jowhari: Il y en a donc environ 21 sur 2 000 qui ne répondaient pas à vos critères?

M. Albert Chang : Exactement.

M. Majid Jowhari : Quand vous vous en rendez compte, quelle est la prochaine étape? Comment informez-vous le titulaire qu'il n'est pas autorisé à exploiter ce nom de domaine? Comment la personne qui essaie d'accéder à ce nom de domaine .ca est-elle informée qu'il s'agit d'un domaine frauduleux?

M. Albert Chang: C'est une excellente question.

Nous avons un processus de vérification, le processus de validation de l'information sur le titulaire, dont l'abréviation est VIT. Quand cela arrive, nous envoyons un courriel au titulaire du nom de domaine pour lui demander de confirmer qu'il respecte les critères de présence au Canada de l'ACEI, puis de confirmer son identité. Quand un titulaire ne répond pas à cette demande ou qu'il ne peut pas prouver qu'il respecte les critères de présence au Canada de l'ACEI, nous suspendons le nom de domaine, ce qui signifie que le site Web sera fermé. Ultimement, nous supprimerons le nom de domaine.

M. Majid Jowhari: C'est l'aspect proactif dont faisait mention le représentant du CST, mais avant même que ce nom de domaine canadien n'apparaisse sur le Web, il est déjà bloqué, donc il n'y aura pas d'incidence?

M. Albert Chang: Exactement. J'aimerais aussi souligner qu'à ce jour, nous n'avons reçu aucune plainte concernant un site Web lié à la COVID-19 qui porterait un nom de domaine .ca.

● (1550)

M. Majid Jowhari: Travaillez-vous en collaboration avec le CST, l'informez-vous quand une organisation tente de créer ainsi un nom de domaine? Communiquez-vous souvent avec le CST?

M. Albert Chang: Nous collaborons fréquemment avec le CCCS, mais je ne crois pas que nous lui communiquions chaque nom de domaine individuellement.

M. Majid Jowhari: Où publiez-vous vos résultats?

M. Albert Chang: Sur les noms de domaines, il n'y a pas...

M. Majid Jowhari: Oui.

M. Albert Chang: Ces rapports ne sont pas rendus publics.

M. Majid Jowhari: Ils ne sont pas rendus publics.

M. Albert Chang: Non.

M. Majid Jowhari: Très bien. Je vais maintenant me tourner vers les gens du CST.

Monsieur Jones, je lisais les notes d'information de la Bibliothèque du Parlement, et il y est écrit: « l'efficacité de la technologie de l'ACEI repose sur des renseignements fournis par le CCCS du Centre de la sécurité des communications. » Pouvez-vous nous parler plus en détail des technologies auxquelles vous faites allusion?

M. Scott Jones: De notre point de vue, nous sommes un service de renseignement qui alimente l'ACEI. Je laisserai nos collègues de l'ACEI vous parler de leurs méthodes plus en général, mais nos renseignements nous viennent des activités de défense du gouvernement du Canada. Quand nous observons des attaques ou des compromissions, notamment quand des pourriels ou des tentatives de hameçonnage nous sont envoyés, nous transmettons fréquemment ces indicateurs à nos partenaires, qui comprennent l'ACEI.

L'équipe de l'ACEI peut alors, avec le Bouclier canadien, prendre ces indicateurs et bloquer les menaces, de manière à ce qu'un Canadien qui essaie de cliquer sur le lien ne puisse même pas parvenir au site malicieux. C'est un avantage. Nous défendons le gouvernement du Canada de la même manière, mais c'est notre source d'information. Nous tirons vraiment notre information de nos activités de défense d'un océan à l'autre et sur les réseaux mondiaux. Nous essayons de la transmettre à nos partenaires de l'ACEI pour bien protéger les Canadiens.

M. Majid Jowhari: Je pense que je n'ai plus de temps. Merci, madame la présidente.

La présidente: Merci beaucoup.

Le prochain intervenant sera M. Lemire.

[*Français*]

Monsieur Lemire, vous avez la parole pour six minutes.

M. Sébastien Lemire: Je vous remercie, madame la présidente.

Je veux d'abord souligner la contribution du député Masse, qui nous sensibilise à cet enjeu depuis quelque temps. Il nous amène à en prendre conscience, et nous en venons à mieux le connaître. Comme parlementaire, je sens que nous avons la responsabilité d'agir pour mieux protéger nos concitoyens.

J'aimerais revenir sur l'intervention de M. Marchand. Il a mentionné notamment que, lorsque les conditions économiques et sociales se dégradaient, les attaques externes se produisaient beaucoup plus souvent. On parle ici d'une augmentation qui est de l'ordre de 600 %. De plus, ces informations sont utilisées non pas à court terme, mais davantage à moyen terme, soit à l'intérieur d'une période d'environ 18 mois.

Monsieur Marchand, vous avez dit qu'il y avait un manque sur le plan de la reddition de compte du fait que la situation actuelle facilitait l'ouverture de comptes frauduleux et les activités criminelles. Pouvez-vous nous expliquer en quoi cela représente un problème, concrètement, et quelle forme pourrait prendre la reddition de compte dans les entreprises?

M. Simon Marchand: Je vous remercie beaucoup, monsieur Lemire.

Je vais commencer par clarifier le chiffre de 600 %. Il concerne l'augmentation du nombre d'attaques liées à la COVID-19 pendant cette période très précise, et pas nécessairement l'augmentation liée à des relations de fonction économique. En cas de crise économique, il y aura évidemment une augmentation des attaques de fraudes. Les pourcentages varient.

Cela étant dit, l'absence de reddition de compte dans les entreprises qui relèvent de la compétence fédérale pose problème dans la mesure où toutes les lois actuelles — on peut penser à la Loi sur la protection des renseignements personnels et les documents électroniques, par exemple — forcent les entreprises à révéler le fait qu'elles ont été victimes d'une attaque qui leur a fait perdre de l'information. Cependant, au Canada, il n'y a présentement aucun portrait global du nombre de personnes qui sont effectivement victimes d'une utilisation de leur identité une fois que cette dernière a été volée. Comme les entreprises relevant de la compétence fédérale sont des banques et des entreprises de télécommunications, elles sont des facilitatrices de crimes l'une pour l'autre, c'est-à-dire que l'on base beaucoup la crédibilité d'une identité sur le fait que la personne possède un compte de téléphone ou un compte bancaire. Ce sont donc des entreprises qui ont accès à beaucoup d'informations de nature délicate et qui, une fois qu'un fraudeur a réussi à entrer, vont permettre à ce fraudeur de commettre de plus en plus de fraudes.

Je possède plus de 10 ans d'expérience dans le domaine de la prévention et je travaille en collaboration avec les équipes de prévention de la fraude qui sont mises sur pied dans ces entreprises. Je peux vous dire qu'une équipe de prévention d'une banque ou d'une entreprise de télécommunications n'a aucune obligation de révéler combien de comptes ont été ouverts sur une base quotidienne ou annuelle. Il n'y a même aucune obligation de contacter ou d'identifier les victimes d'un vol d'identité. Cela veut dire que vous pourriez avoir été victime d'un vol d'identité, que votre identité a pu être utilisée pour ouvrir un compte dans une entreprise de télécommunications, par exemple. L'équipe qui s'occupe des fraudes a pu détecter le vol d'identité et renverser l'opération, mais elle n'a pas l'obligation d'en aviser le citoyen, c'est-à-dire le consommateur. Ainsi, ce dernier est complètement aveugle. Personne ne sait quand son identité a été utilisée. Le citoyen ne peut pas prendre d'autres mesures pour se protéger dans l'avenir. Ce manque de reddition de compte empêche le gouvernement de poser des gestes clairs et d'encadrer les processus d'identification et d'authentification des gens qui vont ouvrir des comptes bancaires ou des comptes de téléphone.

● (1555)

M. Sébastien Lemire: Si j'ai bien compris, monsieur Marchand, il est important d'informer le Centre antifraude du Canada de ce type de situation, par exemple.

Pour une entreprise, quels sont les avantages et les désavantages d'une reddition de compte rigoureuse sur le plan des fraudes? On connaît les avantages et les désavantages que cela entraîne pour les individus, pour les citoyens, mais qu'en est-il des entreprises?

M. Simon Marchand: Le premier avantage de la reddition de compte sera de donner au gouvernement un portrait clair de la situation. Cela permettra de connaître exactement le nombre de victimes et d'orienter les mesures qui seront prises pour renforcer les mesures de sécurité dans les banques et les entreprises de télécommunications.

Cela représente certainement un poids pour les entreprises qui devront faire rapport, mais je pense que ce poids n'est pas démesuré, puisque le travail est déjà fait. Les données sont déjà connues. Il suffirait de les transmettre au législateur, à un organisme supervisé par le gouvernement qui pourrait s'occuper de présenter ces données de manière plus large et anonyme afin de permettre aux députés d'avoir accès à l'information et de savoir exactement ce qui se passe au Canada.

M. Sébastien Lemire: J'aimerais maintenant poser une question à M. Fortin, de l'Autorité des marchés financiers.

Monsieur Fortin, que pensez-vous de l'obligation qui pourrait être imposée aux compagnies d'informer le Centre antifraude des situations de fraude?

M. Jean-François Fortin: Je vous remercie de votre question, monsieur Lemire.

Cela ne relève pas nécessairement de notre compétence. Nous sommes une agence de mise en application de la loi. Je dirai tout de même que c'est une bonne idée. Je ne sais pas ce qui serait faisable sur le plan légal. Tout à l'heure, je vous écoutais parler et je me disais que, dans les moyens déployés pour prévenir la fraude, il y a évidemment le volet éducation et transparence. C'est un volet très important.

Dans un contexte comme celui-là, la question que vous avez posée à M. Marchand sur le fait d'informer les gens qui ont été victimes d'un vol d'identité ou dont les informations peuvent être utilisées par des tiers pourrait être un bon moyen de prévenir la fraude.

M. Sébastien Lemire: Pour terminer, je vais adresser ma prochaine question au représentant de la Gendarmerie royale du Canada.

L'obligation pour les compagnies de fournir une reddition de compte beaucoup plus rigoureuse vous aiderait-elle dans votre travail, si la loi était modifiée, par exemple?

[*Traduction*]

Comm. adj. Eric Slinn: C'est une question difficile. Beaucoup d'entreprises veulent protéger l'intégrité de leurs systèmes et tout et tout, donc elles ont peur de rendre des comptes, parfois.

La présidente: Malheureusement, c'est tout le temps que nous avions pour cette intervention.

La prochaine série de questions sera de six minutes, et je donne la parole à M. Masse.

La parole est à vous.

M. Brian Masse: Merci, madame la présidente.

J'aimerais remercier les témoins, vous remercier, madame la présidente, et remercier les autres membres du Comité de ce travail continu. Je vous en suis tous très reconnaissant.

L'une des choses qui a capté mon attention dans les témoignages que nous avons entendus, qui étaient excellents, c'est que nous nous fions aux médias sociaux, y compris à Facebook, pour enquêter et nous renseigner sur la façon de nous protéger contre la fraude. Cependant, Facebook a récemment lui-même été trouvé coupable et a dû payer 9 millions de dollars en amende pour avoir trompé des Canadiens. En fait, il semble qu'il ait fait « des déclarations fausses ou trompeuses sur la confidentialité des renseignements personnels des Canadiens » . Pourtant, nous dépensons des dizaines de millions de dollars des contribuables en publicités sur cette plateforme.

Je m'adresserai d'abord à M. Marchand, puisqu'il a probablement une bonne perspective des États-Unis.

Concernant la fraude chez les entreprises, Volkswagen a conclu une entente de 14,7 milliards de dollars avec les États-Unis. Au Canada, le Bureau de la concurrence lui a imposé une amende de 2,5 millions de dollars. Equifax a signé une entente de 600 millions de dollars aux États-Unis; au Canada, le Bureau de la concurrence ne lui a imposé aucune amende. Plus récemment, Facebook s'est fait imposer une amende de 5 millions de dollars aux États-Unis, puis une autre de 9,5 millions de dollars au Canada.

À mes yeux, le Bureau de la concurrence, le Commissariat à la protection de la vie privée et le CRTC sont des outils importants pour protéger les Canadiens de la fraude. Leurs pouvoirs semblent toutefois un peu obsolètes.

Pouvez-vous nous expliquer s'il y a un désalignement entre les peines imposées au Canada et celles imposées aux États-Unis, et nous dire si cela rend la responsabilisation difficile, même lorsque la fraude est commise par ce qu'on appelle des entités commerciales?

● (1600)

La présidente: Monsieur Marchand.

[*Français*]

M. Simon Marchand: Je vous remercie de la question.

Je pense que le problème n'est pas tant le manque d'harmonisation que l'absence de perception d'un risque réel de se voir infliger des frais ou une pénalité. Des frais sont prévus pour la non-divulgation d'une fuite d'informations importantes, mais encore faut-il qu'il y ait perception d'un risque réel de se faire infliger une pénalité. C'est ce qui manque ici.

Dans certains cas, on va considérer le risque de devoir payer des frais comme le prix à payer pour faire des affaires. À mon avis, ce n'est pas une approche saine ni même éthique de la gestion de risques. Les organismes de réglementation manquent de mordant actuellement. C'est peut-être cela, le problème.

[*Traduction*]

M. Brian Masse: Vous avez raison. C'est notamment en raison du coût pour les entreprises que nous nous sommes battus pour nous débarrasser des déductions fiscales pour les amendes et les peines environnementales. En effet, les amendes et les peines imposées aux entreprises étaient déductibles d'impôt au Canada, une chose contre laquelle nous nous sommes battus pendant longtemps. Les bonnes entreprises étaient pénalisées, puisque les mauvaises les déclaraient comme pertes.

Je m'adresserai maintenant à M. Holland.

Concernant votre bon travail à l'ACEI, je remarque qu'il ne semble pas y avoir de vérification. J'avais l'impression que compte tenu du fait que vous autorisez les sites .ca, ceux-ci devaient respecter des normes très élevées, à bien des égards, et c'est peut-être toujours le cas. S'il y a des abus, y a-t-il une enquête qui a lieu? Si quelqu'un s'enregistre auprès de vous et qu'au bout de trois, six ou douze mois, nous nous rendons compte qu'il utilise un nom de domaine pour des activités illicites, même si l'enregistrement s'est fait auprès de vous dans les règles au départ — presque comme un cheval de Troie —, que se passe-t-il?

M. Byron Holland: C'est une bonne question.

C'est toujours un équilibre délicat pour des organisations comme la nôtre, parce que nous sommes intrinsèquement une organisation technique. Nous gérons de l'infrastructure; nous ne surveillons pas ce qui ressort de cette infrastructure. Ce n'est absolument pas notre mandat.

Je ne veux absolument pas chercher à esquiver de notre responsabilité, mais nous intervenons sur le plan technique et non sur celui du contenu. Il y a des règles et des règlements sur la présence et les comportements au Canada; cependant, nous ne sommes pas là pour surveiller proactivement le contenu.

M. Brian Masse: Je vous remercie de cette réponse. Je ne m'attends pas à ce que vous fassiez une chose qui n'est pas de votre ressort. Je présumais seulement, peut-être naïvement, comme beaucoup de Canadiens, que les noms de domaine .ca devaient respecter une norme de protection élevée, surtout que notre gouvernement les utilise. J'en utilise un pour mon propre site, et je m'attendrais à ce que quiconque en utilise un à mauvais escient à un moment donné soit banni, pénalisé ou inscrit à une liste noire si nous voulons mettre fin à la fraude.

Si vous aviez suffisamment de ressources pour cela, est-ce une chose que votre organisation devrait faire ou est-ce que cela devrait relever d'une autre organisation? Je crois fermement que si nous voulons utiliser l'image de marque des sites .ca, nous pourrions nous en servir pour contrôler la fraude et imposer une certaine responsabilité.

Est-ce que cela devrait se faire au moyen des ressources de votre organisation ou est-ce que cela devrait relever de quelqu'un d'autre, d'une tierce partie?

M. Byron Holland: Comme la mission de notre organisation est de nature technique, je pense que la surveillance du contenu devrait être confiée à d'autres organisations conçues spécialement pour cela comme les forces de l'ordre ou même le CRTC. Nous sommes parmi les meilleurs au monde pour ce qui est des fonctions techniques d'Internet, ce qui est en grande partie attribuable à nos règles, mais il faut aussi comprendre les limites de nos fonctions.

● (1605)

M. Brian Masse: Merci, madame la présidente.

La présidente: Merci beaucoup.

C'est M. Motz qui posera la prochaine série de questions.

Vous avez cinq minutes.

M. Glen Motz: Merci, madame la présidente.

Monsieur Masse, j'ai bien aimé votre série de questions. Je pense que c'est vraiment une chose qu'il faudrait corriger dans un avenir très rapproché.

J'aimerais revenir une petite minute à M. Jones avant de m'adresser à mes amis de la GRC.

J'ai bien aimé vos observations sur votre participation à la dernière collaboration pour la mise au point d'un vaccin. Je suis curieux, est-ce le genre de partenariat dont nous devrions nous inquiéter? Faudrait-il craindre un vol de propriété intellectuelle ou de l'espionnage?

M. Scott Jones: Quand nous travaillons avec un ministère, le but est avant tout de lui faire prendre conscience des risques associés à toute forme d'activités en ligne. La seule vérité, c'est que, quelle que soit la technologie utilisée, il y aura toujours des risques.

Nous essayons vraiment proactivement de comprendre ce qui se passe, de manière à comprendre, avant tout, les activités actuelles et de faire en sorte que nos mesures de défense nous protègent bien, mais nous prodiguons aussi des conseils pour que les ministères puissent se protéger eux-mêmes.

M. Glen Motz: Merci.

Y a-t-il un déclin qui s'observe dans le nombre d'intrusions ou d'attaques de certains pays depuis le début du confinement en raison de la pandémie et le cas échéant, de quels pays?

M. Scott Jones: Nous n'avons pas vraiment observé de changement dans l'environnement de la cybersécurité. Le thème de la COVID est devenu dominant, mais le niveau d'activités est resté à peu près le même pour tous les aspects de la cybersécurité.

M. Glen Motz: Pendant la pandémie, avez-vous demandé des mesures proactives pour faire cesser ou atténuer la cyberfraude au Canada?

M. Scott Jones: Nous travaillons avec des partenaires de partout dans le monde, dont des partenaires commerciaux. Par exemple, si nous voyons des reproductions de sites Web du gouvernement du Canada, nous demandons à ce qu'ils soient démantelés.

Nous travaillons également avec nos partenaires des forces de l'ordre dès que nous soupçonnons une quelconque forme de criminalité et bien sûr, nous travaillons en étroite collaboration avec l'unité de coordination de la lutte contre la cybercriminalité de la GRC.

M. Glen Motz: Merci, monsieur Jones.

Je vais profiter du temps qu'il me reste pour me tourner du côté de mes amis de la GRC et du Centre antifraude du Canada.

Avez-vous noté une augmentation des activités frauduleuses? Je crois vous avoir entendu dire dans vos observations préliminaires que vous aviez constaté une hausse dans le contexte de la pandémie.

Comm. adj. Eric Slinn: C'est effectivement le cas.

M. Glen Motz: Est-ce que votre équipe peut compter sur un personnel complet lui permettant de bien gérer un tel accroissement?

Comm. adj. Eric Slinn: Comme bien d'autres organisations, nous avons envoyé nos employés travailler à la maison lorsque la pandémie s'est déclarée. Dans les faits, les choses se sont fort bien déroulées, car chacun a pu utiliser son ordinateur pour continuer à enregistrer les plaintes que nous recevions. Je ne crois donc pas que la pandémie ait vraiment eu un gros impact sur notre organisation. Nous ne dirons jamais non à des ressources supplémentaires pour le travail d'analyse et les mesures proactives à prendre, mais nos activités habituelles ont pu se poursuivre assez normalement.

M. Glen Motz: Ce n'est pas moi qui vais vous apprendre que le Centre antifraude du Canada se retrouve en quelque sorte sur la sellette pour bon nombre des enquêtes qui sont menées sur des fraudes majeures. Est-ce qu'il y a des postes vacants au sein de votre groupe? Êtes-vous en mesure de réagir efficacement dans tous les cas de fraude, et plus particulièrement de fraude majeure, sur lesquels vous devez enquêter?

Comm. adj. Eric Slinn: Je pense qu'il est important de préciser que le Centre antifraude du Canada est en fait un service d'enregistrement des plaintes. Ce n'est pas un groupe qui effectue des enquêtes à proprement parler. On y accomplit un certain travail d'analyse pour voir quelles tendances se dégagent ou quels nouveaux stratagèmes font leur apparition. Le Centre excelle dans ce rôle, mais doit ensuite transmettre les renseignements pertinents aux services policiers responsables, qu'il s'agisse de la GRC ou d'une autre entité.

Le Centre est donc là pour apporter un soutien en consignant les plaintes formulées pour en faire une analyse initiale avant de communiquer le tout à ceux qui vont se charger de l'enquête.

M. Glen Motz: D'après les renseignements que vous recueillez et ce que vous pouvez constater depuis le début de cette crise, diriez-vous que les médecins, les infirmières ou les travailleurs de la santé en première ligne sont tout particulièrement ciblés par les fraudeurs ou les pirates informatiques durant la pandémie actuelle?

Comm. adj. Eric Slinn: Je ne pense pas pouvoir confirmer une telle chose.

Monsieur Guy Paul, êtes-vous en mesure de répondre à cette question?

● (1610)

M. Guy Paul Larocque (officier responsable intérimaire, Centre antifraude du Canada, Gendarmerie royale du Canada): Je ne suis pas certain que le Centre antifraude soit en mesure de préciser si un groupe en particulier est ciblé. Nous pouvons cependant observer que les fraudeurs visent généralement un grand nombre de personnes à la fois. Ils ne semblent faire aucune discrimination. Chacun de nous peut devenir une victime à un moment ou à un autre.

M. Glen Motz: Nous avons pu voir un reportage sur un certain M. Julius, un pirate du Web clandestin qui a volé 1,4 million de noms.

Je suis désolé, madame la présidente. Je n'avais pas vu le carton rouge que vous me présentiez.

La présidente: Je suis désolée de devoir vous interrompre, monsieur Motz.

Les prochaines questions seront posées par Mme Lambropoulos.

Vous avez cinq minutes.

Mme Emmanuella Lambropoulos (Saint-Laurent, Lib.): Merci, madame la présidente.

Je tiens à remercier tous nos témoins de leur participation à notre séance d'aujourd'hui.

Il y a manifestement des gens qui cherchent à tirer profit de la crainte et de la vulnérabilité de certains Canadiens dans le contexte de la COVID-19. Comme ils le font toujours, ces gens-là emploient tous les moyens à leur disposition pour exploiter la situation, mais ils peuvent bien évidemment le faire cette fois-ci à partir d'un angle nouveau.

Étant donné que cette situation risque de perdurer pendant plusieurs mois, sinon un an ou deux, quelles stratégies pourrions-nous mettre de l'avant pour empêcher que des crimes semblables continuent d'être perpétrés?

C'est une question que j'adresse à tous ceux parmi nos témoins qui voudront bien y répondre.

Comm. adj. Eric Slinn: J'ai abordé la question dans mes observations préliminaires. Il vaut toujours mieux prévenir que guérir. Selon moi, on ne fera jamais assez de prévention. Bon nombre de mes collègues qui témoignent aujourd'hui ont parlé de la nécessité d'informer les gens et de leur laisser savoir quels sont les stratagèmes utilisés.

Étant donné qu'une grande partie des menaces viennent de l'étranger, il devient très difficile de faire appliquer nos lois. Il est essentiel de bien faire passer le message, et la prévention doit être au coeur de notre stratégie. Il faut informer la population des nouvelles escroqueries qui ont cours en diffusant l'information sur notre site Web et par l'entremise de nos partenaires.

Comme je l'indiquais, c'est une responsabilité partagée. Nous avons tous un rôle à jouer, mais la prévention est la pièce maîtresse.

Mme Emmanuella Lambropoulos: Merci. Je...

[*Français*]

M. Jean-François Fortin: Madame la présidente, je peux intervenir, si vous me le permettez.

La présidente: Nous vous écoutons.

M. Jean-François Fortin: Je vous remercie.

Je suis tout à fait d'accord sur ce que M. Slinn vient de dire. Selon moi, la sensibilisation et l'éducation sont très importantes. De notre côté, nous intervenons auprès des investisseurs, mais, dans ce cas-ci, on s'adresse à l'ensemble des citoyens canadiens. Il faut faire attention à ce qui nous apparaît comme des situations frauduleuses. Les gens peuvent être attirés par l'appât du gain dans certaines circonstances.

Il y a des stratagèmes où l'on fait la promotion d'une personne qui a inventé un vaccin miracle ou un médicament miracle, par exemple. La Gendarmerie royale du Canada est une équipe d'enquête, tout comme nous. La première chose à faire est d'encourager les gens à faire attention de ne pas tomber dans ce genre de stratagème frauduleux. Nous essayons d'intervenir auprès des personnes âgées, qui peuvent être contactées par téléphone ou sur les médias sociaux. C'est l'un des grands éléments. Les gouvernements ont probablement un rôle à jouer dans l'éducation de la population à cet égard.

[*Traduction*]

Mme Emmanuella Lambropoulos: Merci.

Il est bien certain aussi que l'on va chercher au cours des prochains mois à tirer profit des attentes des gens quant aux médicaments, aux vaccins et aux tests de dépistage des anticorps.

Nous en avons déjà vu des exemples à Montréal où des entreprises ont annoncé des tests semblables, alors que nous savons qu'ils n'ont pas été approuvés par Santé Canada. Quelles mesures sont prises pour protéger les Canadiens lorsqu'on découvre qu'un laboratoire, par exemple, se livre à ce genre d'activités criminelles?

[*Français*]

Ma question s'adresse à M. Fortin.

M. Jean-François Fortin: Pourriez-vous répéter la question, s'il vous plaît?

Mme Emmanuella Lambropoulos: Quelles sont les mesures prises pour protéger les Canadiens contre des entreprises, des laboratoires qui créent de faux médicaments, par exemple, et qui ne sont pas nécessairement approuvés par Santé Canada, une fois qu'on sait que ces laboratoires sont en train de faire ce genre de choses?

● (1615)

M. Jean-François Fortin: Il y a deux volets à votre question. L'un d'eux ne relève pas de notre compétence.

Si l'on est en présence d'une pure fraude comportant d'autres activités criminelles, à ce moment-là, il faudrait travailler avec nos collègues policiers, comme la Gendarmerie royale du Canada ou un autre organisme.

En ce qui nous concerne, si nous voyons ce type de promotion et que les intéressés visent à aller chercher de l'argent auprès d'investisseurs, par exemple, dans un contexte où quelqu'un aurait inventé ou trouvé un vaccin ou un médicament, nous pouvons intervenir pour faire cesser les activités, pour éviter qu'elles se poursuivent. Nous pouvons même obtenir des ordonnances d'interdiction et de blocage pour empêcher que les investisseurs perdent de l'argent. Il y a donc des moyens que nous pouvons prendre pour intervenir de façon très rapide et empêcher que la fraude se poursuive plus longtemps.

Mme Emmanuella Lambropoulos: Je vous remercie beaucoup.

La présidente: Je vous remercie beaucoup.

[*Traduction*]

Le prochain à poser ses questions sera M. Van Popta.

Vous avez cinq minutes.

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

Ma première question sera pour M. Marchand.

Merci pour votre témoignage et pour ces importantes statistiques que vous nous avez communiquées.

Vous nous avez parlé d'un accroissement des vols d'identité dans un contexte où les Canadiens sont nombreux à faire du télétravail, comme nous le faisons actuellement. Je pense que vous avez mentionné une augmentation de 600 % des tentatives d'hameçonnage. Merci encore une fois pour ces précisions, mais pourriez-vous nous indiquer ce que nous pourrions en faire dans notre rôle de législateurs? Avez-vous des recommandations précises à nous faire quant à la manière dont nous pourrions aider les Canadiens à mieux se protéger?

[*Français*]

M. Simon Marchand: Je vous remercie beaucoup de la question.

Il y a peut-être deux outils que nous pourrions regarder à court terme. En fait, le but est de fournir des outils aux entreprises qui sont exposées à ces risques. Maintenant que les fraudeurs ont accès à l'information, comment pouvons-nous donner des outils aux banques et aux entreprises de télécommunications pour empêcher les fraudeurs de les attaquer avec succès?

Les normes STIR/SHAKEN font partie de ces outils. Évidemment, selon moi, comme les Américains vont instaurer ces normes rapidement, on peut s'attendre à ce que des fraudeurs passent au nord de la frontière et viennent tirer profit d'un trou dans la législation, dans la réglementation du Canada.

Les normes STIR/SHAKEN constituent, à mon avis, un outil fondamental parce que les fraudeurs utilisent l'appropriation, ou *scooping*, pour être capables de perpétrer certaines fraudes d'identité. Ce n'est donc pas juste une question d'appels robotisés, c'est aussi une question de vol d'identité.

Quant à l'autre outil, je pense qu'il faut renforcer les règles visant l'identification des clients. En ce moment, un numéro d'assurance social, un permis de conduire ou une carte d'assurance-maladie est suffisant pour ouvrir un compte bancaire ou un compte téléphonique. Ces pièces d'identité sont désuètes. Il va falloir commencer à regarder la question de l'identité numérique, de l'identité biométrique.

Plusieurs pays sont déjà passés à ces niveaux supérieurs d'identification. Pour protéger les citoyens, cela va devenir fondamental de se demander s'il faut exiger une certaine forme d'identification biométrique, plus avancée, au moment d'ouvrir de tes comptes.

[*Traduction*]

M. Tako Van Popta: Merci beaucoup pour cette réponse.

Vous avez fait référence aux normes STIR/SHAKEN. Je sais que le CRTC a indiqué que ces normes sont « les seules solutions viables en matière d'authentification et de vérification qui pourraient permettre d'accroître la confiance des consommateurs à l'égard de l'information sur l'identité de l'appelant. »

Êtes-vous d'accord avec le CRTC à ce sujet?

M. Simon Marchand: Je ne sais pas si c'est vraiment la seule solution, mais c'est assurément un outil précieux.

Je ne pense pas que nous puissions nous permettre de renoncer à cette couche supplémentaire de sécurité et de validation. Nous ne voulons pas permettre aux fraudeurs d'ajouter cet outil à leur arsenal alors que nous pouvons — non pas sans certaines difficultés techniques — le déployer nous-mêmes pour lutter contre la fraude. Ce n'est donc pas le seul moyen à notre disposition, mais c'en est un que nous ne devrions pas négliger.

M. Tako Van Popta: Bien. Merci pour cette réponse.

Je crois que le CRTC a indiqué que ces normes deviendraient d'application obligatoire pour les entreprises de télécommunications plus tard cette année, soit en septembre 2020, si je ne m'abuse. Est-ce un échéancier réaliste?

[*Français*]

M. Simon Marchand: Malheureusement, le problème concernant les normes STIR/SHAKEN, c'est que les opérateurs ne croient pas que cette échéance sera respectée. Si je ne me trompe pas, des représentants de Rogers, de Bell et de Telus se sont présentés devant un comité de la Chambre pour demander un report d'échéance. Je pense qu'il faut être ferme et exiger le déploiement le plus rapidement possible.

Les réseaux de télécommunications au Canada sont désuets. Ils ne permettront pas une application à cent pour cent des normes STIR/SHAKEN. Par contre, je ne pense pas que ce soit une raison pour ne pas commencer le déploiement dès l'automne. Il faut juste s'assurer que les pressions exercées par le lobby des télécommunications ne poussent pas le gouvernement à reporter cette échéance jusqu'à 2021, ce qui serait une erreur, à mon avis.

● (1620)

[*Traduction*]

M. Tako Van Popta: Merci.

Peut-être pourriez-vous nous en dire plus long au sujet des limites associées aux normes STIR/SHAKEN. À titre d'exemple, il semblerait que le filtre ne fonctionne pas si un appel avec mystification de l'identité de l'appelant provient de l'extérieur du Canada ou d'une zone qui n'est pas visée par le protocole STIR/SHAKEN.

[*Français*]

M. Simon Marchand: Oui, absolument.

C'est la plus grande limitation. Cette technologie s'appliquera seulement aux appels émanant du Canada et, éventuellement, des États-Unis. Ce seront tous les pays participants qui bénéficieront de ces avantages. Toutefois, tout ce qui provient de l'extérieur ne sera pas couvert. Par contre, lorsque l'on sait qu'un appel n'a pas la certification STIR/SHAKEN, on sait qu'il s'agit d'un appel comportant un plus haut risque et qu'il faut y prêter attention.

[*Traduction*]

La présidente: Merci beaucoup.

C'est maintenant autour de M. Ehsassi.

Vous avez cinq minutes.

M. Ali Ehsassi (Willowdale, Lib.): Merci, madame la présidente.

Merci à nos témoins d'avoir bien voulu comparaître devant le Comité. J'estime que votre contribution nous est très utile.

Je vais adresser ma première question à M. Jones. Vous avez indiqué dans vos observations que le secteur de la santé fait partie de ceux qui devraient retenir notre attention étant donné qu'il est la cible d'un plus grand nombre de cyberattaques. Les plus hautes instances au Royaume-Uni et aux États-Unis ont pour leur part fait une mise en garde il y a environ un mois quant à l'extrême vulnérabilité des universités. Avez-vous noté une croissance des cyberattaques à l'encontre des universités? Est-ce que vous feriez le même constat?

M. Scott Jones: Merci pour la question.

C'est dans le contexte de la pandémie que j'ai insisté sur la situation du secteur de la santé, mais nous faisons bel et bien le nécessaire auprès de tous les secteurs faisant partie de l'infrastructure essentielle de notre économie, y compris les universités et le milieu de l'éducation dans son ensemble. Nous travaillons à partir des signalements qui nous sont faits pour tous les types de cyberactivités malveillantes. Nous nous efforçons de nous montrer proactifs en communiquant de l'information sur tout ce que nous sommes à même d'observer dans notre défense du gouvernement.

Il faut savoir que nous ne sommes pas là pour surveiller les Canadiens. Notre rôle n'est pas de surveiller ce qui se passe sur les réseaux au Canada. Nous avons pour mandat de défendre le gouvernement, et nous travaillons en fonction des cas qui nous sont signalés.

Il est bien certain que nous avons communiqué avec les universités à ce sujet. Nous leur transmettons proactivement des conseils adaptés à leur situation de telle sorte qu'elles puissent prendre les mesures nécessaires à leur protection. Nous espérons en outre pouvoir établir un partenariat avec les universités afin qu'elles communiquent avec nous lorsqu'elles observent une activité ou un incident. Nous pourrons ainsi conjuguer nos efforts.

M. Ali Ehsassi: Certainement, mais si je parle des universités, c'est notamment parce que l'Université York a été la cible il y a environ trois semaines d'une cyberattaque assez sophistiquée. Est-ce une tendance qui se dégage? Allons-nous voir de plus en plus de situations semblables?

M. Scott Jones: Nous n'avons pas suffisamment d'information pour pouvoir déterminer s'il s'agit d'une tendance, mais nous pouvons certes constater que les universités sont particulièrement vulnérables compte tenu de la nature ouverte de leur fonctionnement et du flux incessant d'étudiants qui y entrent et qui en sortent. Elles mettent en outre l'accent sur le caractère ouvert et collaboratif de leurs réseaux, ce qui les rend d'autant plus difficiles à protéger.

Pour aider les universités à mieux se défendre, nous les avons entre autres sensibilisées au travail accompli par l'Autorité canadienne pour les enregistrements Internet (ACEI). Il y a bien sûr le Bouclier canadien qui procure un avantage immédiat, mais aussi d'autres services offerts aux entreprises. Tous les Canadiens peuvent en bénéficier, et les universités ne sont pas en reste. Je crois d'ailleurs que mon collègue l'a mentionné au départ.

M. Ali Ehsassi: Vous avez indiqué que vous « interveniez » lorsqu'une organisation communique avec vous. Je suppose que c'est un terme propre à votre travail, mais qu'est-ce que cela comprend exactement? Que voulez-vous dire par intervenir? Est-ce que vous aidez les organisations à améliorer leurs systèmes? Essayez-vous de retracer la provenance des attaques? Quelles mesures prenez-vous au juste?

M. Scott Jones: J'ai sans doute été un peu vague en parlant d'intervenir. Nos actions varient en fonction du genre de cyberincident en cause et de ce qui convient ou non à l'organisation ciblée. Si le fraudeur utilise un rançongiciel typique, nous fournissons des conseils pour guider l'organisation. Nous essayons de l'aider à se remettre de l'incident en s'appuyant notamment sur les pratiques qui ont fait leurs preuves. Si l'attaque provient d'un fraudeur plus sophistiqué qui cause des torts manifestes à l'organisation, nous pouvons offrir une aide mieux adaptée à la situation. C'est le cas par exemple si un système important est touché. Nous cherchons certes alors à travailler avec un partenaire commercial pour aider l'entreprise à rebâtir ses mécanismes de défense.

Enfin, si l'intervention de l'État se révèle nécessaire, nous pouvons essayer de déterminer comment les nouveaux pouvoirs conférés au Centre de la sécurité des télécommunications peuvent nous permettre de nous porter à la défense de l'organisation visée. C'est toutefois une solution que nous réservons aux cas où il serait déraisonnable de penser que le secteur commercial peut faire le nécessaire. En fait, nous souhaitons vraiment pouvoir compter sur un secteur commercial dynamique qui est capable de défendre l'industrie canadienne, si bien que nous mettons l'accent sur les partenariats et la capacité de travailler en collaboration.

● (1625)

M. Ali Ehsassi: Merci.

Étant donné le vaste rôle consultatif que vous jouez auprès de différentes organisations d'une manière générale, pourrait-on affirmer que vous établissez ainsi la norme de diligence d'un point de vue juridique quant à savoir si les organisations adoptent bel et bien les meilleures pratiques qui soient pour se mettre à l'abri d'éventuelles pertes?

M. Scott Jones: Comme je suis ingénieur et non pas avocat, je ne suis pas certain de pouvoir me prononcer pour ce qui est de la norme de diligence.

Avec nos collègues d'Innovation, Sciences et Développement économique Canada, nous avons notamment mis en place le programme CyberSécuritaire Canada pour offrir des mesures de contrôle de base en cybersécurité qui sont accessibles aux PME. Selon moi, l'une des faiblesses du secteur commercial de la cybersécurité vient du fait que l'on offre des solutions abordables uniquement pour les entreprises dont les revenus se calculent en millions ou en milliards de dollars. Il nous faut des solutions correspondant aux moyens des petites entreprises canadiennes, et c'est ce que nous essayons de leur offrir.

[*Français*]

La présidente: Je vous remercie beaucoup.

[*Traduction*]

M. Ali Ehsassi: Je pense qu'il doit me rester une vingtaine de secondes.

Le témoin représentant...

La présidente: En fait, vous n'avez malheureusement plus de temps. Nous avons même dépassé ce qui était prévu.

[*Français*]

Je cède maintenant la parole à Mme Gaudreau.

Madame Gaudreau, vous avez la parole pour deux minutes et demie.

Mme Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Bonjour. Je vous remercie, madame la présidente.

J'ai entendu beaucoup de choses qui aident à comprendre pourquoi les gens sont inquiets. Le commissaire à la protection de la vie privée nous dit depuis un certain temps déjà que nous assistons à une crise de confiance. On parle beaucoup de l'éducation en tant que mode de prévention. Selon lui, 90 % des Canadiens ont perdu confiance quant à l'utilisation abusive de leurs données. D'ailleurs, 38 % d'entre eux croient que les entreprises respectent plus ou moins leur droit à la vie privée.

Cela étant dit, on a mentionné tantôt des mesures qu'il serait possible de prendre. M. Marchand a précisé que d'autres pays avaient des lois pour freiner les entreprises. Par exemple, une entreprise qui ne prend pas les outils nécessaires pour protéger les renseignements personnels est passible d'une sanction équivalant à 4 % de son chiffre d'affaires.

Monsieur Marchand, qu'en pensez-vous?

M. Simon Marchand: Je vous remercie de la question.

Ultimement, je pense que l'éducation est une bonne chose. Il faut en effet sensibiliser les gens aux risques auxquels ils s'exposent lorsqu'ils sont sur le Web et qu'ils répondent à des appels. Selon moi, la loi est inadéquate, mais elle touche en partie la protection des données qui sont confiées à une entreprise avec laquelle on a une relation d'affaires. Cependant, tout un pan de la législation est totalement absent, en l'occurrence le fait de s'assurer de ce qu'il advient de l'identité de la personne une fois qu'elle a fait l'erreur de fournir ses renseignements personnels ou que, à son insu, ces renseignements lui ont été volés.

Quand cette identité est utilisée pour obtenir une carte de crédit, ouvrir un compte bancaire, faire du blanchiment d'argent ou autre chose du genre, il ne faut pas seulement considérer le crime, mais également le fait que cela facilite à plus grande échelle l'activité criminelle globale, que ce soit la traite de personnes, le trafic de la drogue ou les activités terroristes. Je pense qu'il faut responsabiliser les entreprises quant à cet autre aspect. Il va falloir mettre en vigueur une loi beaucoup plus mordante pour protéger les gens une fois que leur identité est tombée dans d'autres mains.

Mme Marie-Hélène Gaudreau: D'accord.

La présidente: Je suis désolée, c'est tout le temps dont vous disposiez.

Je cède maintenant la parole à M. Masse.

[*Traduction*]

Vous avez deux minutes et demie.

M. Brian Masse: Merci, madame la présidente.

Ma question s'adresse à M. Slinn de la GRC.

Nous avons vu par le passé des cas où l'on a payé une rançon à la suite d'une cyberattaque avec atteinte à la vie privée. Un bon exemple est celui de l'Université de Calgary. En vertu des lois canadiennes, une entreprise ou une institution est-elle tenue de même reconnaître qu'elle a payé une rançon aux auteurs d'une cyberattaque, ou est-ce qu'une telle divulgation est facultative?

● (1630)

Comm. adj. Eric Slinn: C'est une bonne question. Je ne suis pas absolument certain de la réponse. Je sais que bien des entreprises privées sont réticentes, pour des raisons bien évidentes, à signaler une cyberattaque dont elles sont victimes. En effet, c'est la confiance des gens envers cette entreprise et les données en sa possession qui pourraient en souffrir. Pour être bien honnête avec vous, je ne sais pas s'il y a une obligation légale de signaler le paiement d'une rançon. De prime abord, je croirais que non, mais je me ferai un plaisir de faire les vérifications nécessaires pour pouvoir vous répondre.

M. Brian Masse: Peut-être pourriez-vous le faire également en collaboration avec nos analystes qui font un excellent travail pour nous.

Je serais vraiment curieux de le savoir. Le cas de cette université a finalement été rendu public. Cela nous ramène à ce que disait M. Marchand quant au fait que l'on ne serait même pas tenu de signaler certaines atteintes.

Il y a aussi les liens avec la cybercriminalité. Savez-vous s'il y a eu une augmentation des demandes de rançon? Est-ce qu'une base de données a été créée à ce sujet? Au fil des ans, j'ai pu constater que l'on entendait seulement parler de causes semblables, mais j'aimerais savoir si la GRC tient un registre de ceux qui se sont conformés ou qui ont volontairement admis avoir payé une rançon. J'aimerais aussi savoir si une partie de ces cyberattaques visant à exiger une rançon peuvent émaner d'autres instances gouvernementales, et M. Jones aura peut-être quelque chose à nous dire également à ce sujet.

Comm. adj. Eric Slinn: Nous conservons des données sur tous les cas qui nous sont signalés. Pour les fraudes à l'encontre de particuliers, nous savons qu'une très faible proportion des incidents sont signalés, et c'est sans doute la même chose pour les entreprises.

M. Brian Masse: Monsieur Jones, avez-vous quelque chose à dire au sujet de la possibilité que d'autres gouvernements, et surtout ceux des pays non démocratiques, aient fait des tentatives semblables dans le but d'en tirer un avantage quelconque? Est-ce qu'il y a des données qui sont compilées ou rendues publiques à ce sujet?

M. Scott Jones: S'il y a une chose qui est sûre, c'est qu'une portion très minime des cyberattaques avec demande de rançon sont signalées. Nous le savons. Lorsque les gens décident de parler, c'est généralement parce que la cybercriminalité est en cause. C'est ce que nous avons pu observer.

Nous avons analysé toutes sortes d'autres liens possibles, mais c'est principalement axé sur la cybercriminalité, et je peux vous confirmer que très peu de cas semblables sont divulgués.

M. Brian Masse: Merci beaucoup, madame la présidente.

La présidente: Merci.

Nous passons maintenant au troisième tour de questions avec M. Dreeshen pour commencer.

Vous avez cinq minutes.

M. Earl Dreeshen (Red Deer—Mountain View, PCC): Merci beaucoup, madame la présidente.

À n'en pas douter, nous avons droit aujourd'hui à des témoignages fort intéressants.

Nous ne manquons pas d'entendre certains commentaires, même en provenance du gouvernement, quant à savoir si l'on souhaite vraiment ou non faire enquête sur les fraudes à ce moment-ci. J'estime que cela ouvre sans doute la porte encore davantage aux criminels qui veulent profiter de la situation, ce qui est plutôt frustrant.

J'aimerais faire un retour en arrière. À la fin mars, le Centre pour la sécurité des télécommunications a annoncé avoir fermé des sites Web frauduleux qui avaient usurpé l'identité de l'Agence de la santé publique du Canada, de l'Agence du revenu du Canada et, plus récemment, de l'Agence des services frontaliers du Canada. Le général Vance, le chef d'état-major de la Défense de notre pays, vient de nous faire savoir que certains indices laissent croire que les adversaires du Canada comptent exploiter l'anxiété croissante causée par la pandémie actuelle.

J'adresse ma question aux gens de la GRC. Quelle forme pourraient prendre selon vous de telles attaques? De quels pays est-il question et prenons-nous actuellement des mesures pour contrer cette menace?

Comm. adj. Eric Slinn: En ce qui concerne les auteurs des menaces, ils se trouvent généralement dans des pays qui nous sont connus. Ils n'exploitent pas forcément la pandémie de COVID-19. Il pourrait s'agir d'arnaques amoureuses ou encore d'hameçonnage.

Il y a certains particuliers, certains pays, qui sont toujours des plaies, pour ainsi dire. Nous collaborons dans la mesure du possible avec nos partenaires internationaux, qu'il s'agisse du Groupe des cinq ou d'autres, qui nous aident à démanteler certains réseaux.

M. Earl Dreeshen: En août 2019, la GRC a indiqué aux médias que son enquête sur les appels frauduleux de la part de l'ARC ciblant des Canadiens était une priorité nationale, que 39 soi-disant centres d'appels dans des pays comme l'Inde avaient été fermés, et que 45 personnes à l'étranger avaient été arrêtées. En février 2020, deux Canadiens impliqués dans cette fraude ont également été arrêtés.

Quelles ressources déploie actuellement la GRC dans ce type d'enquête sur la fraude à l'étranger? Est-ce que bon nombre des escroqueries liées à la COVID-19 proviennent de l'étranger?

● (1635)

Comm. adj. Eric Slinn: Je ne peux vous indiquer les ressources exactes. Je peux toutefois vous dire, car je suis responsable des opérations policières fédérales anticriminelles, que j'ai envoyé une directive à toutes les opérations criminelles des divisions pour réorienter, comme on fait pour la pandémie, les ressources destinées à la lutte contre la criminalité financière vers la fraude liée à la COVID-19, ce qui accroîtra notre capacité de collecte de renseignements et d'application de la loi. Nous sommes conscients de notre obligation, et nous tentons d'être plus performants. Nous continuerons à travailler avec nos partenaires internationaux.

Je crois que le projet auquel vous faites référence était OCTAVIA, qui a eu lieu en février. Ce genre d'arnaque continue d'avoir lieu.

M. Earl Dreeshen: Merci beaucoup.

Madame la présidente, puis-je donner les deux minutes qu'il me reste à Mme Gray, s'il vous plaît?

La présidente: Bien sûr.

Mme Tracy Gray (Kelowna—Lake Country, PCC): Merci beaucoup. Merci, madame la présidente.

Ma question est destinée au commissaire adjoint Slinn et à l'inspecteur Larocque. Nous savons que les appels et les textos frauduleux liés à la COVID-19 se sont multipliés au cours des derniers mois et ont ciblé des Canadiens vulnérables, y compris des aînés et des Néo-Canadiens. Vous nous l'avez affirmé aujourd'hui. À quel moment ces appels seraient-ils considérés comme illégaux?

Comm. adj. Eric Slinn: Je vais demander à mon collègue de répondre, car ma réponse serait probablement trop longue.

M. Guy Paul Larocque: Merci, monsieur le commissaire.

Lorsque l'escroc tente de communiquer avec une victime potentielle, son comportement devient illégal. Il est presque impossible d'enquêter sur chaque cas, vu le volume écrasant. Comme nous l'avons expliqué plus tôt, on nous signale de nombreux cas de fraude, mais il faut regarder la tendance dans son ensemble. Voilà l'avantage que nous avons lorsque les gens rapportent un incident au centre d'appel. Nous avons alors une vue d'ensemble et pouvons transmettre les renseignements au corps policier ou au partenaire pertinent qui nous aidera par la suite.

Mme Tracy Gray: Merci.

Vous avez déjà indiqué que la fraude est à la hausse. Quels signalements fait-on à la GRC et au Centre antifraude du Canada? Avez-vous une idée du nombre d'appels qui pourraient provenir de numéros mystifiés? Pouvez-vous l'estimer?

M. Guy Paul Larocque: Non, pas en ce qui concerne les numéros mystifiés. J'ai des statistiques sur la fraude liée à la COVID-19 que nous avons commencé à compiler depuis le début de mars. La vaste majorité des plaintes reçues portaient sur des textos. Les appels étaient au troisième rang d'importance.

Mme Tracy Gray: D'accord. Je comprends...

La présidente: Madame Gray, malheureusement, votre temps de parole est échu.

Au tour maintenant de M. Erskine-Smith.

Vous avez cinq minutes.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Merci beaucoup.

J'ai une première question pour le Centre de la sécurité des télécommunications. La semaine dernière, une agence de renseignement américaine a laissé entendre que des organisations qui mènent des recherches sur la COVID-19 pourraient être ciblées par des pirates liés au gouvernement chinois. Avons-nous des preuves au Canada qui indiqueraient que cet avertissement est bien fondé?

M. Scott Jones: Nous avons émis une déclaration commune avec nos collègues du Centre de la sécurité des télécommunications pour aviser que des organisations canadiennes pouvaient s'attendre à être ciblées par non seulement... mais également par divers acteurs étrangers. L'une des choses que nous soulignons, c'est la nécessité de prendre des mesures proactives à l'égard de tout acteur qui pourrait s'intéresser à ce type d'activité ou d'information. Je crois que c'est en fait la première fois que nous avons fait une déclaration commune avec le SCRS et c'était justement pour attirer l'attention là-dessus.

M. Nathaniel Erskine-Smith: L'avertissement portait sur des menaces possibles. Ces menaces possibles se sont-elles déjà concrétisées?

M. Scott Jones: Notre objectif, c'est de nous assurer que nous transmettons les renseignements aux gens afin qu'ils puissent se protéger avant qu'un incident ait lieu...

M. Nathaniel Erskine-Smith: Il n'y a pas encore eu d'incident?

M. Scott Jones: Certaines organisations de recherche ont été compromises, et nous les aidons à minimiser les dégâts. Nous cherchons toujours qui est à l'origine des attaques.

M. Nathaniel Erskine-Smith: Avons-nous des preuves qui indiquent qu'un acteur étranger aurait tenté de pirater des recherches sur la COVID-19?

M. Scott Jones: Nous allons devoir faire des vérifications et vous revenir. Nous cherchons essentiellement à empêcher ce genre d'activité avant qu'il y ait une brèche, quel que soit l'acteur. Nous visons quiconque cible ce type d'organisations, que ce soient des criminels, des États ou des pirates individuels du monde.

M. Nathaniel Erskine-Smith: Nous avons reçu un avertissement du CST et du SCRS sur une attaque potentielle, qui aurait pu avoir lieu, mais dont vous ne semblez pas être aussi certain aujourd'hui.

● (1640)

M. Scott Jones: Nous continuons à travailler avec les organisations, mais l'une des choses que nous ne faisons pas... Nous n'avons pas de loupe géante pour examiner le Canada et l'activité sur Internet. Nos activités ne visent pas les Canadiens, ce qui fait que nous nous fions à un partenariat et à la collaboration des collègues du secteur privé, du secteur de la recherche et d'autres ordres de gouvernement qui nous signalent des cas, ce qui nous permet de brosser un tableau.

M. Nathaniel Erskine-Smith: Les acteurs des secteurs public ou privé vous ont-ils dit qu'ils avaient remarqué un incident et qu'ils voulaient votre aide à ce sujet?

M. Scott Jones: Nous avons travaillé avec certains acteurs du secteur privé. Il reste à voir si les incidents portaient sur la COVID-19 ou des travaux de recherche-développement, mais nous travaillons en ce moment avec des acteurs du secteur privé. Notre travail augmente au fur et à mesure que les gens prennent connaissance des services que nous pouvons fournir et de la nature du travail que nous pouvons réaliser ensemble. Bien sûr, au fur et à mesure que nous faisons savoir ce qui...

M. Nathaniel Erskine-Smith: En ce qui concerne la COVID-19, des établissements ou des organisations se sont-elles adressées à vous pour vous dire qu'elles ont subi un incident lié à leurs recherches sur la COVID-19?

M. Scott Jones: Oui, certaines organisations ont signalé une activité qui peut être perçue comme étant malicieuse, ou du moins suspecte. Nous travaillons avec elles pour voir si l'intention était bien malicieuse, qui en était l'auteur et si l'attaque était réussie.

M. Nathaniel Erskine-Smith: Y a-t-il eu des cas où vous avez été en mesure de déterminer la source du piratage?

M. Scott Jones: Nous signalons ces cas à la section responsable du renseignement pour en déterminer l'origine.

M. Nathaniel Erskine-Smith: Je vois.

Ma prochaine question est destinée au CST et à la GRC.

Nos électeurs ne cessent de nous signaler des arnaques. La GRC a fait des calculs et a trouvé que les particuliers arnaqués perdent environ 100 millions de dollars par année, et ce sont celles qui ont été déclarées. À mon avis, elles sont sous-déclarées, car les gens sont gênés d'en être les victimes. Nous en entendons parler constamment, et les victimes ne sont pas seulement des aînés, quoique les aînés en représentent la majorité.

Nous avons beaucoup investi dans la cybersécurité au cours des dernières années. Vous êtes les experts. Y a-t-il des mesures que prennent d'autres pays que nous ne prenons pas? Selon votre expérience et vos connaissances, y a-t-il des mesures que le gouvernement pourrait prendre pour mieux protéger notre société contre de telles activités frauduleuses?

M. Scott Jones: Je vais commencer, et ensuite je céderai la parole à mes collègues de la GRC.

La première chose que nous avons faite, c'était de donner des conseils pratiques aux Canadiens sur les mesures qu'ils peuvent prendre. Tous les pays le font. Nous avons tenté de rendre les conseils aussi accessibles que possible comme, par exemple, le programme Pensez cybersécurité.

La deuxième chose que nous avons tenté de faire, c'est de trouver des partenaires qui peuvent aider les Canadiens. L'ACEI en est un bel exemple. Ce sont des choses que tous les Canadiens peuvent considérer pour immédiatement renforcer leur cybersécurité. Les cybercriminels cherchent des proies faciles. Si leurs efforts ne sont pas rentables, ils passent ensuite à la prochaine cible, ce qui fait...

M. Nathaniel Erskine-Smith: Je comprends, et je sais qu'il me reste très peu de temps, mais le gouvernement ne peut-il rien faire, selon vous, pour vous aider à améliorer votre travail?

M. Scott Jones: Nous tentons de remplir notre mandat actuel. Tout autre élément serait une question d'orientation qui devrait probablement être débattue par le ministère et les députés.

M. Nathaniel Erskine-Smith: Merci beaucoup.

La présidente: Merci beaucoup.

La prochaine intervenante est Mme Gray.

Vous avez cinq minutes.

Mme Tracy Gray: Merci beaucoup, madame la présidente.

Ma question est destinée au commissaire adjoint.

Nous avons beaucoup parlé des mesures antifraude et de la mystification. Je me demandais s'il existe des dispositions visant ceux qui mystifient leur numéro de téléphone comme, par exemple, les télévendeurs. Pouvez-vous me confirmer que la mystification du numéro de l'appelant est toujours légale au Canada, même si ceux qui s'en servent le font avec une intention malveillante?

Comm. adj. Eric Slinn: Je vais m'en remettre à l'inspecteur Larocque, car il connaît mieux ce domaine, mais la mystification est problématique. Il est difficile de prouver où un appel a été mystifié et les logiciels utilisés rendent la tâche encore plus ardue.

Monsieur Larocque, vous pourrez peut-être nous en dire plus.

M. Guy Paul Larocque: Merci, mon commissaire.

Globalement, les appels directs étaient le premier moyen utilisé l'année dernière par les fraudeurs pour cibler les Canadiens, selon les signalements qui nous ont été faits. Il est raisonnable de présumer que la plupart de ces appels ont été mystifiés.

La difficulté est la suivante: il n'est pas illégal de mystifier un numéro, car il existe des applications pour que les gens puissent jouer des tours. Or, les criminels s'en servent pour frauder les gens. À ce moment-là, ce n'est pas la mystification qui est illégale. Ce sont les actes des fraudeurs, qui se présentent comme des représentants d'un organisme gouvernemental pour extorquer de l'argent aux Canadiens.

● (1645)

Mme Tracy Gray: Diriez-vous qu'il existe suffisamment de voies de communication entre le CRTC et la GRC pour lutter contre la fraude téléphonique pendant la pandémie actuelle?

M. Guy Paul Larocque: Nous tenons des téléconférences fréquemment pour en discuter. Nous communiquons avec nos partenaires principaux de façon hebdomadaire pour discuter des tendances actuelles et de l'évolution de la situation. Nous communiquons fréquemment avec nos partenaires habituels.

Mme Tracy Gray: Disons, par exemple, que le CRTC reçoit une plainte concernant un appel frauduleux. Vous indiquez que vous communiquez sur une base hebdomadaire. Y a-t-il une façon d'accélérer le processus lorsque vous constatez une tendance émergente ou un acte grave? Y a-t-il un protocole accéléré?

M. Guy Paul Larocque: Oui. Nos appels servent essentiellement à discuter des tendances de renseignement que nous pouvons communiquer, mais s'il y a un dossier urgent ou émergent, nous avons les protocoles nécessaires qui nous permettent de transmettre les renseignements plus rapidement. Nous le faisons le jour même ou le lendemain s'il s'agit de renseignements « chauds ».

Mme Tracy Gray: À partir du nombre de signalements faits au Centre antifraude du Canada, quel en serait le pourcentage qui fait l'objet d'enquêtes et de chefs d'accusation? Avez-vous ces chiffres?

M. Guy Paul Larocque: Malheureusement pas, parce qu'il est très difficile de quantifier ces aspects. Il faudrait demander à Statistique Canada afin de mieux comprendre ce qui a fait l'objet d'enquêtes ou de chefs d'accusation en raison des protocoles ou des politiques en matière de signalement que doivent respecter les corps policiers du pays.

Mme Tracy Gray: Pensez-vous que l'application de la loi est suffisante dans le cas des appels frauduleux?

M. Guy Paul Larocque: Il m'est très difficile de répondre à la question, parce que nous pensons toujours que nous pourrions en faire plus. Il y a toujours des choses que nous pourrions améliorer dans l'application de la loi.

La fraude est un problème collectif. Nous devons pouvoir éduquer le public. Nous pensons que l'éducation publique est l'aspect clé qui permet de freiner la fraude. Nous ne pourrons jamais empêcher les actions des fraudeurs, mais nous pouvons aider le public à reconnaître les risques associés à la fraude. De cette façon, les citoyens pourront éviter les tentatives de fraude lorsqu'ils les reconnaîtront.

Mme Tracy Gray: D'accord.

Comm. adj. Eric Slinn: L'inspecteur Larocque est gentil. Lorsque je suis venue témoigner en mars, j'ai indiqué que nous devions faire mieux, et cela vaut non seulement pour la GRC, mais également pour tous les corps policiers. Ce n'est pas un crime aguichant comme ceux liés à la drogue et ainsi de suite. En tant que communauté, nous devons faire mieux. Nous avons également fait appel à l'Association canadienne des chefs de police afin de mieux nous outiller par rapport à la fraude.

Mme Tracy Gray: Merci.

Normalement, le CST utiliserait les critères habituels d'évaluation de la sécurité de la technologie de l'information pour évaluer les propriétés affichées des produits informatiques. Bien évidemment, notre comité s'est beaucoup penché sur la question. Nous étudions notamment l'amélioration de l'accès aux réseaux pour les Canadiens, et bien sûr...

La présidente: Madame Gray, malheureusement, votre temps de parole est échu. J'en suis désolée.

Mme Tracy Gray: D'accord. Merci.

La présidente: Le prochain intervenant est M. Longfield.

Vous avez cinq minutes.

M. Lloyd Longfield (Guelph, Lib.): Merci.

Madame Gray, je crois que nous nous intéressons au même sujet, et je pourrai peut-être donner suite à vos questions.

Moi aussi, j'ai des questions pour la GRC. À Guelph, nous avons la chance d'avoir un ancien agent de la GRC, Gord Cobey, comme chef de police. Nous collaborons de près. De plus, la Police provinciale de l'Ontario dessert les environs de Guelph, ce qui fait que nous avons des corps policiers de ressorts différents qui travaillent ensemble et qui entretiennent des liens.

Monsieur Slinn, lors de votre dernière comparution, vous avez parlé de l'éducation du public et à quel point il est important de transmettre les renseignements rapidement. Si c'est possible de le dire en séance publique, pouvez-vous nous indiquer comment les corps policiers transmettent les renseignements? Y a-t-il une façon dont nous pouvons vous aider à réagir plus rapidement à la COVID-19, comme nous avons eu à le faire dans d'autres secteurs?

● (1650)

Comm. adj. Eric Slinn Je vous remercie de la question.

Je crois que le Centre antifraude du Canada est une excellente centrale pour la collecte d'une bonne partie des renseignements. Le centre réussit à transmettre les renseignements presque en temps réel ou en faire des analyses de tendances, et émet des bulletins ou des avis aux divers organismes de maintien de l'ordre. Le centre renseigne également le Service canadien de renseignements criminels, qui effectue une grande partie du suivi des renseignements.

Pour répondre à votre question, je dirais que nous avons le cadre nécessaire pour transmettre rapidement les renseignements sur la fraude aux divers organismes de maintien de l'ordre du pays. Il s'agit simplement d'accorder plus de ressources ou de moyens aux enquêtes sur la fraude. Ces enquêtes ne sont pas faciles. Les enquêtes internationales peuvent être très compliquées, et il n'est pas facile d'obtenir des éléments de preuve à l'étranger.

M. Lloyd Longfield: Ce que nous observons durant cette pandémie de COVID, c'est que les autorités en matière de santé publique communiquent très ouvertement l'information au public, ce qui aide les gens à comprendre quels sont les comportements qui contribuent à combattre la pandémie et les comportements nuisibles. Est-ce que cela ouvre la porte à une plus grande communication de l'information concernant les attaques auxquelles nous faisons face ou est-ce que cela équivaudrait à lever nos chapeaux aux méchants?

Comm. adj. Eric Slinn: Non, je ne pense pas. Je crois que c'est ce que nous nous efforçons de faire par l'intermédiaire du Centre antifraude du Canada. Peut-être que votre question est la suivante: devrions-nous diffuser l'information plus largement, faire en sorte que les organismes locaux d'application de la loi diffusent l'information sur leurs sites Web? Je pense que c'est une excellente observation, et nous pouvons certainement en tenir compte.

M. Lloyd Longfield: Merci.

Très peu de Canadiens connaissent le Centre antifraude du Canada et le travail qu'il accomplit. J'ai sous les yeux un rapport qui indique que 188 Canadiens ont été victimes d'escroqueries liées à la COVID et ont perdu au total 1,2 million de dollars entre mars et mai 2020.

Je crois que je dois m'adresser à M. Larocque. Comment ces chiffres se comparent-ils à ceux d'autres années? Je crois que, plus tôt durant la réunion, j'ai entendu dire qu'on n'avait pas enregistré une hausse très importante, mais j'aimerais savoir si ces chiffres sont plus élevés que ceux de l'année dernière à la même période?

M. Guy Paul Larocque: Oui, ils sont plus élevés. Le nombre de signalements qu'a reçu le Centre antifraude du Canada est environ 25 % plus élevé pour les quatre premiers mois de l'année.

Bien sûr, en avril, nous avons observé une augmentation des courriels d'extorsion, ce qui a contribué à accroître les chiffres. En avril uniquement, nous avons reçu environ 5 000 plaintes de plus. Pour ce qui est d'aviser le public, le Centre antifraude du Canada a publié des bulletins d'information. Nous avons publié à deux reprises un bulletin sur les escroqueries liées à la pandémie, qui a été diffusé sur notre site Web ainsi que dans les médias sociaux et qui a été transmis à un grand nombre de nos partenaires. Nous essayons d'élargir notre réseau pour faire connaître le plus possible ces escroqueries, afin que le public sache exactement quoi faire.

M. Lloyd Longfield: Merci.

Il me reste moins d'une minute, alors je vais poursuivre avec vous. Ma question porte sur la possibilité que les députés facilitent l'hameçonnage. Durant la dernière semaine, j'ai pris part à une rencontre Webex avec le maire et le député provincial, comme je le fais régulièrement, j'ai eu des rencontres dans Microsoft Teams avec des élèves d'une école secondaire, et j'ai en ce moment cette rencontre Zoom. Est-ce que nous contribuons au problème en utilisant ces applications? Est-ce que nous devrions être plus conscients de certaines choses?

M. Guy Paul Larocque: Je ne suis pas certain d'avoir bien compris la question, mais tous les efforts visant à nous éduquer les uns les autres contribueront certainement à mieux nous protéger. Nous avons commencé à mettre en oeuvre une initiative mise en place au Royaume-Uni qui s'appelle Tell2. Si chaque personne informe deux autres personnes, l'information se répandra rapidement à l'échelle du pays.

M. Lloyd Longfield: C'est très bien. Je vous remercie beaucoup.

M. Guy Paul Larocque: Je vous en prie.

La présidente: Je vous remercie beaucoup.

[*Français*]

Monsieur Savard-Tremblay, vous avez la parole pour deux minutes et demie.

M. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ): Je vous remercie, madame la présidente.

Ma question concerne les frontières. Puisque les fraudeurs américains peuvent facilement traverser la frontière, est-ce que les lois canadiennes, compte tenu particulièrement du retard dans l'application des normes STIR/SHAKEN, nous rendent particulièrement vulnérables?

Je ne sais trop à qui adresser ma question, peut-être au représentant de la Gendarmerie royale du Canada.

● (1655)

M. Simon Marchand: Je peux répondre rapidement, si vous me le permettez.

M. Simon-Pierre Savard-Tremblay: Nous vous écoutons, monsieur Marchand.

M. Simon Marchand: Sans me prononcer précisément sur les normes STIR/SHAKEN, je peux vous dire qu'au moment de l'implantation au Canada de la technologie de la carte à puce EMV, on a observé ceci. Dans les mois qui ont suivi le déploiement de la technologie et une fois que la masse critique a été atteinte, on a vu les fraudeurs passer au sud de la frontière assez rapidement pour pouvoir continuer de cloner des cartes, alors qu'ici la tendance s'estompait.

Pour les fraudeurs, la frontière n'est pas un problème. Ils vont aller là où il y a le moins de résistance et le moins d'obstacles pour commettre leurs crimes. Il est donc raisonnable de croire que, si les normes STIR/SHAKEN sont déployées aux États-Unis et pas au Canada, les fraudeurs vont venir usurper des numéros de téléphone ici.

M. Simon-Pierre Savard-Tremblay: Il y aurait donc une espèce de concurrence entre les deux systèmes, où le Canada se distinguerait par son laxisme à appliquer véritablement une norme. Ai-je bien résumé vos propos?

M. Simon Marchand: Oui. Dans tous les cas de fraude, les fraudeurs vont là où les lois sont les plus faciles à contourner et où il y a moins de réglementation. Si l'on ne déploie pas la norme ici et qu'elle est déployée au sud de la frontière, les fraudeurs viendront au Canada.

M. Simon-Pierre Savard-Tremblay: Diriez-vous qu'il y a urgence d'agir et de légiférer en la matière?

M. Simon Marchand: Comme je l'ai mentionné plus tôt, il est fondamental de passer à l'action en ce qui concerne les normes STIR/SHAKEN. En matière de sécurité de l'information et de protection des consommateurs, le Canada est en retard par rapport à l'Europe et à certains États américains. Il devient urgent d'agir, parce que si l'on ne le fait pas, on va devenir la cible d'organisations criminelles, qui vont venir attaquer les citoyens d'ici.

M. Simon-Pierre Savard-Tremblay: Madame la présidente, est-ce que j'ai le temps de formuler une autre question?

La présidente: Il vous reste 20 secondes.

M. Simon-Pierre Savard-Tremblay: D'accord. Je ne crois pas que ce soit suffisant.

Je remercie M. Marchand et l'ensemble de mes collègues.

La présidente: Je vous remercie beaucoup.

[*Traduction*]

La parole est maintenant à M. Masse.

Vous disposez de deux minutes et demie.

M. Brian Masse: Je vous remercie, madame la présidente.

Ce qui m'a vraiment irrité à propos de la situation concernant Facebook, c'est que cette entreprise a eu recours également à des applications tierces. Aux États-Unis, elle est tenue de verser 5 milliards de dollars, et au Canada, 9 millions de dollars. Cette somme ne couvre même pas les frais de publicité du gouvernement du Canada. Nous diffusons de la publicité sur la fraude sur la plateforme de cette entreprise qui a induit les Canadiens en erreur. Je pense que c'est inapproprié. Je suppose que nous disposons de très peu d'outils.

Je vais m'adresser à nouveau à M. Marchand. En ce qui concerne les normes STIR/SHAKEN, je comprends ce qu'ont fait valoir les entreprises, mais elles n'ont pas réussi à nous convaincre de ne pas mettre en œuvre ces normes, car, même si toutes les entreprises n'adoptent pas immédiatement les normes STIR/SHAKEN, celles-ci auront des avantages clairs. Ces normes permettraient de filtrer les appels téléphoniques. Les consommateurs auraient des choix et un certain pouvoir. Ils pourraient choisir de ne pas répondre à un appel qui n'a pas été filtré. Ils auraient davantage de contrôle.

Que pourrions-nous faire d'autre? Cela ne me dérange pas si vous rejetez ces idées. Vous ne me blesserez pas. Devrions-nous mettre en place une initiative énergique semblable au programme Échec au crime? Devrions-nous avoir recours au publipostage, car nous pouvons contrôler le message diffusé aux Canadiens par l'entremise du système postal? Devrions-nous envisager de mettre sur pied une commission royale d'enquête?

Plus nous consacrons d'argent à la prévention de la fraude, moins nous en consacrons à la prévention d'autres crimes. Nous ne pouvons pas passer à la vitesse supérieure dans ce pays parce qu'il semble y avoir un chaînon manquant.

M. Simon Marchand: C'est une question très vaste. Il faudrait probablement y consacrer toute une réunion de deux heures.

Nous pourrions avoir recours au publipostage — pourquoi pas? — mais nous avons vu des fraudeurs intercepter du courrier. S'ils veulent vraiment cibler quelqu'un, ils vont intercepter son courrier. Je crois que cela nous amène à penser à un autre niveau d'identification, l'identification numérique, grâce à des données biométriques, qui sont à l'épreuve des fraudeurs, car ils ne peuvent pas reproduire la voix ou une donnée biométrique. Je crois donc que c'est la prochaine étape.

Les données biométriques sont des données sensibles, alors, il est certain qu'il faudrait tenir des consultations publiques pour veiller à ce que les gens comprennent bien les paramètres qui sont établis et la façon dont les données seront gérées et manipulées.

M. Brian Masse: Merci.

Je vous remercie, madame la présidente.

Je tiens à remercier tous les groupes de témoins pour leur travail sur le sujet. Je sais qu'ils ont accompli du bon travail au fil des ans. Je l'ai constaté et je leur en suis reconnaissant.

La présidente: Je vous remercie beaucoup.

Voilà qui conclut cette troisième série de questions.

Je vous remercie tous pour votre présence aujourd'hui. Je vous remercie beaucoup pour vos témoignages.

[*Français*]

Je vous remercie beaucoup de votre patience en ce qui concerne la technologie.

● (1700)

[*Traduction*]

Je remercie également nos techniciens, nos interprètes, le greffier et nos analystes.

Nous nous réunirons à nouveau demain.

La séance est levée.