CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

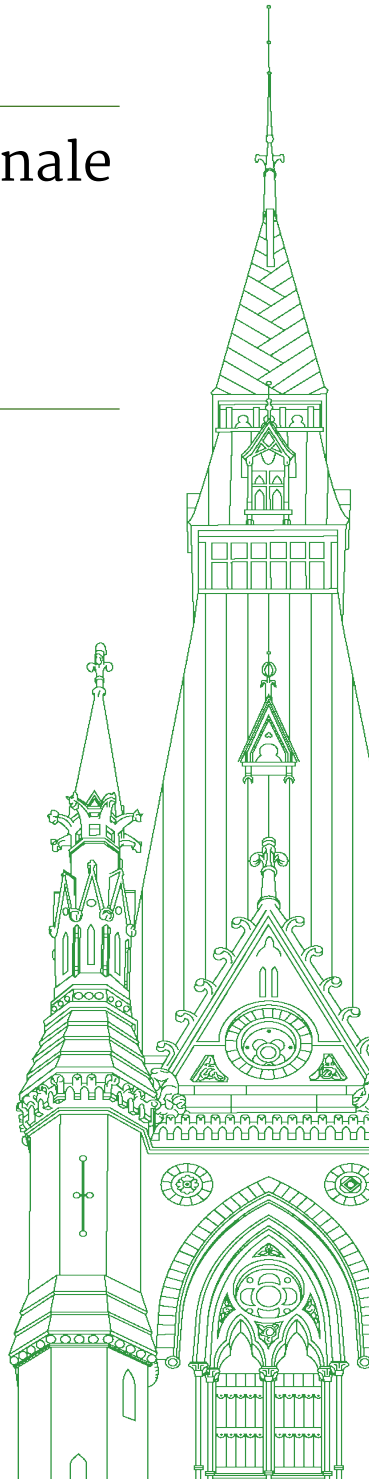
44e LÉGISLATURE, 1re SESSION

Comité permanent de la défense nationale

TÉMOIGNAGES

NUMÉRO 013

Le lundi 28 mars 2022



Président : L'honorable John McKay

Comité permanent de la défense nationale

Le lundi 28 mars 2022

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Chers collègues, il y a quorum, et donc, la séance est ouverte.

J'ai quelques points à mentionner avant que nous appelions nos témoins.

Tout d'abord, notre collègue Rob Oliphant a la COVID. Bien sûr, il était présent à la réunion de mercredi avec nous, et certains d'entre nous ont pris des photos avec lui. M. Motz, sagement apparemment, ne l'a pas fait. Pour votre propre santé, vous devriez être conscients de cela.

Vous remarquerez que notre deuxième groupe compte maintenant deux témoins, alors qu'auparavant, il en avait trois. Le troisième témoin, M. Tadej Nared, a écrit au greffier ce matin pour lui annoncer qu'il a lui aussi la COVID. Il espérait pouvoir s'en tirer, mais c'est apparemment un peu plus difficile pour lui, alors nous devrons nous assurer d'avoir l'occasion de l'inviter à nouveau.

Madame Gallant.

Mme Cheryl Gallant (Renfrew—Nipissing—Pembroke, PCC): L'inviterons-nous à revenir?

Le président: C'est simplement une question d'occasion de l'inviter à revenir. C'est là le problème.

Cela dit, je vois que nous avons deux témoins qui n'ont apparemment pas la COVID. C'est un bon début.

Nous avons Cherie Henderson, directrice adjointe des Exigences, au Service canadien du renseignement de sécurité, et M. Sami Khoury, dirigeant principal du Centre canadien pour la cybersécurité au Centre de la sécurité des télécommunications.

Monsieur Khoury, je suis intensément jaloux de cette cravate. C'est une belle cravate. Je suis sûr qu'il y a une histoire derrière.

Sur ce, je donne la parole à Mme Henderson pour sa déclaration préliminaire de cinq minutes.

Mme Cherie Henderson (directrice adjointe, Exigences, Service canadien du renseignement de sécurité): Monsieur le président, membres du Comité, bonjour.

Je m'appelle Cherie Henderson et je suis directrice adjointe des Exigences au Service canadien du renseignement de sécurité. Je vous remercie pour cette invitation à comparaître une nouvelle fois devant vous cette année afin d'aborder, cette fois-ci, la question de la cybersécurité. Je vous suis reconnaissante de cette occasion de discuter avec vous de ce sujet très important.

En tant que principal organisme du gouvernement du Canada chargé d'enquêter sur les menaces qui pèsent sur la sécurité du pays, le SCRS enquête aussi sur les cybermenaces. Il utilise donc les moyens d'enquête dont il dispose, notamment les mandats, pour recueillir des renseignements sur la manière dont des auteurs de cybermenaces exploitent le cyberespace afin de se livrer à de l'espionnage, à des actes de sabotage et à de l'ingérence contre le Canada et la population canadienne. Le SCRS collabore également avec divers partenaires canadiens et étrangers.

Son utilité réside dans sa capacité de recueillir des renseignements sur la nature et l'ampleur des cyberactivés hostiles ainsi que sur les intentions de leurs auteurs. Ces renseignements aident aussi les partenaires au sein du gouvernement du Canada à s'acquitter de leur mandat et leur permettent de mieux orienter les politiques étrangères et nationales, de protéger les entités canadiennes essentielles et de renforcer les mesures de cybersécurité générales du pays.

La Loi sur le SCRS confère aussi au Service le pouvoir d'utiliser des mesures de réduction de la menace pour limiter les cybermenaces qui pèsent sur le Canada. L'échange en temps opportun de renseignements exploitables constitue l'une des principales difficultés à surmonter dans la protection des infrastructures essentielles. À cette fin, le SCRS utilise divers moyens, comme communiquer et collaborer régulièrement avec ses partenaires. Le Service a offert à des partenaires des séances d'information portant sur les menaces d'espionnage et d'ingérence étrangère liées à des cyberintervenants étatiques ainsi que sur les effets qu'une attaque au rançongiciel commise par un groupe de cybercriminels pourrait avoir sur la sécurité nationale.

En raison de l'évolution rapide de la technologie de nos jours, le Service constate un changement d'une ampleur sans précédent dans le contexte de la menace, qui est devenu plus complexe, plus instable, moins prévisible et, par conséquent, plus difficile. Les auteurs de menace œuvrent dans l'espace virtuel, tout en tirant parti de technologies qui leur permettent de dissimuler leurs activités et leur identité. De plus, à mesure que le monde devient de plus en plus interdépendant, ils ont plus d'occasions que jamais de mener des activités malveillantes.

Outre les éléments criminels, il faut aussi tenir compte des cyberintervenants étatiques hostiles qui mènent des activités malveillantes afin de faire avancer les intérêts de leur pays, que ce soit sur le plan politique, économique, militaire ou idéologique ou sur le plan de la sécurité. Les cyberintervenants étatiques hostiles cherchent à compromettre des systèmes informatiques en manipulant leurs utilisateurs ou en exploitant des failles de sécurité pour avoir accès à des secrets commerciaux. Ils peuvent aussi chercher à atteindre divers objectifs par la perturbation d'infrastructures ou de services essentiels. Les attaques de ce genre ne vont pas disparaître. En fait, elles sont en plein essor.

Depuis de nombreuses années, le SCRS constate des cybermenaces persistantes et sophistiquées parrainées par des États, dont la fréquence et la complexité ne cessent d'augmenter. Des entreprises canadiennes de presque tous les secteurs ont été visées et compromises.

Un accès non autorisé et malveillant à des infrastructures essentielles peut avoir des conséquences dramatiques sur la sécurité de la population canadienne. Pensez à tous les systèmes que nous utilisons dans nos vies, notamment ceux qui soutiennent les télécommunications, les chaînes d'approvisionnement, les transports et les secteurs de l'énergie, de la santé et des finances. Toute ingérence dans ces systèmes peut avoir des effets imprévus sur notre sécurité et notre bien-être ainsi que sur la sécurité nationale.

En raison de la pandémie, un nombre sans précédent de gens travaille à la maison, où les conditions sont moins sécuritaires. Cette nouvelle norme de travail accroît le risque d'exposition à des cyberactivités malveillantes visant des réseaux et des informations sensibles. Nous avons tous entendu parler d'attaques au rançongiciel commises par des cybercriminels contre des entreprises et des organismes publics, notamment des hôpitaux au plus fort de la pandémie.

Compte tenu de la nature mondiale des menaces qui pèsent sur la sécurité et de leur caractère toujours plus interdépendant, le SCRS ne peut pas remplir son mandat en vase clos. Les membres de l'appareil de la sécurité et du renseignement font preuve d'une formidable collaboration et travaillent à fournir au gouvernement du Canada les meilleurs renseignements et avis possible au sujet des cybermenaces.

Dans l'actuel contexte mondial de la menace, les différents partenaires doivent utiliser leur mandat et les pouvoirs qui leur sont conférés par la loi pour protéger le Canada et la population canadienne. C'est exactement ce que le SCRS fait et continuera de faire.

● (1535)

Merci de m'avoir donné l'occasion de prendre la parole aujourd'hui. Je répondrai avec plaisir à vos questions.

Le président: Merci, madame Henderson.

Nous accueillons maintenant M. Khoury, pour cinq minutes.

Allez-y, s'il vous plaît.

M. Sami Khoury (dirigeant principal, Centre Canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Merci, monsieur le président, et membres du Comité, de m'avoir invité à comparaître aujourd'hui.

Je m'appelle Sami Khoury. Je suis le dirigeant principal du Centre canadien de la cybersécurité, souvent appelé le cybercentre du Centre de la sécurité des télécommunications.

Le CST, qui relève de la ministre de la Défense nationale, est l'un des principaux organismes de sécurité et de renseignement du Canada, avec le mandat de cybersécurité à cinq volets découlant de la Loi sur le Centre de la sécurité des communications adoptée en 2019. Nous utilisons notre expertise technique dans les cinq volets de notre mandat, et nous le faisons pour assurer la sécurité des Canadiens.

[*Français*]

J'aimerais vous offrir un aperçu du contexte actuel des cybermenaces.

Il est évident que, globalement, les cybermenaces évoluent rapidement. Le nombre et le degré de sophistication des cyberincidents, y compris ceux qui sont liés aux infrastructures essentielles, continuent de s'accroître.

De plus en plus d'activités quotidiennes importantes se font maintenant en ligne, notamment les transactions bancaires, les services gouvernementaux, les services de santé, le commerce et l'éducation, ce qui les expose à des menaces. Nous avons pu le constater lorsque la pandémie de la COVID-19 nous a obligés à dépendre davantage de l'infrastructure numérique. Les auteurs de menaces en ont profité en multipliant les tentatives d'exploitation des vulnérabilités humaines et technologiques.

[*Traduction*]

En plus de cette augmentation des cyberincidents, j'aimerais souligner certaines des tendances particulières que nous avons observées.

Nous avons déterminé que la cybercriminalité demeure la menace la plus susceptible de toucher les Canadiens. Aujourd'hui et à l'avenir, les particuliers et les organisations du Canada continueront d'être confrontés à la fraude en ligne et à des tentatives de vol de renseignements personnels, financiers et d'entreprise. Nous avons également déterminé que les rançongiciels visant le Canada continueront de cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles. La protection de ces organisations et réseaux est essentielle à la productivité et à la compétitivité des entreprises canadiennes et cruciale pour la défense du Canada. Si la cybercriminalité est la menace la plus susceptible de toucher les Canadiens et les entreprises canadiennes, les cyberprogrammes parrainés par la Chine, la Russie, la Corée du Nord et l'Iran constituent la plus grande menace stratégique pour le Canada.

● (1540)

[*Français*]

Pour en savoir plus sur les cybermenaces qui pèsent sur le Canada, je vous invite à lire le document « Évaluation des cybermenaces nationales 2020 », publié par le CST.

Je suis conscient que l'invasion russe de l'Ukraine préoccupe actuellement le Comité. Je ne peux pas parler de nos opérations particulières dans le cadre de cette présentation, mais je peux confirmer que nous suivons de près les activités de cybermenace associées à ces manœuvres militaires.

[*Traduction*]

Aujourd'hui, nous n'avons pas connaissance de menaces précises contre les organisations canadiennes liées aux événements en Ukraine et dans les environs. Mais à mesure que la situation évolue, je peux vous assurer que nous continuons à surveiller le contexte des cybermenaces au Canada et dans le monde, y compris les cybermenaces visant les réseaux d'infrastructures essentielles.

Bien que les tendances que j'ai décrites aujourd'hui semblent assez inquiétantes, le cybercentre travaille sans relâche avec les intervenants et établit de solides partenariats dans tout le Canada pour créer une conscience commune du contexte des menaces et promouvoir les mesures nécessaires pour s'en protéger et s'en défendre.

[*Français*]

Nous continuons également de publier des avis et des conseils, liés en grande partie aux cybermenaces russes, qui permettront aux Canadiens et aux entreprises canadiennes d'améliorer leurs pratiques en matière de cybersécurité.

Le CST communique également du renseignement important sur les cybermenaces à l'Ukraine pour lui permettre de mieux défendre ses réseaux.

Aussi, nous collaborons avec le ministère de la Défense nationale et les Forces armées canadiennes dans le cadre de mesures qui favorisent la coopération sur le plan du renseignement et qui soutiennent la cybersécurité.

[*Traduction*]

Comme l'environnement de la cybermenace au Canada évolue rapidement, nous avons tous un rôle. La cybersécurité est une préoccupation touchant « l'ensemble de la société ». Il faudra toute notre expertise et notre collaboration pour protéger le Canada et les Canadiens.

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

Le président: Merci, monsieur Khoury.

Merci, madame Henderson.

Nous passons maintenant à notre tour de six minutes.

Madame Findlay, allez-y, s'il vous plaît.

L'hon. Kerry-Lynne Findlay (Surrey-Sud—White Rock, PCC): Merci, monsieur le président.

Merci d'être des nôtres aujourd'hui. Nous vous en sommes très reconnaissants.

Madame Henderson, à quel type de cybermenaces le Canada est-il confronté quotidiennement et quelle proportion de ces attaques est parrainée par l'État?

Mme Cherie Henderson: D'après ce que je comprends actuellement, le Canada subit quotidiennement des milliers de cyberattaques dans tout le pays, et de nombreuses organisations font l'objet de ces attaques. Je n'ai pas de statistiques précises sur les pays d'où proviennent ces attaques. Je laisse cela à mon collègue, M. Khouri, mais je peux dire... ou la quantité... permettez-moi de corriger cela: je ne connais pas le nombre provenant de chaque pays. M. Khouri a peut-être de meilleures statistiques à ce sujet.

Ce que je peux dire, c'est que nous utilisons certainement tous les outils dont nous disposons pour faire enquête sur ces menaces...

L'hon. Kerry-Lynne Findlay: Je comprends cela, mais lorsque j'étais ministre du Revenu national — c'était il y a quelques années maintenant, les libéraux sont heureux de l'apprendre — nous avons subi des milliers de cyberattaques quotidiennes à l'Agence du revenu du Canada. On m'a dit qu'elles ont proliféré depuis et qu'elles sont beaucoup, beaucoup plus nombreuses. Êtes-vous d'accord pour dire que c'est un problème qui prend de l'ampleur?

Mme Cherie Henderson: Oui, tout à fait. C'est un problème qui prend de plus en plus d'ampleur, et nous devons tous en être conscients.

Au fur et à mesure que nous progressons dans le domaine de la technologie, il y a beaucoup plus de cyberactivité dans ce domaine et beaucoup plus de cyberacteurs. Historiquement, nous nous sommes concentrés sur les attaques parrainées par l'État, mais avec la prolifération des outils, beaucoup plus d'acteurs sont entrés dans l'arène.

L'hon. Kerry-Lynne Findlay: Que l'un d'entre vous réponde à cette question: quels secteurs de l'économie canadienne sont, selon vous, les plus vulnérables aux cyberattaques?

Mme Cherie Henderson: Je peux commencer.

C'est l'une des choses qui me préoccupent beaucoup. Le service enquête et essaie de faire beaucoup de sensibilisation pour informer nos industries de recherche et nos entreprises qui participent à la recherche et au développement. Comme vous le savez, le Canada est un chef de file en matière de recherche et développement et possède une grande quantité de propriété intellectuelle très précieuse.

De nombreux pays aimeraient mettre la main sur cette recherche sans avoir à y consacrer de l'argent et des investissements. Pour toutes ces industries, nous nous efforçons de sensibiliser les gens afin qu'ils puissent se protéger.

Nous faisons également très attention à nos infrastructures essentielles. Les infrastructures essentielles sont indispensables au maintien de notre vie quotidienne, et c'est un autre domaine qui est très vulnérable et qui devrait assurer un très haut niveau de protection et de sensibilisation.

Je peux peut-être passer la parole à M. Khoury pour d'autres remarques.

● (1545)

L'hon. Kerry-Lynne Findlay: Avez-vous des remarques à faire à ce sujet, monsieur Khoury, sur les secteurs les plus vulnérables de l'économie canadienne?

M. Sami Khoury: Je vous remercie de cette question.

Du point de vue du cybercentre, notre priorité est de défendre le Canada contre toutes sortes de cyberincidents, quel que soit le secteur, mais nous accordons une attention particulière aux secteurs des infrastructures essentielles pour nous assurer qu'ils disposent des outils nécessaires pour se protéger.

L'hon. Kerry-Lynne Findlay: Je ne suis pas sûre, mais M. Khoury est peut-être mieux placé pour répondre à cette question. En ce qui concerne les cybermenaces, comment évaluez-vous les capacités de cyberattaque de ces acteurs étatiques: la Chine, la Russie, la Corée du Nord et l'Iran?

M. Sami Khoury: Dans notre évaluation nationale de la cybermenace en 2020, nous avons indiqué que les capacités de ces quatre pays — la Russie, la Chine, la Corée du Nord et l'Iran — sont des programmes parrainés par l'État qui représentent la plus grande menace stratégique pour le Canada. Il est difficile de comparer l'un à l'autre, mais je dirais que, dans le contexte actuel, nous devons tenir compte des tensions géopolitiques et des cybermenaces russes.

L'hon. Kerry-Lynne Findlay: Comment évaluez-vous une cybermenace posée par Anonymous?

M. Sami Khoury: Les Anonymous, comme beaucoup d'autres organisations, représentent un certain niveau de menace pour la cybersécurité d'un pays. Nous avons vu certains d'entre eux s'aligner sur la Russie et d'autres sur la cause ukrainienne dans le contexte de la tension géopolitique actuelle.

Encore une fois, nous tirons le maximum d'enseignements de tous les incidents, et c'est pourquoi nous encourageons toutes les victimes à nous les signaler, afin que nous puissions apprendre et promouvoir de nouvelles pratiques en matière de cybersécurité. Nous prenons tous ces renseignements, nous les digérons et nous publions de nouveaux conseils et orientations.

L'hon. Kerry-Lynne Findlay: Savez-vous que Huawei a été impliqué dans une tentative de piratage des télécommunications australiennes, l'Australie étant bien sûr membre de notre Groupe des cinq?

M. Sami Khoury: Je vais laisser à l'Australie le soin de commenter la nature de l'incident qui...

L'hon. Kerry-Lynne Findlay: Je ne vous ai pas demandé la nature de l'incident. J'ai demandé si vous étiez au courant que cela s'était produit.

M. Sami Khoury: Nous suivons les activités de Huawei et d'autres exploitants de services de télécommunications dans le monde, et cela nous aide à assurer la sécurité de l'infrastructure canadienne des télécommunications.

L'hon. Kerry-Lynne Findlay: Savez-vous également que China Telecom Americas, China Unicom Americas et ComNet ont également été accusés d'espionnage pour le gouvernement de la Chine?

M. Sami Khoury: Encore une fois, nous suivons tous ces rapports. Ils aident à formuler la position du cybercentre sur la façon de protéger l'infrastructure canadienne des télécommunications.

L'hon. Kerry-Lynne Findlay: Madame Henderson, êtes-vous au courant de la loi chinoise sur le renseignement national qui oblige les sociétés d'État et les autres sociétés à recueillir des renseignements pour l'État chinois sur demande?

Mme Cherie Henderson: Oui, je suis au courant de cette loi. Il s'agit d'une loi qui a été adoptée en 2017, si je ne m'abuse. Cette loi oblige effectivement toutes les entreprises chinoises à soutenir toutes les exigences du gouvernement chinois.

L'hon. Kerry-Lynne Findlay: Merci.

Le président: Merci, madame Findlay.

Madame Lambropoulos, vous avez six minutes, s'il vous plaît.

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

J'aimerais remercier nos deux témoins d'être ici pour répondre à nos questions aujourd'hui.

Madame Henderson, je vais commencer par vous. Si vous pensez que M. Khoury peut répondre à certaines des questions de façon un peu plus approfondie, j'aimerais beaucoup que vous les lui transmettiez également.

Vous avez mentionné que le raffinement des cyberattaques a augmenté au fil des ans, que les choses vont probablement continuer à évoluer dans ce sens et qu'il y en a de plus en plus chaque fois. Pensez-vous que le SCRS et ses partenaires disposent des outils nécessaires pour faire face à ces nouvelles menaces sophistiquées? Étant donné que les choses deviennent de plus en plus sophistiquées au fil du temps, pensez-vous que ces organisations, y compris la vôtre, seront en mesure de continuer à répondre à ces menaces et à les contrer?

Mme Cherie Henderson: C'est une très bonne question. Je vous en remercie.

Il est très important, comme je pense que M. Khoury et moi-même l'avons dit, que chaque organisme ayant des responsabilités en matière de sécurité nationale soit en mesure d'enquêter sur ces attaques en utilisant les outils que chaque organisme apporte à la lutte, en un sens. C'est pourquoi il est extrêmement important que nous coopérions tous afin de remplir chacun de nos mandats. C'est une telle union que nous pourrons combattre avec succès l'environnement de menace actuel auquel nous sommes confrontés.

Il est également important, je crois, que tous les Canadiens et toutes les sociétés et industries soient très conscients de la cybermenace et puissent prendre les précautions et les mesures nécessaires pour se protéger. Je pense qu'il est également important, au fur et à mesure que nous avançons, de nous assurer que nous nous attachions continuellement à déterminer si nous avons besoin de nouveaux outils et s'il existe des moyens de nous améliorer. C'est pourquoi nous parlons de moderniser, par exemple, le SCRS pour voir s'il y a de nouveaux outils que nous pourrions utiliser pour aider à protéger le Canada et les Canadiens à l'avenir.

Je répète qu'il est extrêmement important que chaque organisme coopère et nous communiquons très bien ensemble pour nous assurer que nous utilisons tous les outils dont nous disposons à l'heure actuelle.

● (1550)

Mme Emmanuella Lambropoulos: Merci beaucoup.

Monsieur Khoury, avez-vous quelque chose à ajouter à cela?

M. Sami Khoury: Je fais écho aux propos de Mme Henderson. Il s'agit d'un effort de toute la société. Nous apprenons beaucoup de tous les cyberincidents au sein du gouvernement. À partir de cette expérience, nous transmettons cette information au secteur public, au secteur privé et aux citoyens canadiens en général, et nous réduisons collectivement le coût de la cybersécurité.

Mme Emmanuella Lambropoulos: Merci beaucoup.

Dans la foulée de ce que vous venez de mentionner, soit la modernisation de la Loi sur le SCRS, je me demande s'il y a quelque chose que vous aimeriez mentionner ici — sans nécessairement compromettre la cybersécurité canadienne — que nous devrions examiner, même dans notre rapport et nos propres recommandations au sein du Comité de la défense. Par ailleurs, existe-t-il actuellement des obstacles qui nous empêchent d'améliorer la situation actuelle au Canada?

Mme Cherie Henderson: Il n'y a pas d'obstacle, en soi, qui nous en empêcherait. Je crois que nous devons nous assurer que, premièrement, nous avons tous les outils nécessaires et que nous sommes pleinement conscients de l'évolution de la technologie et de son développement. Ensuite, il est également extrêmement important que nous trouvions un équilibre entre les droits et la vie privée des Canadiens au fur et à mesure que nous avançons.

C'est une façon très délicate d'aller de l'avant — s'assurer que nous avons les outils pour attraper les criminels, mais aussi protéger les droits des Canadiens. Il faut un certain nombre de recherches et d'études pour veiller à ce que nous arrivions là où il se doit et que nous ayons ce dont nous avons besoin pour protéger notre sécurité nationale.

Mme Emmanuella Lambropoulos: Monsieur Khoury, avez-vous des recommandations pour cette étude particulière que vous aimeriez partager avec nous aujourd'hui?

M. Sami Khoury: Du point de vue du cybercentre, le travail d'équipe à l'échelle du gouvernement et du Canada est extrêmement important. Le signalement des cyberincidents sera très important, afin que nous tirions des leçons de tous les incidents qui se produisent et que nous puissions améliorer la cybersécurité du pays.

Mme Emmanuella Lambropoulos: Merci beaucoup.

Monsieur le président, combien de temps me reste-t-il?

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

Mme Emmanuella Lambropoulos: Ma prochaine question appartient à une tout autre catégorie et concerne un peu plus la Russie.

Nous savons qu'une grande partie des cybermenaces à notre endroit proviennent de la Russie. De nombreuses cyberattaques proviennent de Russie. Je veux savoir comment ils sont capables de nier qu'ils commettent de tels actes. Qui utilisent-ils pour atteindre et influencer les Canadiens de quelque façon que ce soit pour qu'ils pensent d'une certaine façon?

Mme Cherie Henderson: Je dirais que la Russie est un acteur de cybermenace extrêmement capable. Nous savons que les services de renseignement russes se sont déjà livrés à des campagnes de désinformation pour discréditer et créer des divisions en Occident, pour promouvoir l'influence de la Russie à l'étranger et pour faire pression pour obtenir la fin des sanctions occidentales. Nous savons également que la Russie recueille secrètement des renseignements politico-économico-militaires au Canada par le biais d'activités de menace ciblées à l'appui de ses propres intérêts.

Je ne peux pas vous parler de mesures précises, mais je peux vous dire que le SCRS utilise toute la gamme d'outils à sa disposition pour contrer ces activités russes.

● (1555)

Le président: Merci, madame Lambropoulos.

Nous avons maintenant Mme Normandin, pour six minutes, s'il vous plaît.

[*Français*]

Mme Christine Normandin (Saint-Jean, BQ): Merci beaucoup, monsieur le président.

Madame Henderson et monsieur Khoury, je vous remercie de votre présence.

Ma première question s'adresse à Mme Henderson, mais si vous voulez y répondre, monsieur Khoury, je vous prie de le faire.

J'aimerais d'abord savoir si le Canada a la capacité de suivre la trace de la cryptomonnaie en provenance ou à destination de groupes illégaux ou terroristes.

Mme Cherie Henderson: Je vous remercie de votre question, mais, personnellement, je n'ai pas l'information nécessaire pour y répondre.

[*Traduction*]

Je vous dirigerais vers le CANAFE, qui serait le meilleur service pour répondre à ce type de question.

[*Français*]

Mme Christine Normandin: Monsieur Khoury, est-ce que vous voulez ajouter quelque chose?

M. Sami Khoury: J'allais justement suggérer le Centre d'analyse des opérations et déclarations financières du Canada, soit le CANAFE, qui a la capacité de mieux répondre à cette question.

Mme Christine Normandin: Je vous remercie.

Cela m'amène à une autre question. À votre avis, le CST aussi bien que le SCRS travaillent-ils trop en vase clos? J'inclus là-dedans la question des forces armées. Y a-t-il suffisamment de communications entre les deux?

M. Sami Khoury: Je vous remercie de cette question.

Absolument. Nous sommes en contact constant avec nos voisins, avec le SCRS et avec nos collègues des Forces armées canadiennes. Nous les appuyons dans deux de leurs missions, soit Unifier et Reassurance. Il existe donc de bons canaux d'échange d'informations entre ces deux entités et nous. Nous travaillons aussi avec le reste du gouvernement pour atténuer les risques qui se présentent contre le gouvernement fédéral et avec nos partenaires dans les provinces et dans le domaine privé.

Mme Christine Normandin: J'ai une question peut-être plus pointue sur ce sujet.

Madame Henderson, est-ce que vous êtes capable de nous donner un aperçu du rôle de la Task Force Osprey au sein du CST? Non, ce serait plus pour vous, monsieur Khoury. Pourriez-vous nous donner un peu plus d'informations sur le rôle de la Task Force Osprey?

M. Sami Khoury: Je pense que je vais vous diriger plus vers les Forces armées canadiennes pour avoir une réponse à cette question. Si elles ne peuvent pas y répondre, je vous pourrai vous fournir une réponse.

Mme Christine Normandin: Je comprends que c'est quand même une partie de l'organisation des Forces qui travaille au sein du CST. Ai-je raison?

M. Sami Khoury: J'aimerais mieux vous le confirmer par écrit, si vous me le permettez.

Mme Christine Normandin: Je vous en remercie.

Ma prochaine question s'adresse à l'un et l'autre des témoins.

J'aimerais savoir s'il est arrivé que le Canada ait été contraint de privatiser, d'une certaine façon, par manque de compétence, de personnel ou de matériel, certains de ses services pour s'assurer qu'ils sont à la hauteur. Est-ce déjà arrivé?

M. Sami Khoury: Le Centre canadien pour la cybersécurité joue un rôle important dans l'intégrité de nos chaînes d'approvisionnement. Si nous devons examiner de manière détaillée la privatisation d'un service — je parle du gouvernement fédéral à ce moment-là —, nous avons un rôle à jouer dans l'évaluation de ce programme.

Si vous parlez d'une menace intérieure, je vous dirigerais plutôt vers Mme Henderson pour qu'elle donne plus de nuances à cette réponse.

Mme Christine Normandin: En fait, ma question visait davantage à savoir si le CST ou le SCRS avait déjà eu recours au secteur privé dans le cadre de certaines de leurs opérations pour combler, peut-être, des lacunes au sein de leurs services.

M. Sami Khoury: C'est sûr que nous travaillons avec le secteur privé dans beaucoup de dossiers. Dans certains cas, ils partagent avec nous des détails des cybermenaces. Il s'agit donc plutôt d'une relation complémentaire, mais, dans le cas de cyberincidents, il y a des choses que le CST ou le Centre canadien pour la cybersécurité ne font pas.

C'est alors le rôle du secteur privé de venir aider une victime, par exemple, à se replacer.

Mme Christine Normandin: C'est parfait, merci.

J'ai une question supplémentaire qui s'adresse plutôt à Mme Henderson, mais, monsieur Khoury, vous voudrez peut-être aussi y répondre.

Depuis quelques années, il y a eu des discussions sur la possibilité de mettre sur pied un service du renseignement extérieur. Le service du renseignement sert beaucoup plus à des évaluations locales. La partie humaine du service de renseignement n'existe pas sur le territoire étranger.

Serait-il pertinent de considérer cette idée dans le contexte actuel de la guerre en Ukraine et des nouvelles menaces que connaît le Canada, c'est-à-dire d'avoir un modèle basé, par exemple, sur la CIA?

● (1600)

Mme Cherie Henderson: Je vous remercie de cette question, à laquelle je vais répondre en anglais.

[*Traduction*]

C'est une autre question très intéressante. Je dirais qu'en vertu de l'article 12 de la Loi sur le SCRS, nous pouvons mener une enquête à l'étranger s'il est déterminé que notre sécurité nationale est menacée. Ce que nous ne pouvons pas faire à l'étranger, c'est toute activité en vertu de l'article 16 de la Loi sur le SCRS, qui nous permet de recueillir des renseignements politiques ou économiques à l'appui de la défense nationale ou des affaires étrangères.

En vertu de l'article 12 — les menaces à la sécurité du Canada —, ce n'est pas un problème. C'est en vertu de l'article 16 que nous devons rester au Canada pour recueillir des renseignements.

[*Français*]

Mme Christine Normandin: Je vous remercie.

J'aurai des questions de suivi à mon prochain tour, monsieur le président.

[*Traduction*]

Le président: Je vous remercie. Nous allons devoir en rester là.

Madame Mathyssen, vous avez six minutes. Allez-y, s'il vous plaît.

Mme Lindsay Mathyssen (London—Fanshawe, NPD): Merci beaucoup aux deux témoins.

Je vous remercie, monsieur le président.

Nous avons, bien sûr, vu l'armement des médias sociaux. Ici, au Canada, des groupes de trolls en ligne ont été créés. On a semé la méfiance, la haine et les théories du complot en ligne. Il y a eu une ingérence éventuelle dans nos élections, et certainement dans la société en général.

Le NPD a demandé au gouvernement de réunir un groupe de travail national pour contrer la haine en ligne et protéger la sécurité publique. De quelle manière pouvons-nous rendre les plateformes de médias sociaux juridiquement responsables de l'aggravation de la méfiance, de l'ingérence dans les élections et des complots en ligne, et de l'élimination de l'extrémisme avant qu'il ne puisse causer de réels dommages?

M. Sami Khoury: Dans l'*Évaluation des cybermenaces nationales 2020*, nous avons mentionné qu'Internet était à la croisée des chemins et que nous observons de plus en plus de désinformation et de tromperies qui ne se limitent pas aux campagnes politiques ou aux périodes électorales. Nous assistons à une utilisation beaucoup plus large de la désinformation et des tromperies. Nous l'observons sans aucun doute dans le contexte du conflit russo-ukrainien.

Du point de vue du cybercentre, nous dénonçons ces activités. Nous ne sommes pas un organe de réglementation, donc nous ne sommes pas ici pour commenter les plateformes de médias sociaux elles-mêmes. Il s'agit plutôt de savoir comment nous pouvons travailler avec les Canadiens, en général, qu'ils sachent repérer la désinformation et les tromperies, pour qu'ils soient des lecteurs informés, s'assurant qu'ils obtiennent les nouvelles de sources fiables — tant du point de vue des nouvelles que de celui des TI — et que le domaine qui héberge l'information est également fiable.

Nous avons publié un bulletin très récemment, il y a deux ou trois semaines, portant précisément sur la désinformation, les tromperies et la cybermalveillance. Nous espérons que les gens le liront et y puiseront de précieux renseignements qui les aideront dans leur collecte d'information ou dans leur présence sur les médias sociaux.

Mme Lindsay Mathyssen: Vous faites donc porter la responsabilité aux utilisateurs eux-mêmes. Vous ne voyez aucun rôle que les entreprises de médias sociaux doivent assumer dans ce domaine. Est-ce bien ce que vous dites?

M. Sami Khoury: Du point de vue du cybercentre, notre rôle est de défendre le pays contre les incidents de cybersécurité et de donner aux Canadiens et aux entreprises canadiennes les outils nécessaires pour élever la barre en matière de cybersécurité.

Nous ne sommes pas une agence ou un centre responsable de la réglementation des médias sociaux. Je m'en remets à d'autres organismes gouvernementaux pour répondre à cet aspect de la question.

Mme Lindsay Mathyssen: D'accord.

Madame Henderson, dites-vous la même chose que M. Khoury, ou quelque chose de légèrement différent?

Mme Cherie Henderson: Je crois que M. Khoury a répondu à la question. Aucun de nos deux organismes n'est ici pour réglementer les plateformes de médias sociaux. C'est la responsabilité des autres ministères et peut-être de la société dans son ensemble, quant à la façon de gérer cette situation.

● (1605)

Mme Lindsay Mathyssen: D'accord. Changeons un peu de sujet, en ce qui concerne le recrutement et la rétention, nous avons certainement beaucoup entendu parler des défis que rencontrent les Forces armées canadiennes à cet égard.

Pouvez-vous nous dire si le SCRS a fait face à des défis semblables pour ce qui est de recruter et de s'assurer que l'on dispose des talents nécessaires dans nos rangs pour faire face aux cybermenaces dont nous parlons aujourd'hui?

Mme Cherie Henderson: Le SCRS a un programme de recrutement très actif pour rechercher les bons talents, et nous explorons toujours de nouvelles façons de trouver les bons talents et de les amener dans le service.

Il y a de nombreux Canadiens qui aimeraient beaucoup travailler dans le domaine de la sécurité nationale au sein de notre service, et nous trouvons des moyens de les encourager à se joindre à nous et de les encourager à rester. Vous avez mentionné la rétention. Avec l'évolution de l'environnement de travail, cela devient parfois un peu difficile dans le monde de la sécurité nationale, mais nous examinons tous les moyens de recruter et retenir notre personnel.

Mme Lindsay Mathyssen: Plus tôt, à notre comité, il y a plusieurs semaines maintenant, nous avons reçu un expert, Christian Leuprecht, du Collège militaire royal. Il a dit au Comité qu'il n'y a tout simplement pas assez de ressources pour attirer les talents dans les Forces armées canadiennes. Il a dit que les FAC, par exemple et précisément, sont en concurrence avec environ 200 000 postes vacants dans le domaine de la cybersécurité en Amérique du Nord.

Encore une fois, le défi est d'amener les bonnes personnes à franchir la porte et à s'intéresser à l'idée de la sécurité nationale. Est-ce que le SCRS se heurte aux mêmes problèmes et questions découlant de la compétitivité extrême de cette industrie?

Mme Cherie Henderson: Les FAC sont une organisation beaucoup plus grande que nous, donc leurs défis de recrutement sont très différents des nôtres. Nous avons certainement été témoins d'un énorme intérêt à travailler pour ce service, rien que par le volume des demandes que nous recevons.

Le président: Merci, madame Mathyssen. Voilà qui termine le premier tour.

Le deuxième tour commence avec M. Doherty.

Je vois que nous avons 25 minutes de questions et qu'il ne nous reste que 20 minutes. Je vais maintenir cinq minutes par intervenant et nous commencerons simplement plus tard.

Monsieur Doherty, vous avez cinq minutes.

M. Todd Doherty (Cariboo—Prince George, PCC): Merci, monsieur le président, et merci à nos invités de leur présence.

Je vais poser cette question à la fois à M. Khoury et à Mme Henderson. Elle est très simple.

Est-ce que Huawei représente une menace pour la sûreté et la sécurité du Canada?

M. Sami Khoury: D'un point de vue cybernétique, la sécurité de l'infrastructure des télécommunications est une chose que nous prenons très au sérieux. Le gouvernement procède à un examen de ces technologies émergentes et indique qu'une décision sera annoncée en temps voulu.

Entretemps, nous travaillons avec nos partenaires et d'autres organismes pour atténuer les risques découlant de l'utilisation des technologies visées, y compris Huawei.

M. Todd Doherty: Madame Henderson.

Mme Cherie Henderson: Je ne vais pas parler de Huawei en particulier, mais je tiens à souligner, comme dans ma réponse à une question plus tôt, que la loi chinoise sur la sécurité nationale oblige toutes les sociétés à s'engager dans des activités à l'appui des exigences du gouvernement.

M. Todd Doherty: C'est pourquoi j'ai posé cette question. Je comprends.

À la suite de cette question et de ce commentaire, madame Henderson, diriez-vous que certaines positions politiques des dernières années ont nui à notre réputation au sein du Groupe des cinq? Sommes-nous exclus de réunions importantes parce que nous avons toujours Huawei à la table et que nous sommes toujours en partenariat avec Huawei?

Mme Cherie Henderson: À l'heure actuelle, le gouvernement du Canada est engagé dans un examen continu qui est dirigé par Sécurité publique et qui détermine l'approche canadienne pour la mise en oeuvre de la technologie 5G et des réseaux de télécommunications.

M. Todd Doherty: Croyez-vous que nos alliés voient cela comme une menace et s'inquiètent du fait que Huawei soit toujours à la table avec le Canada?

Mme Cherie Henderson: Tous nos alliés ont adopté des approches différentes à l'égard de la technologie 5G, de Huawei et de la mise en oeuvre, et ils adoptent diverses mesures d'atténuation pour protéger leur sécurité nationale en réponse aux besoins de l'environnement qui leur est propre, et nous continuons tous à parler et à travailler très étroitement ensemble.

● (1610)

M. Todd Doherty: Pensez-vous que nos alliés ont des inquiétudes concernant un partenariat du Canada avec Huawei?

Mme Cherie Henderson: Je ne peux pas dire ce que pensent les alliés à ce stade, mais ce que je peux dire, c'est que nous collaborons tous très étroitement.

M. Todd Doherty: Comment définiriez-vous , faute d'un meilleur terme, une cyberattaque du style Pearl Harbor, et sommes-nous prêts à y faire face?

Mme Cherie Henderson: Nous collaborons étroitement avec nos partenaires du monde entier ainsi qu'avec nos partenaires nationaux afin d'éduquer et d'informer les infrastructures essentielles, les diverses entreprises, l'industrie et nos propres ministères afin qu'ils renforcent leurs ressources et assurent leur cybersécurité, et nous travaillons constamment ensemble pour trouver les nouvelles façons dont nous pourrions être attaqués, afin de nous préparer et aider tous les ministères à se protéger contre une cyberattaque massive.

M. Todd Doherty: Qu'est-ce qui vous empêche de dormir la nuit?

Mme Cherie Henderson: Beaucoup de choses me tiennent réveillée la nuit.

M. Todd Doherty: Quelle est la tempête parfaite et qu'est-ce qui vous empêche de dormir la nuit en ce qui concerne notre sécurité nationale, les cyberattaques et les cybermenaces?

Mme Cherie Henderson: Je dirais qu'à l'heure actuelle, nous travaillons tous très fort et surveillons de près la situation et l'environnement actuels, ainsi que les progrès technologiques, afin de nous assurer que nous avons les moyens de nous protéger. Nous sommes aussi forts que le maillon le plus faible, ce qui signifie que nous devons vraiment collaborer, éduquer et tirer des leçons des erreurs de chacun afin de pouvoir tout consolider et nous protéger aujourd'hui et demain. C'est un environnement en constante évolution, et nous ne pouvons jamais baisser la garde, car il y a toujours un acteur de la menace qui serait prêt à essayer de profiter de nos systèmes et de notre pays et d'avoir un impact extrêmement négatif sur notre sécurité nationale.

M. Todd Doherty: Je ne vous mettrai pas les mots dans la bouche, mais vous dites que nous sommes aussi forts que notre maillon le plus faible. Diriez-vous que le Canada est considéré comme un maillon faible au sein du Groupe des cinq parce que nous envisageons toujours Huawei et sommes en négociation avec cette société?

Mme Cherie Henderson: Non, je ne le dirais pas, car, comme je l'ai mentionné plus tôt, chaque pays doit trouver les mesures d'atténuation qui fonctionnent dans son cas particulier, et nous travaillons tous de façon extrêmement étroite pour partager l'information afin de nous assurer que nous nous aidons tous à nous protéger à l'avenir.

Le président: Merci, monsieur Doherty.

M. Todd Doherty: Merci.

Le président: Monsieur Fisher, qu'est-ce qui vous empêche de dormir la nuit? Vous avez cinq minutes pour nous le dire.

M. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Merci beaucoup, monsieur le président. Je ne vous parlerai pas de ce qui me tient éveillé la nuit, mais je suis sûr que ce n'est pas de la même gravité que dans le cas de nos témoins exceptionnels.

Merci beaucoup d'être ici et de votre témoignage.

J'ai essayé de lire beaucoup de choses pour me préparer à la réunion d'aujourd'hui. Il y a beaucoup de choses ici qui traitent des cybermenaces et de la cybersécurité, et en fait je vais faire un compliment à Mme Gallant en face. À mes débuts au Comité de la défense nationale, elle était l'un des membres qui menaient la charge sur les cybermenaces et la cybersécurité, et j'ai beaucoup appris d'elle.

Certaines de mes lectures parlaient du fait que le Canada était presque un dommage collatéral en ce qui concerne les cybermenaces et la cybersécurité, essentiellement en raison de notre proximité avec les États-Unis et de nos liens avec eux.

Je vais vous demander ceci à tous les deux, en commençant peut-être par Mme Henderson. Est-ce toujours vrai, maintenant que nous venons de déclencher d'importantes sanctions contre la Russie? Aucun d'entre nous dans cette salle n'est le bienvenu en Russie pour ses vacances d'été. Sommes-nous plus que des dommages collatéraux maintenant que nous avons décrété ces sanctions massives contre la Russie et ses oligarques?

Mme Cherie Henderson: Comme je l'ai dit plus tôt, nous travaillons en étroite collaboration avec nos partenaires, car, comme l'a souligné M. Doherty, nous sommes aussi forts que notre maillon le plus faible, et comme nous travaillons tous en étroite collaboration pour partager nos expériences respectives, pour apprendre et pour nous perfectionner, je ne dirais pas que nous sommes des dommages collatéraux. Je dirais que nous sommes un partenaire et que nous collaborons étroitement avec nos alliés pour établir ces partenariats et augmenter nos connaissances et notre sensibilisation.

● (1615)

M. Darren Fisher: D'accord.

Je ne savais pas si M. Khoury allait intervenir à ce sujet, mais c'est très bien. Je vous en remercie.

M. Sami Khoury: J'allais faire écho à ce que Mme Henderson a dit.

M. Darren Fisher: D'accord. C'est excellent.

De nombreux acteurs étatiques sous-traitent maintenant à des réseaux criminels, par exemple, ce que nous entendons souvent au sujet de la Russie. Comment pouvons-nous suivre les acteurs étatiques lorsqu'ils sous-traitent leurs cybermenaces dans le monde entier?

C'est à celui qui veut répondre.

M. Sami Khoury: Je suis heureux d'essayer de répondre à cette question.

Nous sommes conscients du lien qui existe entre les services de renseignement russes et les organisations cybercriminelles. C'est une chose que nous avons signalée dans notre évaluation des cybermenaces nationales de 2020 et plus récemment dans le contexte du conflit entre l'Ukraine et la Russie.

Nous avons vu des organisations cybercriminelles prendre parti d'un côté ou de l'autre. Du point de vue du cybercentre, nous avons la tâche de défendre le pays, de défendre le Canada et de défendre les infrastructures essentielles contre toutes sortes de menaces, qu'elles soient le fait d'États ou de cybercriminels, et de promouvoir la cybersécurité dans tous les domaines.

De toute évidence, dénoncer un pays pour sa cyberactivité est une tâche qui incombe à l'ensemble du gouvernement... et Affaires mondiales Canada est responsable du cadre d'attribution. Du point de vue du cybercentre, nous apporterions une contribution au dossier qui aiderait AMC à prendre la décision de nommer un pays publiquement.

M. Darren Fisher: En 45 à 60 secondes, l'un d'entre vous peut-il m'aider à mieux comprendre le piratage « éthique »? Qu'est-ce qu'un pirate éthique?

M. Sami Khoury: Je dirais que c'est un pirate sans mauvaise intention. C'est une personne qui s'introduit dans un système pour y découvrir une vulnérabilité et qui la signale ensuite au propriétaire du système en disant: « J'ai trouvé cette vulnérabilité dans votre système et voici comment vous devriez la corriger ». C'est l'opposé d'un pirate qui s'introduit dans un système et vole des renseignements, puis demande une rançon ou endommage le système.

M. Darren Fisher: C'est très utile. Je vous remercie.

Je pense connaître la réponse à cette question, mais d'où viennent la plupart des cyberattaques ou des tentatives de cyberattaques? Surtout, comment pouvons-nous nous défendre contre elles en tant que pays?

M. Sami Khoury: Les cyberattaques, du point de vue du cybercentre, viennent d'à-peu-près n'importe où. Nous défendons le gouvernement contre les cyberattaques qui viennent de partout, et aussi avec différentes intentions, qu'elles soient parrainées par un État ou criminelles. Défendre, c'est relever la barre et diffuser, autant que possible, des renseignements en temps opportun. La mesure du succès ici serait la rapidité avec laquelle nous détectons l'incident, la rapidité avec laquelle nous l'atténuons et la rapidité avec laquelle nous le transformons en une leçon apprise, afin que nous puissions aider à protéger les Canadiens.

Le président: Merci, monsieur Khoury et monsieur Fisher.

Madame Normandin, vous disposez de deux minutes et demie pour poursuivre cette épidémie stupéfiante de collégialité.

[*Français*]

Mme Christine Normandin: Merci beaucoup, monsieur le président.

Je vais faire un retour sur deux des questions que j'ai posées. La première concerne le Centre d'analyse des opérations et déclarations financières du Canada, le CANAFE.

Serait-il pertinent qu'il y ait une meilleure collaboration entre le Centre de la sécurité des télécommunications, le CST, et le Service canadien du renseignement de sécurité, ou SCRS, concernant le suivi de la cybermonnaie qui peut être utilisée par des groupes terroristes?

M. Sami Khoury: Je vous remercie de cette question.

Nous travaillons de près avec nos collègues du CANAFE, mais nous n'avons pas de mandat d'investigation. Souvent, lorsqu'il y a de la cybermonnaie qui se déplace, c'est dans des cas de rançon ou d'autres cas de nature criminelle. Je vais donc rediriger la question à la GRC, car cela relève davantage de sa compétence.

Mme Christine Normandin: C'est parfait, merci.

Madame Henderson, vous parliez de l'article 12 de la Loi sur le Service canadien du renseignement de sécurité, qui permet d'avoir des activités outre-mer. Je comprends que c'est possible, mais, ce que je veux savoir, c'est s'il serait souhaitable de l'officialiser, c'est-à-dire de créer un service permanent outre-mer pour s'assurer que le SCRS a plus de tentacules un peu partout sur la planète.

● (1620)

[*Traduction*]

Mme Cherie Henderson: Le SCRS est un organisme de renseignement national. Comme je l'ai dit, nous avons la capacité et l'autorité d'enquêter sur toute menace à l'étranger qui constitue une menace pour notre sécurité nationale. Nous avons une représentation à l'étranger, comme cela est reconnu publiquement — nous avons un agent à Paris, à Londres et à Washington —, qui soutient toutes les relations de travail avec nos partenaires à l'étranger.

Nous avons la capacité d'enquêter pour protéger notre sécurité nationale.

[*Français*]

Mme Christine Normandin: Finalement, je voudrais vous poser une brève question à tous les deux.

On sait qu'il y a des cyberattaques liées à des rançons et d'autres qui servent à déstabiliser les pays.

Comment se répartissent les cyberattaques que subit le Canada?

M. Sami Khoury: C'est difficile d'y attacher un nombre, parce que les cas sont sous-rapportés. Ce ne sont pas toutes les victimes de cyberattaques qui nous contactent pour les rapporter. Je peux décrire celles qui visent le gouvernement ou la surface d'attaque de ce dernier, mais c'est difficile de comparer cela aux cyberattaques liées aux rançons.

Cela dit, le gouvernement est certainement une cible attrayante.

Mme Christine Normandin: Merci beaucoup. Je pense que c'est tout le temps que j'avais.

[*Traduction*]

Le président: Madame Mathyssen, vous avez deux minutes et demie.

Mme Lindsay Mathyssen: Merci.

Les médias ont cité des responsables américains anonymes qui ont dit que la Chine avait signalé être disposée à fournir, éventuellement, un soutien économique et militaire à l'attaque de la Russie en Ukraine. Quelle est la probabilité, selon vous, que la Chine étende ce soutien, peut-être sous la forme d'une coopération aux cyberopérations visant l'occident — l'Ukraine et les alliés occidentaux?

Je crois bien que cela s'adresse à vous deux.

M. Sami Khoury: Nous savons, d'après les évaluations des cybermenaces, que la Chine a un programme cybernétique parrainé par l'État, tout comme la Russie. Nous devons défendre le gouvernement et la société canadienne dans son ensemble contre ces deux menaces, qu'il s'agisse d'une menace stratégique contre le gouvernement ou d'un vol de propriété internationale ou de choses de ce genre.

En ce qui concerne la nature de la relation entre la Russie et la Chine, je m'en remets à notre collègue du renseignement, qui est peut-être mieux placée pour en parler.

Mme Cherie Henderson: Sans parler de la relation entre la Chine et la Russie en particulier, je dirais que ces deux pays sont des acteurs de la menace extrêmement capables qui agiront dans leur intérêt et en fonction de leurs besoins.

Le président: Monsieur Motz, vous avez cinq minutes.

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

Je remercie les témoins de leur présence.

C'est un plaisir de vous revoir, madame Henderson. J'espère que ma question ne vous mettra pas dans l'embarras.

Je vais d'abord répondre à une question concernant le CPSNR, le Comité des parlementaires sur la sécurité nationale et le renseignement. Dans son rapport, que je ne vais pas détailler, car il est long, ses membres ont cité et décrit la cyberattaque d'un réseau du ministère de la Défense nationale en 2017 qui s'est soldée par le vol par un acteur étatique d'une quantité importante de données. Le réseau en question ne faisait pas partie du Service Internet d'entreprise de Services partagés Canada, et n'était donc pas protégé par les capteurs du réseau du Centre de la sécurité des télécommunications.

Je vais vous poser la question en premier, mais je suis sûr que M. Khoury interviendra également. Il est important de noter que le réseau compromis contenait une technologie ancienne qui ne pouvait pas être corrigée et était donc vulnérable aux cybermenaces. Le MDN et les FAC utilisent-ils maintenant des technologies à jour et entièrement corrigées dans tous leurs systèmes et réseaux?

Mme Cherie Henderson: Je ne peux pas répondre à cette question. Je ne sais pas si M. Khoury aurait une réponse à vous donner à ce sujet.

M. Sami Khoury: Je m'en remets au MDN pour la réponse à cette question sur l'état précis de ses TI.

M. Glen Motz: Je vous remercie tous les deux. Je sais que vous devez être prudents, mais c'est votre organisation qui a repéré le problème, après tout. Êtes-vous encore aussi alarmés par le fait que le problème existe et qu'il y a encore des vulnérabilités de sécurité avec une technologie non corrigée?

M. Sami Khoury: Nous avons travaillé sans relâche avec le MDN, ainsi qu'avec le reste du gouvernement, pour augmenter la couverture des capteurs que le cybercentre a mis à la disposition du gouvernement pour la défense. Nous sommes assurément dans un bien meilleur espace aujourd'hui que nous l'étions en 2017.

En ce qui concerne la technologie et les anciens systèmes, je m'en remets au MDN. Ils connaissent le mieux leur environnement pour dire si certaines technologies ont été mises à jour ou non.

● (1625)

M. Glen Motz: Très bien.

Vous avez mentionné il y a juste une seconde, M. Khoury, lorsque je vous ai demandé quelle était la prévalence du problème des vieux logiciels non corrigés dans les systèmes et les réseaux fédéraux en général, vous avez dit que vous vous améliorez. Y a-t-il encore des vulnérabilités? Je ne vous demande pas de les décrire, mais où en sommes-nous par rapport à il y a deux ou trois ans?

M. Sami Khoury: Je dirais que nous sommes en bien meilleure posture, mais l'application de correctifs à un système n'est pas sans risque. Chaque ministère, y compris Services partagés et d'autres, doit évaluer l'impact de l'application d'un correctif à un système. Parfois, cela brise la technologie, ou cela brise les systèmes actuellement utilisés. Je m'en remets à eux pour l'évaluer.

Nous avons mis en place toute une série de capacités de sécurité dont nous sommes très fiers pour protéger le gouvernement fédéral, à ce stade.

M. Glen Motz: Super.

Dans le cadre de l'opération Unifier des Forces armées canadiennes, le CST partage des renseignements sur les menaces avec l'Ukraine et aide ce pays à se défendre contre les cyberattaques. Le CST ou les Forces armées canadiennes participent-ils à des cyberopérations actives dans le cadre de l'opération Unifier?

M. Sami Khoury: Lorsque nous avons repéré des cyberactivités dirigées contre l'Ukraine, nous avons partagé ces indicateurs avec les responsables ukrainiens afin qu'ils puissent mieux défendre leurs réseaux. Au-delà de cela, sur la question des cyberopérations, je suis malheureusement incapable de répondre.

M. Glen Motz: D'accord. C'est très bien.

Le 25 février de cette année, un jour après l'invasion de l'Ukraine par la Russie, Conti Group, une organisation criminelle organisée affiliée à la Russie et spécialisée dans les attaques de rançongiciel, s'est engagée à soutenir l'invasion et a menacé de représailles toute activité de guerre dirigée contre la Russie. D'autres groupes de rançongiciel se sont joints au groupe Conti dans sa promesse de soutien.

Comment les menaces de représailles de Conti Group et d'autres groupes de rançongiciel ont-elles touché la planification de la cyberdéfense du Canada?

Cette question s'adresse à vous deux.

M. Sami Khoury: Nous connaissons bien le groupe Conti. Il était actif au Canada avant l'invasion, donc nous avons une bonne connaissance de la façon de nous défendre contre elle. Nous avons lancé une grande campagne sur les rançongiciels en décembre pour attirer l'attention sur ce problème. À la suite de l'invasion de l'Ukraine par la Russie, nous avons publié à deux reprises des bulletins de mise en garde à l'intention des exploitants d'infrastructures essentielles, pour attirer leur attention sur la menace que représentent la Russie et les groupes affiliés à la Russie, afin qu'ils puissent mieux se défendre.

Nous tirons constamment des leçons de ce qui se passe sur le terrain, nous mettons à jour nos conseils et nos directives, nous mettons à jour nos flux concernant les menaces et nos indicateurs de compromission, et nous défendons...

Le président: Merci, monsieur Khoury et monsieur Motz.

Monsieur May, allez-y pour les cinq dernières minutes, s'il vous plaît.

M. Bryan May (Cambridge, Lib.): Merci beaucoup, monsieur le président.

Merci à nos deux témoins de cet après-midi.

Monsieur Khoury, pouvez-vous commenter le travail du Centre canadien de la cybersécurité avec divers secteurs industriels et nous en dire plus sur le sujet?

M. Sami Khoury: Oui. Bien que la mission première du cybercentre soit de protéger le gouvernement et de diriger la réponse aux cyberincidents, nous travaillons en collaboration étroite avec les secteurs public et privé. Nous avons un certain nombre de plateformes d'engagement avec ces secteurs par le truchement de tables sectorielles, qu'il s'agisse de l'énergie, de l'électricité ou des soins de santé. Certaines se réunissent plus régulièrement que d'autres. Avec la table ronde sur les soins de santé, qui comprend la communauté des soins de santé de tout le Canada, des hôpitaux et des cliniques, nous nous réunissons toutes les deux semaines, voire toutes les semaines.

De concert avec le secteur de l'électricité, nous avons lancé un projet pilote appelé Lighthouse pour lui permettre d'évaluer les menaces qui pèsent sur ses réseaux. De même, nous avons un autre projet pilote avec l'Association canadienne du gaz, dans le cadre duquel nous l'aidons à prendre conscience des menaces qui pèsent sur son secteur.

Au-delà de ça, nous nous penchons aussi sur les résultats à l'échelle nationale. Nous avons travaillé avec CIRA, l'organisme canadien de gestion des adresses Internet, pour mettre gratuitement à la disposition des Canadiens un service de protection DNS, de sorte que lorsque l'on navigue en ligne, si l'on pointe sur le Bouclier canadien, on peut être sûr qu'aucun site Web malveillant ne se trouve là où l'on va. Nous avons un programme de collaboration assez large avec le secteur privé.

● (1630)

M. Bryan May: Merci.

Selon vous, quels secteurs d'infrastructures essentielles sont les mieux équipés pour se défendre contre les cyberattaques?

M. Sami Khoury: Il est difficile de comparer un secteur à un autre. Les menaces peuvent être différentes. Le cybercentre a pour rôle de veiller à transmettre tous les renseignements à tous les secteurs essentiels — qu'il s'agisse des finances, de l'énergie, des transports ou des soins de santé — et de nous assurer qu'ils disposent tous des outils dont ils ont besoin pour se protéger en cas de cyberattaque. Il est difficile de dire d'emblée lequel est mieux préparé que les autres.

M. Bryan May: Je reconnais cela, mais peut-être qu'une meilleure façon de poser la question est de demander quels secteurs doivent s'améliorer considérablement, à votre avis. Lesquels ont besoin de plus de travail, et comment pouvons-nous les aider à relever la barre?

M. Sami Khoury: Il existe un programme dans le cadre duquel nous pouvons travailler avec les différentes entités pour évaluer leur maturité en matière de cybersécurité, et nous sommes heureux de collaborer avec toutes celles-ci. Chaque secteur a des besoins différents, donc les programmes que nous adaptons, par exemple, au milieu municipal, sont différents des programmes que nous adaptons au secteur bancaire. Nous devons couvrir l'ensemble des secteurs canadiens afin de nous assurer qu'ils sont tous protégés.

M. Bryan May: Pour répondre à ma dernière question, vous pourrez tous deux intervenir si vous prenez chacun environ 30 à 35 secondes, ce qui n'est peut-être pas juste. À votre avis, des exigences de déclaration comme celles qui ont été récemment adoptées aux États-Unis amélioreraient-elles la situation au Canada?

Monsieur Khoury, vous pouvez commencer.

M. Sami Khoury: Nous savons que les incidents liés aux rançongiciels sont sous-signalés, alors nous encourageons tout le monde à nous contacter, qu'il s'agisse d'un petit ou d'un grand incident, pour nous faire part de la nature du cyberincident afin que nous puissions en tirer des leçons et réagir rapidement pour atténuer la menace dans tout le Canada. Plus il y aura de signalements, mieux ce sera pour relever la barre collective au Canada.

Mme Cherie Henderson: Je suis d'accord. Je crois fermement que nous devons vraiment avoir une communication ouverte, pour soulever les problèmes et en débattre, et pour encourager tout le monde à signaler un incident. De nombreuses entreprises sont très craintives et pensent que cela aura une incidence très négative sur elles, mais tout cela peut être géré de manière sécurisée, de sorte que nous ne donnons pas les identités, mais que nous recueillons autant de renseignements que possible pour les protéger, ainsi que d'autres entreprises.

M. Bryan May: Merci beaucoup à vous deux.

Le président: Au nom du Comité, je tiens à remercier nos deux témoins, M. Khoury et Mme Henderson, pour leur contribution à notre étude sur l'analyse des menaces. Le cyberespace est unique en ce sens qu'il semble terriblement difficile de comprendre ce qui se passe, étant donné sa nature à la fois obscure et omniprésente. Je vous remercie pour vos idées et votre travail au nom de notre nation.

Sur ce, nous allons suspendre la séance pendant que nous réunissons le prochain groupe de témoins. Nous vous remercions.

● (1630)

(Pause)

● (1635)

Le président: Nous accueillons maintenant Benoît Dupont, professeur et titulaire de la chaire de recherche du Canada en cybersécurité à l'Université de Montréal, et John Hewie, agent de la sécurité nationale chez Microsoft.

Je vais demander à chacun d'entre vous de faire une déclaration préliminaire de cinq minutes.

Nous commençons par M. Dupont pour cinq minutes.

Allez-y, je vous en prie, monsieur.

[*Français*]

M. Benoît Dupont (professeur et titulaire de la chaire de recherche du Canada en cybersécurité, Université de Montréal, à titre personnel): Je vous remercie, monsieur le président, mesdames et messieurs les membres du Comité, de m'avoir invité à témoigner devant vous. Je répondrai à vos questions dans les deux langues officielles, mais je vais témoigner en français.

Je suis professeur à l'Université de Montréal, titulaire de la Chaire de recherche du Canada en cybersécurité et directeur scientifique du Human-Centric Cybersecurity Partnership, un regroupement d'une trentaine de chercheurs en cybersécurité et de partenaires gouvernementaux et du secteur privé, dont Microsoft.

Comme les autres témoins qui ont comparu avant moi devant ce comité, j'aimerais insister sur les transformations technologiques qui sont en train de redéfinir les paramètres des conflits militaires dans lesquels le Canada se trouve, et se trouvera, à l'avenir, engagé. Les cyberattaques et la désinformation sont, bien évidemment, dans tous les esprits à la lumière de l'invasion qui se déroule en Ukraine, mais, sur un horizon plus long, les technologies numériques, telles que l'intelligence artificielle, la 5G, l'Internet des objets, l'informatique quantique ou l'avènement des interfaces neuronales, représentent également des défis qui risquent de modifier de manière radicale les conflits armés.

Ces changements prévisibles et annoncés nous obligent à réfléchir aux stratégies qui doivent, dès maintenant, être mises en œuvre pour s'y préparer. Dans un premier temps, il me semble essentiel de réfléchir aux implications stratégiques à moyen et à long terme de ces technologies afin d'anticiper le rôle qu'elles vont jouer dans les conflits futurs, par exemple en 2025 ou en 2030, et de commencer à s'y préparer dès maintenant, aussi bien par l'acquisition de capacités techniques nouvelles que par le recrutement et la formation des opérateurs qui vont être amenés à utiliser ces capacités techniques. Ce travail de prospective est indispensable si l'on veut que nos forces armées s'adaptent de manière proactive à un environnement en changement constant.

Ces changements technologiques doivent aussi s'accompagner de changements profonds en ce qui concerne le recrutement et la formation de spécialistes en cybersécurité, dont le rôle va prendre une importance croissante. La pénurie généralisée de main-d'œuvre dans ce domaine, qui a déjà été évoquée, je crois, par mon collègue M. Christian Leuprecht, touche le secteur privé, et elle va requérir de la créativité de la part des forces armées afin de pouvoir attirer les personnes qualifiées. Certains pays ont déjà mis en place des procédures de recrutement spécifiques pour leurs forces armées, alors que d'autres ont fait le choix de développer des forces de réservistes spécialisés permettant de mobiliser rapidement des personnels qualifiés en temps de crise. À ma connaissance, la réflexion du Canada en ce domaine reste embryonnaire.

Au-delà des ressources humaines, il me semble vital de développer une souveraineté numérique en défense sur certaines technologies clés comme l'intelligence artificielle ou l'informatique quantique, où le Canada est un leader en recherche, mais accuse un certain retard sur le plan industriel. Cela implique donc le développement délibéré d'écosystèmes industriels d'innovation pouvant contribuer à la défense du Canada et de ses alliés. À ce titre, j'aimerais rappeler que le partenariat de sécurité AUKUS, entre les États-Unis, le Royaume-Uni et l'Australie, qui a été annoncé en septembre 2021 et auquel le Canada n'a pas été invité, ne porte pas uniquement sur la fourniture de sous-marins nucléaires à l'Australie, mais prévoit également une très forte intégration des efforts de recherche-développement et de commercialisation de ces trois pays dans les domaines stratégiques de la cybersécurité, de l'intelligence artificielle et de l'informatique quantique.

En conclusion, face à un paysage de menaces technologiques toujours plus complexe et à des adversaires qui intensifient leur usage de cyberattaques, on ne pourra pas trouver de réponses efficaces à ces défis dans les manières de faire traditionnelles, qui ont déjà démontré cruellement leurs limites. Les innovations qui sont requises ne pourront pas non plus se contenter de copier à l'identique les solutions imaginées et mises en œuvre par notre voisin et nos alliés. Je pense qu'il faut que nous engagions un véritable travail de réflexion en profondeur sur nos intérêts, nos ressources et nos stratégies, qui va se concrétiser en des mesures audacieuses, qui vont nous permettre de rattraper notre retard.

● (1640)

Le président: Merci, monsieur Dupont.

[*Traduction*]

Ensuite, nous avons M. Hewie de Microsoft.

M. John Hewie (agent de la sécurité nationale, Microsoft Canada inc.): Bonjour, monsieur le président et mesdames les vice-présidentes.

Permettez-moi tout d'abord de vous remercier de m'avoir invité à comparaître pour vous éclairer sur les cybermenaces au Canada et sur l'état de préparation opérationnelle des Forces armées canadiennes à y faire face.

Je suis John Hewie, agent de la sécurité nationale chez Microsoft au Canada.

L'une de nos responsabilités principales et mondiales en tant qu'entreprise est d'aider à défendre les gouvernements et les pays contre des cyberattaques. Ce rôle a rarement été aussi important que ces dernières semaines en Ukraine. Chez Microsoft, nous suivons tous de près cette invasion tragique, illégale et injustifiée.

Elle est devenue une guerre à la fois cinétique et numérique, avec des images horribles ainsi que des cyberattaques moins visibles contre des réseaux informatiques accompagnées de campagnes de désinformation sur Internet, parrainées par l'État.

Notre travail le plus important à cet égard en Ukraine a été d'aider à protéger les infrastructures ukrainiennes contre les cyberattaques russes. Ces cyberattaques continues ont été précisément ciblées et nous sommes particulièrement préoccupés par celles qui visent des cibles numériques civiles ukrainiennes, notamment les infrastructures essentielles, les services d'intervention d'urgence et les efforts d'aide humanitaire. De concert avec le gouvernement ukrainien, nous avons mis en oeuvre des protections techniques de cybersécurité auprès de dizaines d'organisations ciblées. Nous aidons aussi des organisations ukrainiennes à déplacer leurs services vers le nuage afin qu'elles puissent continuer à fonctionner potentiellement depuis l'extérieur du pays. Nos équipes d'intervention en cas de catastrophe ont aussi épaulé de nombreux groupes qui fournissent de l'aide au peuple ukrainien.

Nos efforts ont nécessité une coordination constante et étroite avec le gouvernement ukrainien, l'Union européenne, le gouvernement américain, l'OTAN et les Nations unies. Nous nous sommes engagés à soutenir l'Ukraine et à aider à protéger son gouvernement, ses citoyens et notre personnel.

Si les événements en Ukraine retiennent certainement l'attention du monde, d'autres cybercriminels continuent à cibler et attaquer tous les secteurs des infrastructures essentielles, notamment la santé publique, les technologies de l'information, les services financiers et les secteurs de l'énergie. Les attaques au rançongiciel sont de plus en plus sophistiquées et parviennent à paralyser des gouvernements et des entreprises. Les profits tirés de ces attaques montent en flèche, ce qui contribue à alimenter les intérêts financiers criminels et ceux parrainés par des États. Selon des estimations mondiales, le coût des violations de données dans le monde dépassera les 5 000 milliards de dollars d'ici 2024.

Au cours de la dernière année, 58 % de toutes les cyberattaques d'État observées par Microsoft ont été attribuées à la Russie, suivie de la Corée du Nord, de l'Iran et de la Chine. Les acteurs russes ciblent de plus en plus les organismes gouvernementaux s'occupant de politique étrangère, de sécurité nationale et de défense aux fins de la collecte de renseignements.

La compromission de SolarWinds fin 2020 par un acteur russe est un exemple des attaques croissantes et préoccupantes observées contre la chaîne d'approvisionnement. Ces renseignements et d'autres sont exposés dans le deuxième rapport annuel de Microsoft sur la défense numérique qui présente notre point de vue sur l'environnement mondial des cybermenaces.

Microsoft a récemment pris l'engagement mondial sans précédent d'investir 20 milliards de dollars dans la cybersécurité au cours des cinq prochaines années. Notre stratégie globale en matière de sécurité repose sur une approche globale qui englobe la diplomatie en promouvant la paix numérique et en préconisant des normes de comportement acceptable dans le cyberespace, la perturbation de l'infrastructure cybercriminelle à l'aide de partenariats novateurs en matière de poursuites civiles et d'application de la loi et, bien sûr, la défense contre les cyberattaques qui ciblent Microsoft et nos clients dans le monde entier à l'aide de la technologie infonuagique avancée — une approche de la sécurité fondée sur la confiance zéro qui met à contribution des partenariats d'échange d'information et des milliers de personnes hautement qualifiées.

Les relations que nous entretenons depuis 15 ans avec le Centre de la sécurité des télécommunications et maintenant avec le Centre canadien pour la cybersécurité sont de bons exemples de ces partenariats. Dans ce contexte, nous échangeons des renseignements sur les nouvelles menaces et les techniques de cyberdéfense rendues possibles par le programme de sécurité gouvernemental de Microsoft.

Il suffit de regarder autour de nous pour nous rendre à l'évidence que la technologie numérique joue un rôle essentiel dans presque toutes les facettes de notre vie. La mission de Microsoft est de donner à chaque personne et à chaque organisation sur la planète les moyens d'en faire plus. Nous ne pouvons y parvenir qu'en protégeant le monde numérique que nous utilisons tous. Il est devenu très clair pour le monde que la cybercriminalité et les attaques commanditées par des États constituent des menaces critiques pour la sécurité nationale et l'économie du Canada. Aucune entité ne peut, à elle seule, lutter efficacement contre ces menaces. Il est primordial de collaborer avec l'industrie, le milieu universitaire, la société civile et les gouvernements, au Canada et à l'étranger.

En tant qu'entreprise à l'avant-garde de la cybersécurité, nous sommes là pour apporter notre soutien, parfaire nos connaissances et notre savoir-faire et jouer un rôle essentiel en aidant à améliorer l'état de préparation du Canada et de l'ensemble du gouvernement, y compris les Forces armées canadiennes.

Je vous remercie, mesdames et messieurs, pour votre temps et votre attention. Je suis prêt à répondre à vos questions.

● (1645)

Le président: Merci à vous deux.

Nous en sommes à la série de six minutes.

Chers collègues, je regarde l'horloge, et si nous faisons un tour de six minutes et l'autre tour de cinq minutes, nous n'avons aucune chance de même venir près de finir à l'heure, alors je vais commencer par un tour de cinq minutes.

Sur ce, monsieur Doherty, vous disposez de cinq minutes.

M. Todd Doherty: Merci à nos invités de leur présence.

Monsieur Hewie, je suis heureux que vous ayez évoqué l'incident de cyberespionnage de SolarWinds en 2021. À votre avis, quelle responsabilité devrait incomber aux fournisseurs de logiciels et de technologie de l'information pour garantir que leurs produits et services sont vraiment sûrs?

M. John Hewie: Je vous remercie de cette question.

Évidemment, les fournisseurs de technologie ont une responsabilité cruciale de veiller à ce que leurs logiciels et leurs services soient aussi sûrs que possible. Microsoft prend cette responsabilité très au sérieux.

Bien que nous ayons été les chefs de file du monde et des organisations technologiques du monde entier en matière de développement et d'éducation concernant les choses comme le cycle de vie du développement de la sécurité, dont Microsoft a été le pionnier il y a plus de 10 ans, et bien sûr avec des améliorations continues en matière d'échanges de renseignements et de partenariats avec des organisations et des gouvernements du monde entier, et en collaborant avec nos concurrents, y compris Amazon, Google et beaucoup d'autres dans le milieu de la sécurité, en faisant de notre mieux pour créer des logiciels fiables et dignes de confiance, bien honnêtement, nous sommes face à des adversaires qui sont très déterminés, très patients et très bien financés.

Les logiciels d'aujourd'hui sont incroyablement complexes et bien que nous nous efforçons de réduire le plus possible leurs vulnérabilités, c'est une tâche qui nous demande de ne jamais baisser la garde et à laquelle nous continuons à travailler.

M. Todd Doherty: L'une des choses intéressantes, c'est que nous avons entendu de nombreux témoignages selon lesquels il y a une grave pénurie de main-d'oeuvre de même qu'à l'égard de la prochaine génération d'experts en cybersécurité possédant ces compétences. Au cours des huit prochaines années, nous constatons qu'il y aura environ 3,5 millions de postes à pourvoir dans le monde.

Que fait Microsoft pour aider à combler ce manque, non seulement en Amérique du Nord, mais dans le monde entier?

M. John Hewie: Je vous remercie.

C'est une excellente question, qui est en fait très importante. Nous sommes aussi tout à fait conscients de cette pénurie de ressources et de compétences dans le milieu de la sécurité. Nous prenons plusieurs mesures.

Ici, expressément au Canada, rien que l'an dernier, Microsoft a investi des millions de dollars dans les compétences, les outils et les programmes de sécurité pour aider à attirer de nouvelles personnes et beaucoup plus de diversité dans le domaine de la sécurité ici au Canada. Nous avons des partenariats pour soutenir différentes universités et différents établissements d'enseignement à travers le pays avec des programmes d'acquisition de compétences et je pense que nous essayons de sensibiliser la communauté dans son ensemble au fait que ce n'est pas simplement un problème qui sera résolu par des bolés de la technologie qui savent configurer des réseaux. Il y a des questions juridiques, des questions de droit civil et tout simplement une diversité. Nous avons besoin d'une réflexion très variée pour combler ce manque de compétences et, ensemble, aider à combattre ce problème.

M. Todd Doherty: Le 28 février, le président de Microsoft, Brad Smith, a publié l'information suivante:

> Plusieurs heures avant le lancement de missiles ou le mouvement de chars le 24 février, le Centre du renseignement sur les menaces de Microsoft... a détecté une nouvelle série de cyberattaques offensives et destructrices contre l'infrastructure numérique de l'Ukraine. Nous avons immédiatement informé le gouvernement ukrainien de la situation, y compris de notre identification de l'utilisation d'un nouveau maliciel (que nous avons baptisé FoxBlade) et nous lui avons donné des conseils techniques sur les mesures à prendre pour contrer ce maliciel.

Quand et dans quelles circonstances le Centre du renseignement sur les menaces de Microsoft a-t-il commencé à collaborer avec le gouvernement ukrainien?

● (1650)

M. John Hewie: Le Centre du renseignement sur les menaces de Microsoft suit en permanence un certain nombre d'acteurs dans le monde. Nous le faisons depuis plusieurs années et c'est vraiment pour aider à guider non seulement la façon dont nous intégrons des protections de cybersécurité dans nos produits et services, mais aussi pour aider à informer nos différents clients dans le monde entier et leur fournir des renseignements.

M. Todd Doherty: Qui est derrière FoxBlade?

M. John Hewie: Je ne crois pas avoir les détails à portée de la main sur les personnes auxquelles nous avons attribué FoxBlade, mais il s'agissait sans équivoque d'une attaque au moyen d'un maliciel d'effacement qui visait l'infrastructure ukrainienne.

M. Todd Doherty: Quel était l'objectif et a-t-il été atteint?

Le président: Veuillez être très bref.

M. John Hewie: D'après ce que nous observons, le virus d'effacement FoxBlade est un bon exemple de ce qui semble constituer une attaque de type rançongiciel contre l'infrastructure, mais qui est en fait une attaque destructrice. L'intention est de crypter les données, mais il n'y a pas de possibilité de les restaurer ni d'intention de la part de l'adversaire de demander une rançon à la victime.

Le président: Merci, monsieur Doherty.

Monsieur Spengemann, vous disposez de cinq minutes. Je vous en prie.

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

Je remercie nos deux témoins de leur présence cet après-midi.

Le domaine est extrêmement complexe, comme vous et nos témoins précédents l'avez souligné. Il est hautement interdisciplinaire. Nous parlons de la mise en place d'un écosystème qui, à bien des égards, n'a pas encore été établi, ou ne l'a pas été suffisamment. Ensuite, nous avons l'invasion de l'Ukraine par la Russie qui a mis en évidence toute la situation et illustré l'urgence avec laquelle nous devons nous pencher sur cette question.

Cela concerne le secteur privé, les infrastructures publiques civiles et le secteur militaire. Dans le cadre de la réponse de l'Union européenne, du Canada et de nombre de nos alliés en ce qui concerne l'application des sanctions, nous avons vu à quelle vitesse le secteur privé et les marchés financiers entrent en action lorsqu'il est question de sécurité.

J'aimerais que chacun de vous prenne un moment pour nous donner un aperçu de l'état de cet écosystème, en tenant compte de ses complexités et de ses interdisciplinarités. Que faut-il faire de toute urgence, du point de vue du gouvernement fédéral? Quels sont certains des défis, sur le plan opérationnel, en ce qui concerne les ressources humaines, le changement de mentalité et le fait d'envisager la sécurité numérique comme un domaine dans lequel un investissement est nécessaire de toute urgence et, idéalement, en croissance rapide?

Si vous pouviez préciser un peu vos observations initiales pendant 45 secondes chacun... Il me reste peu de temps, et ce serait utile.

Le président: Cinq heures, minimum.

[*Français*]

M. Sven Spengemann: Professeur Dupont, vous pouvez répondre le premier. Ensuite, j'aimerais entendre M. Hewie.

[*Traduction*]

M. Benoît Dupont: Le gouvernement du Canada vient d'annoncer un investissement de 80 millions de dollars dans le réseau d'innovation en cybersécurité par l'entremise d'ISDE. Je pense qu'il s'agit d'une excellente initiative, car elle va rassembler plus de 120 partenaires universitaires et industriels du secteur privé et des administrations provinciales, municipales et fédérales. Je pense que cette initiative doit être soutenue et probablement accélérée.

En ce qui concerne la formation, nous devons faire appel à des personnes de toutes sortes de disciplines, puisque vous avez mentionné qu'il s'agit d'une approche interdisciplinaire. Lorsque nous avons passé en revue toutes les disciplines concernées, nous en avons répertorié plus de 40, de la santé publique aux sciences politiques en passant par la psychologie et l'informatique, bien sûr. Je pense que nous devons favoriser une mobilisation beaucoup plus importante dans le travail interdisciplinaire au Canada et réfléchir à la façon dont cela pourrait être mis à profit pour protéger les biens, les groupes vulnérables et les infrastructures essentielles du Canada.

M. Sven Spengemann: Merci beaucoup.

Allez-y, monsieur Hewie.

M. John Hewie: J'appuierais ce que mon collègue vient de dire. Absolument, aucune entité ne peut combattre ces menaces à elle seule. Nous avons entendu des thèmes similaires de la part des témoins précédents. Nous avons besoin d'une collaboration solide entre le gouvernement, l'industrie et le milieu universitaire, tant au niveau national qu'international.

Je pense qu'il est important de reconnaître que lorsque nous parlons du cyberespace, le secteur privé — l'industrie privée, en particulier les fournisseurs de services infonuagiques comme Microsoft — exploitent une grande partie de cette infrastructure. C'est ce que les Forces canadiennes appelleraient le « cyberespace de combat ». Nous avons certainement une vision qui nous est propre et c'est probablement une vision différente de cette des organismes gouvernementaux. En collaborant, nous pouvons vraiment compléter les capacités de chacun pour défendre et protéger les clients, les organisations, les gouvernements et tous les Canadiens dans cet espace.

● (1655)

M. Sven Spengemann: Merci beaucoup à vous deux.

Il me reste environ une minute et demie.

Brièvement, à propos d'un enjeu qui se rapporte davantage à la défense, quel est le point de vue de chacun de vous sur la capacité offensive, en ce qui concerne le domaine cybernétique?

M. John Hewie: Je vais peut-être me lancer en premier.

La réponse de la part de Microsoft est brève: Microsoft n'approuve pas les cyberactivités offensives et ne s'y livre pas.

M. Sven Spengemann: Merci beaucoup.

[*Français*]

Professeur Dupont, pouvez-vous répondre, s'il vous plaît?

[*Traduction*]

M. Benoît Dupont: C'est un sujet sur lequel je dispose de très peu d'information. Je travaille dans le milieu universitaire, c'est donc un sujet qui est très éloigné de mon travail.

M. Sven Spengemann: D'accord, c'est utile. Cela me laisse un peu plus de temps.

Lorsque nous examinons les points de connexion interdisciplinaires en ce qui concerne les cyberattaques, dans quelle mesure notre système est-il cloisonné et à quel point les divers cloisonnements qui doivent réagir à ce problème sont-ils séparés? Dans quelle mesure sont-ils coordonnés à l'heure actuelle?

M. Benoît Dupont: Il y a un réel effort de coordination avec le Centre canadien pour la cybersécurité et par l'entremise d'autres initiatives, mais il est probablement encore à la traîne. C'est un enjeu tellement complexe et nous devons probablement y injecter beaucoup plus d'effort, d'énergie et d'argent.

Je pense qu'il reste encore beaucoup de travail à faire. Beaucoup de gens sont très conscients de la nécessité de décloisonner tous ces groupes isolés.

Le président: Merci.

M. Sven Spengemann: Merci beaucoup, monsieur le président.

[*Français*]

Le président: Madame Normandin, vous avez la parole pour cinq minutes.

Mme Christine Normandin: Merci beaucoup, monsieur le président.

Professeur Dupont, vous avez mentionné que le Canada accusait un retard sur le plan industriel. On a parlé de SolarWinds, et on sait que c'est FireEye, un groupe de réflexion américain, qui a mis au jour la brèche.

Est-ce le genre d'initiative qui manque au Canada, ou les lacunes se trouvent-elles plutôt du côté gouvernemental?

Sinon, serait-ce plutôt l'équilibre et la collaboration entre les deux qui sont lacunaires?

M. Benoît Dupont: FireEye est une entreprise privée, ce n'est pas un groupe de réflexion. Elle a à peu près le même type d'expertise que Microsoft.

Je pense que le retard au Canada est attribuable au fait que les questions de sécurité et de cybersécurité ne sont pas en haut de la liste des priorités politiques. C'est jugé comme un sujet important, mais pas forcément comme un sujet prioritaire qui nécessite l'attention des plus hautes instances politiques, contrairement à d'autres pays où ces responsabilités sont directement rattachées au bureau du président ou du premier ministre. C'est quelque chose qui nous distingue de nos alliés.

Mme Christine Normandin: Cela m'amène à ma prochaine question.

Concernant le développement de la cybercapacité, entre autres, dans le domaine militaire, pouvez-vous nommer des pays dont nous pourrions nous inspirer davantage?

M. Benoît Dupont: Il y a quelques initiatives intéressantes en Europe dont nous pourrions certainement nous inspirer. Notamment, au Royaume-Uni, les forces armées ont créé une réserve de cyberdéfense pour attirer des gens du secteur privé pour travailler temporairement sur des questions de sécurité nationale.

Mon collègue Christian Leuprecht a parlé aussi d'un parcours de recrutement spécifique, en Allemagne, qui permet d'attirer des gens dans des carrières militaires. Ils obtiennent le rang de lieutenant-colonel et des compétences très particulières, ce qui accélère leur intégration. La France a mis en place une réserve de cyberdéfense également.

Effectivement, il y a des initiatives très intéressantes dans certains pays. Certains d'entre eux ont la même taille que le nôtre et n'ont pas forcément les ressources illimitées des États-Unis. Nous pourrions donc nous inspirer de certaines de ces initiatives.

Mme Christine Normandin: Peut-on penser que c'est justement ce genre d'initiatives qui a fait que certains pays sont devenus membres de l'AUKUS, contrairement au Canada, qui n'en est pas membre et qui accuse un retard?

M. Benoît Dupont: Oui. Cela dépend de la priorité qui est accordée à ces questions et des investissements qui y ont été consentis au cours des dernières années, effectivement.

Mme Christine Normandin: Je vais préparer un peu le terrain pour notre prochaine étude.

Vous avez parlé de recrutement. Les Forces armées canadiennes devraient-elles revoir leurs critères de recrutement lorsqu'il s'agit d'aller chercher des gens spécialisés?

Devraient-elles éliminer certains aspects de la formation qui sont plus techniques ou plus liés au terrain et éviter les mutations, qui découragent plusieurs personnes?

Devrait-on se concentrer davantage sur les compétences plutôt que sur la formation militaire générale?

M. Benoît Dupont: Effectivement, les compétences très spécialisées qui sont requises nécessitent que les gens puissent avoir la garantie qu'ils vont rester dans ces fonctions plusieurs années.

Également, il y a des questions salariales qui sont importantes. Même si les gens qui considèrent ces carrières dans l'armée sont des gens qui ne sont pas motivés par l'appât du gain, il faut quand même qu'on puisse leur offrir des salaires concurrentiels par rapport à ceux du secteur privé, qui est en mesure d'offrir d'excellentes rémunérations dans ce domaine. Donc, il faut aussi réfléchir au système de rémunération pour ce type de fonctions particulières.

● (1700)

Mme Christine Normandin: Vous avez parlé, dans votre exposé, de la souveraineté numérique. Pouvez-vous préciser ce que vous entendez par là?

Voulez-vous dire que le gouvernement devrait conserver le numérique comme sa chasse gardée?

Cela ouvre-t-il la porte à la collaboration avec le secteur privé?

M. Benoît Dupont: Quand je parle de la souveraineté numérique, je fais allusion au fait qu'on développe, au Canada, des entreprises et des ressources qui sont capables de produire des technologies et des services canadiens liés à ces questions technologiques et stratégiques. Il s'agit d'aider à développer des entreprises et des industries canadiennes qui vont pouvoir vendre des produits à l'extérieur du pays, mais aussi fournir à nos forces armées des technologies auxquelles on peut faire totalement confiance.

Mme Christine Normandin: Ce serait sans égard à l'aspect public ou privé.

M. Benoît Dupont: C'est exact.

Mme Christine Normandin: D'accord, merci beaucoup.

Il me reste peu de temps, mais peut-être aurez-vous le temps de me répondre.

Quand on analyse des cyberattaques liées à des rançons, comparativement à celles qui visent à déstabiliser un pays, est-ce qu'on cherche les mêmes choses? Les analyse-t-on de la même façon? Cherche-t-on les mêmes compétences dans les équipes de cyberdéfense dans les deux cas?

M. Benoît Dupont: Oui, ce sont les mêmes compétences qui sont requises pour faire les mêmes types d'analyse et pour déterminer quel type de réponse on doit apporter. La seule exception, dans le cas des rançons, c'est qu'il y a des compétences additionnelles de négociation qui peuvent être mises en œuvre, mais c'est plutôt le cas du côté du secteur privé.

Mme Christine Normandin: Je vous remercie beaucoup.

Je pense que mon temps est écoulé.

[*Traduction*]

Le président: Merci.

Madame Mathyssen, vous disposez de cinq minutes. Je vous en prie.

Mme Lindsay Mathyssen: Merci beaucoup.

Monsieur Dupont, j'ai été très impressionnée par votre description de certaines technologies qui progressent. Je me sentais aussi vieille que notre président...

Des députés: Oh, oh!

Mme Lindsay Mathyssen: ... en ce qui concerne les interfaces neuronales. J'aimerais en apprendre beaucoup plus à ce sujet.

Pouvez-vous nous en dire plus sur les technologies que vous décriviez?

M. Benoît Dupont: Quand je parlais d'interface neuronale, il s'agit d'un nouveau type de technologie qui tente de connecter le cerveau humain aux machines afin d'accélérer la communication entre les deux. Par exemple, Elon Musk investit beaucoup d'argent dans une société qui s'appelle Neuralink, qui essaie d'implanter des électrodes dans le cerveau humain afin de communiquer beaucoup plus rapidement, et plus efficacement, avec les ordinateurs. L'objectif initial est de combiner l'intelligence artificielle et l'intelligence humaine.

Ce n'est pas de la science-fiction. C'est ce qui se passe en ce moment même en recherche et développement.

Mme Lindsay Mathyssen: Je crois en avoir entendu parler. C'est la possibilité de contourner parfois certaines mauvaises connexions. Par exemple, si une personne a eu un accident et que sa moelle épinière ne fonctionne pas comme elle le devrait, ces liaisons neuronales permettent alors de la contourner. Est-ce de cela que vous parlez explicitement? Est-ce l'un des exemples de ce dont vous parlez essentiellement?

M. Benoît Dupont: C'est l'un des exemples. C'est l'un des premiers cas d'utilisation, mais les applications seront beaucoup plus larges.

Mme Lindsay Mathyssen: Pouvez-vous nous en dire plus en ce qui concerne la défense et l'armement? Parlez-vous de l'industrie de la défense?

M. Benoît Dupont: Oui. On pourrait envisager d'implanter des interfaces neuronales dans le cerveau de soldats pour en faire des combattants beaucoup plus efficaces.

Mme Lindsay Mathyssen: À votre avis, dans combien de temps verrons-nous ces applications?

M. Benoît Dupont: C'est difficile à savoir, car tout cela est très secret et confidentiel. C'est en développement. Il y a des articles et des documentaires. Des investisseurs investissent des millions de dollars dans ces technologies. C'est sûr que ça s'en vient.

Mme Lindsay Mathyssen: Compte tenu de l'incapacité de Tesla à mettre au point une technologie de conduite autonome aussi rapidement qu'elle le souhaitait, j'imagine qu'il y a passablement d'obstacles sur la route, sans mauvais jeu de mots.

Les gouvernements du monde entier, à l'échelle internationale et au Canada, ont-ils un cadre législatif? Sont-ils sur le point d'offrir des protections contre ce nouveau type de technologie dont vous parlez, pas seulement les liaisons neuronales, mais les autres technologies dont vous parliez?

● (1705)

M. Benoît Dupont: Je ne suis pas au courant de la présentation de projets de loi. Je suis sûr que ces technologies seraient assujetties aux cadres de réglementation de la santé publique et des produits pharmaceutiques.

Mme Lindsay Mathyssen: Vous avez fait référence aux discussions de M. Leuprecht — et ici, c'est toujours Mme Normandin qui me vole mes questions — au sujet du recrutement, du maintien en fonction et de la concurrence que les Forces armées canadiennes et nos forces de sécurité doivent affronter de la part de sociétés pour les postes non pourvus en informatique au sein de nos institutions. En fait, il est question d'une grande partie de ces activités de recrutement et de maintien en fonction dans le document du MDN intitulé « Protection, Sécurité, Engagement », mais sa rédaction date aussi de plusieurs années.

Est-ce que cela correspond toujours à ce dont nous avons besoin? Devons-nous actualiser ce besoin? Où en sommes-nous dans la direction prise par le gouvernement en ce qui concerne le recrutement et le maintien en fonction?

M. Benoît Dupont: Je pense que les besoins sont toujours très grands. Les types de profils dont nous avons besoin sont à peu près les mêmes. Nous avons besoin de personnes qui possèdent une formation technique. Elles sont très demandées, non seulement par le secteur privé dans le domaine de la cybersécurité, mais aussi par d'autres secteurs dans le développement de l'IA et des jeux vidéo. Toutes les industries informatiques sont avides de tous ces gens et elles se livrent une concurrence féroce pour attirer ces gens talentueux.

Le président: Merci, madame Mathyssen, pour cette merveilleuse série de questions sur les liaisons neuronales. Nous attendons avec impatience les cinq minutes de questions de Mme Gallant.

Madame Gallant, vous disposez de cinq minutes.

Mme Cheryl Gallant: Merci, monsieur le président.

Monsieur Hewie, vous avez parlé des attaques de SolarWinds dans le contexte de la défense nationale du Canada.

M. John Hewie: J'ai parlé de SolarWinds dans le contexte de la nouvelle tendance que nous observons chez les États-nations adverses, mais surtout chez la Russie, à compromettre la chaîne d'approvisionnement. Ce que j'entends par « compromettre la chaîne d'approvisionnement », c'est qu'au lieu de s'en prendre individuellement à une entité donnée, ces acteurs vont s'en prendre aux logiciels ou aux systèmes technologiques que ces entreprises utilisent et essayer de les compromettre.

Dans le cas de SolarWinds, la compromission de la société SolarWinds elle-même, dont le logiciel est utilisé par de nombreuses entreprises dans le monde, y compris des gouvernements, a été attribuée à la Russie. Les données dont nous disposons indiquent que la seule compromission de SolarWinds a fini par se répercuter sur plus de 18 000 organisations dans le monde.

Mme Cheryl Gallant: La portée de l'attaque contre SolarWinds fait-elle toujours l'objet d'une enquête?

M. John Hewie: Je n'ai pas de détail à vous fournir sur l'état actuel de cette enquête.

Mme Cheryl Gallant: Aucun logiciel de la défense nationale canadienne n'a été touché par cette attaque. Est-ce bien ce que vous dites?

M. John Hewie: Je ne suis pas au courant d'une façon ou d'une autre.

Mme Cheryl Gallant: Vous avez mentionné FoxBlade tout à l'heure. Savez-vous s'il est utilisé ou non contre des membres de l'OTAN?

M. John Hewie: Je n'ai pas non plus d'information à ce sujet, mais je peux dire que ce n'est pas la première fois qu'un acteur étatique utilise ce maliciel destructeur.

Mme Cheryl Gallant: FoxBlade aurait-il le potentiel d'engendrer une mortalité massive?

M. John Hewie: Je suppose que s'il visait des infrastructures essentielles et entraînait une chaîne de défaillances catastrophiques, il pourrait certainement avoir une incidence néfaste sur les vies humaines.

Mme Cheryl Gallant: Il y a l'expression « technologie d'émulation de menaces » telle qu'elle s'applique à Cobalt Strike. Qu'est-ce que cela signifie et comment serait-elle appliquée ou utilisée contre notre défense nationale?

● (1710)

M. John Hewie: Je suis désolé, je ne connais pas l'expression « technologie d'émanation de menaces »?

Mme Cheryl Gallant: C'est « technologie d'émulation de menaces ».

M. John Hewie: Technologie d'émulation de menaces... Non, je suis désolé, je ne connais pas cette expression non plus.

Mme Cheryl Gallant: D'accord.

Le CST estime qu'il est très peu probable que des auteurs de cybermenaces cherchent à perturber intentionnellement les infrastructures essentielles canadiennes et à causer des préjudices importants ou des pertes de vie.

Cela dit, dans quelle mesure sommes-nous vulnérables avec l'Internet des objets, étant donné qu'un objet aussi simple que votre réfrigérateur envoie des pings? Il semble y avoir tellement de vulnérabilités et c'est la voie d'accès la moins protégée qui sera attaquée, alors comment le CST peut-il être si confiant, selon vous, qu'il est peu probable que ces infrastructures soient perturbées?

M. John Hewie: À mon avis, il est vraiment difficile de prédire l'avenir dans cet espace, et c'est pourquoi nous avons vu le thème du besoin de collaborer sur l'échange de renseignements et la recherche de différentes façons de lutter contre ces menaces, pas seulement du point de vue défensif, mais en préconisant des choses comme ce que Microsoft fait en ce qui concerne nos objectifs de paix numérique et en préconisant des cybernormes du comportement acceptable dans le cyberespace afin qu'il y ait des conséquences pour ces acteurs.

Pour répondre plus précisément à votre question sur l'Internet des objets, Microsoft et de nombreux autres acteurs de l'industrie s'inquiètent du fait que l'on connecte ces appareils à Internet à un rythme effréné et qu'il n'y a pas nécessairement de structure ni d'organisation parmi les fournisseurs ni même de réglementation pour garantir que ces appareils sont construits et sécurisés dès la conception et qu'ils sont exploités en toute sécurité, ou même que le fournisseur puisse les mettre à jour plus tard. Ces objets sont des cibles faciles à compromettre pour les acteurs qui les utiliseront ensuite contre les gouvernements, les infrastructures essentielles, Microsoft ou toute autre organisation dans le cadre d'une cyberattaque.

Mme Cheryl Gallant: Je n'ai pas eu l'occasion de poser cette question au premier tour, mais GiveSendGo, une plateforme basée aux États-Unis, a été piratée. Savez-vous qui est l'auteur présumé ou soupçonné de ce piratage?

M. John Hewie: Je suis désolé, nous n'avons pas d'information sur cette situation.

Le président: Merci, madame Gallant.

Monsieur Kelloway, bienvenue au Comité.

M. Mike Kelloway (Cape Breton—Canso, Lib.): Merci de m'accueillir, monsieur le président.

Bonjour à mes collègues, au personnel et aux témoins.

Permettez-moi de dire, monsieur le président, qu'à mon avis, loin de vieillir, vous vous améliorez.

Le président: Vous disposez maintenant de 10 minutes.

M. Mike Kelloway: Je dispose maintenant de 10 minutes?

Des voix: Oh, oh!

M. Mike Kelloway: C'est fantastique.

Je tiens à vous remercier de vos déclarations liminaires et de vos réponses à un grand nombre des excellentes questions qui vous ont été posées.

J'aimerais revenir sur un point en particulier. Monsieur Hewie, je pense que vous avez souligné l'importance d'examiner la cybersécurité dans une perspective intégrée. Cela comprend le gouvernement, le secteur privé et le milieu universitaire.

J'ai quelques questions, et elles s'adressent aussi à M. Dupont. Pouvez-vous nous donner un exemple dans lequel ce cadre intégré fonctionne bien?

Le deuxième élément concerne ceci. Je vais vous brosser un tableau. Vous avez l'occasion de parler de cette collaboration entre le secteur privé, les gouvernements et le milieu universitaire. Quelles sont les trois premières recommandations que vous nous feriez pour que nous les examinions concrètement et de façon approfondie?

Nous pourrions commencer par M. Hewie, puis passer à M. Dupont.

Merci.

M. John Hewie: J'aimerais vous faire part d'un exemple très opportun et très proche de nous, à savoir le travail que Microsoft a accompli. J'ai évoqué notre collaboration de longue date avec le Centre de la sécurité des télécommunications et le Centre canadien pour la cybersécurité. Une partie des renseignements sur les menaces que le Centre canadien de cybersécurité collecte et conserve, dans le cadre de ce qu'il voit au moyen de ses différents capteurs et lentilles et qui sont communiqués aux infrastructures essentielles ici au Canada est aussi communiquée à Microsoft. Cela s'est fait au cours des deux dernières années de façon automatisée.

Ces indicateurs et signaux fournis par le Centre canadien pour la cybersécurité finissent par contribuer à améliorer les protections de tous les produits et services de Microsoft à l'échelle mondiale dans le nuage. Ils contribuent à fournir ce niveau de protection supplémentaire aux clients du monde entier et du Canada, y compris le gouvernement canadien et les organisations de consommateurs du monde entier.

C'est un très bon exemple de partenariat avec l'industrie qui a une incidence réelle grâce à l'échange de renseignements clés.

● (1715)

M. Mike Kelloway: Allez-y, monsieur Dupont.

M. Benoît Dupont: Un autre excellent exemple est l'ECMC — l'Échange canadien de menaces cybernétiques — qui réunit 150 sociétés canadiennes. Il leur fournit des renseignements sur les menaces provenant du Centre canadien pour la cybersécurité, mais le secteur privé combine aussi tous ces [*difficultés techniques*] renseignements et les communique aux entreprises canadiennes, petites et grandes.

L'un des principaux problèmes est que nous avons beaucoup parlé des infrastructures essentielles, mais le Canada est un pays de petites et moyennes entreprises et celles-ci sont touchées par les rançongiciels et elles ne peuvent souvent pas se payer le même calibre de technologie de cybersécurité. Nous devons également réfléchir à la façon dont nous pouvons [*difficultés techniques*] nous devons y réfléchir davantage.

M. Mike Kelloway: Nous avons perdu les derniers instants.

Le président: Pourriez-vous répéter les dernières phrases, s'il vous plaît?

M. Mike Kelloway: Oui. Merci, monsieur Dupont.

M. Benoît Dupont: Vous voulez que je répète les dernières phrases?

Le président: Oui, nous avons été victimes d'un piratage russe.

M. Benoît Dupont: Il aurait pu être chinois.

Je disais simplement que le gouvernement canadien doit continuer à réfléchir à la façon d'aider les PME, les petites et moyennes entreprises, car elles emploient 95 % de la main-d'œuvre canadienne et fournissent de nombreux services et certaines fonctions essentielles aux grandes entreprises. Elles sont aussi visées par des attaques contre la chaîne d'approvisionnement et leurs ressources sont très limitées pour faire face aux problèmes de cybersécurité.

M. Mike Kelloway: Combien de temps me reste-t-il, monsieur le président?

Le président: Il vous reste 30 secondes.

M. Mike Kelloway: Très brièvement, la deuxième partie de ma question s'adresse à vous deux.

Si vous aviez l'occasion de parler à cette équipe de collaboration — les meilleurs et les plus brillants, pour ainsi dire — et si vous aviez une ou deux recommandations à leur faire, quelles seraient-elles? Commençons par une seule, pour gagner du temps.

M. John Hewie: La première est que les fondements de la cybersécurité sont plus importants que jamais. Quand je parle des « fondements », je parle de garder les systèmes à jour, d'utiliser des technologies modernes et d'activer des choses comme l'authentification multifactorielle.

À notre avis, pour toutes les attaques et les compromissions de clients dont nous avons connaissance, le respect des principes de base et l'activation de l'authentification multifactorielle permettraient d'en éviter la grande majorité. Malheureusement, bien que nous collaborions avec des organismes comme Pensez cybersécurité pour faire cette sensibilisation, il reste beaucoup d'amélioration à apporter en ce qui concerne les fondements.

Le président: Monsieur Dupont, vous allez devoir passer en douce cette réponse dans les deux minutes et demie dont Mme Normandin dispose.

Madame Normandin, vous avez deux minutes et demie.

[*Français*]

Mme Christine Normandin: Merci beaucoup, monsieur le président.

Ma question s'adresse aux deux témoins. Dans le cadre de la crise en Ukraine, nous avons beaucoup parlé du rôle des pirates informatiques de bonne foi, c'est-à-dire de ceux qui ont répondu à l'appel du président Zelenski et qui ont piraté certains réseaux de la Russie.

Monsieur Hewie, jusqu'à quel point ces pirates sont-ils bien vus?

Professeur Dupont, est-ce qu'ils peuvent présenter un risque à long terme, surtout si on les laisse aller et qu'on les encourage?

Par exemple, y a-t-il un risque qu'ils deviennent des voyous, parce qu'on n'a pas pu les contrôler, surtout si on les a encouragés?

J'aimerais que les deux témoins me fassent part de leur analyse du rôle de ces pirates informatiques de bonne foi et qu'ils me disent si nous devrions nous en inquiéter d'une certaine façon.

M. Benoît Dupont: Je vais intervenir le premier. Leur rôle complexifie encore plus le travail des agences gouvernementales, parce qu'il devient très compliqué de savoir qui fait quoi dans ce nouvel environnement dans lequel tout le monde peut s'improviser attaquant et peut répondre à des appels de très bonne foi, je ne le nie pas.

Le risque, c'est que certains de ces pirates, qui ne maîtrisent pas forcément toutes les nuances des systèmes qu'ils attaquent, puissent monter des attaques qui vont endommager des infrastructures critiques dans un pays comme la Russie et affecter la vie de civils russes, qui ne sont pas impliqués forcément dans les attaques contre l'Ukraine. Ces attaques risquent de déborder aussi dans d'autres pays au-delà de la Russie et d'être difficiles à contrôler.

Je pense qu'il faut prendre cela avec énormément de précautions, éviter de s'enthousiasmer et réfléchir avant à toutes les implications non contrôlées et non anticipées de ces attaques menées par des groupes isolés.

● (1720)

Mme Christine Normandin: Merci.

Monsieur Hewie, pouvez-vous répondre aussi?

[*Traduction*]

Le président: Vous avez environ 30 secondes.

M. John Hewie: Je voudrais réitérer la position de Microsoft, à savoir que nous ne soutenons certainement pas des activités cyberoffensives, principalement pour un certain nombre de raisons.

Nous avons constaté que les armes cybernétiques sont généralement très difficiles à cibler et que les dommages collatéraux risquent de s'étendre au-delà des cibles visées, un peu comme l'attaque NotPetya en Ukraine il y a quelques années, qui a fini par toucher des organisations du monde entier et dont la récupération a coûté des centaines de millions de dollars. C'est un exemple de dommage collatéral potentiel qui pourrait être extrême.

Le président: Je vous remercie.

Madame Mathyssen, en dépit de mon meilleur jugement, vous avez deux minutes et demie.

Mme Lindsay Mathyssen: Merci, monsieur le président.

Un problème majeur que nous avons constaté par rapport à cette menace à la cybersécurité est l'espionnage et le vol de propriété intellectuelle canadienne. Quelles recommandations nous feriez-vous pour lutter contre cette forme de vol numérique?

J'ajouterais qu'une grande partie de nos données sont gérées différemment d'une province à une autre. Quel défi cela représente-t-il par rapport aux protections offertes par la cybersécurité et des sociétés comme Microsoft?

La question s'adresse aux deux témoins.

M. John Hewie: Je pourrais peut-être commencer pour celle-ci et M. Dupont pourrait poursuivre.

Dans notre rapport sur la défense numérique, nous avons bien sûr décrit certaines activités que nous avons observées et détectées, notamment l'espionnage par certains États-nations adverses que j'ai déjà évoqué. Bien honnêtement, ces acteurs, qu'il s'agisse de cybercriminels ou d'acteurs étatiques, recherchent des failles dans notre protection, des failles dans nos processus et ils cherchent à les exploiter.

Les conseils généraux de Microsoft, qu'il s'agisse de protection contre l'espionnage ou d'autres types d'attaques par rançongiciel, seraient très franchement similaires. Nous encouragerions certainement les organisations possédant une propriété intellectuelle sensible, ou que nous pourrions appeler des « actifs de grande valeur » à investir dans des protections supplémentaires pour ces actifs de grande valeur, plutôt que d'essayer de protéger de la même façon tout ce qui se trouve dans l'organisation.

M. Benoît Dupont: Le gouvernement canadien a lancé un nouveau programme de sécurité de la recherche pour essayer d'aider, ou de forcer ou d'obliger les universités à mieux protéger leur propriété intellectuelle et à les sensibiliser. À mon avis, c'est une excellente initiative pour essayer de contrer la fuite de propriété intellectuelle canadienne.

Le gouvernement doit envisager d'aider les universités à financer ces nouveaux efforts qu'elles doivent déployer. Ce serait peut-être un conseil à donner.

Le président: Merci, madame Mathyssen.

Nous avons M. Motz pour cinq minutes. Je vous en prie.

M. Glen Motz: Merci beaucoup, monsieur le président.

Merci à nos témoins de leur présence.

Pour le bien de notre président, et pour vous ramener au tout début, nous pensons tous connaître les définitions, mais pouvez-vous tous les deux définir très brièvement ce qu'on entend par « cybersécurité » et nous préciser les différences entre « vulnérabilité », « menace » et « risque »?

M. John Hewie: Je peux peut-être tenter de répondre.

M. Glen Motz: Oui, s'il vous plaît, une réponse brève.

M. John Hewie: La « cybersécurité » consiste en fait à protéger votre infrastructure informatique ou votre identité dans le contexte numérique, sur Internet ou lors d'une connexion à un réseau. Il s'agit de ces protections de sécurité étendues au domaine cybernétique.

Une « vulnérabilité » est un problème au sein d'un code logiciel qu'un adversaire donné pourrait exploiter à des fins imprévues.

Les « menaces » peuvent être considérées comme un éventail d'organisations criminelles ou d'États-nations adverses.

Chez Microsoft, nous avons aussi collaboré avec le Citizen Lab de l'école Munk de l'Université de Toronto pour essayer de braquer les projecteurs sur ce que nous appelons les « acteurs offensifs du secteur privé » qui créent des logiciels espions destinés à être vendus à des gouvernements et à d'autres organisations.

En fait, le risque et la gestion du risque sont les éléments sur lesquels toutes les organisations cherchent à concentrer leurs efforts commerciaux. Il y a toujours un compromis entre les risques et les avantages et il n'y a qu'une quantité limitée d'argent et de ressources humaines…

● (1725)

M. Glen Motz: Je vais vous interrompre, monsieur Microsoft.

Monsieur Dupont, avez-vous quelque chose à ajouter ou quelque chose de substantiellement différent à ajouter?

M. Benoît Dupont: Eh bien, j'ajouterais que la cybersécurité ne consiste pas seulement à protéger les systèmes, mais aussi à protéger les renseignements qui y résident et à aider les personnes qui les utilisent à adopter les comportements qui renforceront concrètement l'ensemble de l'architecture des personnes, des machines et des renseignements qui travaillent de concert.

M. Glen Motz: D'accord. Bien. Merci beaucoup de ces réponses.

J'ai une dernière question pour vous deux. Plusieurs organisations canadiennes ont des politiques de divulgation responsable qui offrent des incitatifs financiers à ce que nous appelons les « pirates éthiques » pour qu'ils s'abstiennent de dévoiler des détails sur la sécurité et les vulnérabilités de logiciels qu'ils découvrent dans les produits ou les services de cette organisation jusqu'à ce qu'un correctif soit disponible.

Cependant, les personnes qui divulguent des vulnérabilités de sécurité dans un programme de divulgation responsable se plaignent souvent du fait que l'organisation à laquelle elles divulguent des renseignements ne respecte pas les règles du jeu. Parfois, une organisation qui a été avisée d'une vulnérabilité dans ses produits ou services en minimise l'importance afin de payer une prime moins élevée, n'accorde pas le mérite voulu aux pirates éthiques ou exige un délai déraisonnable avant la divulgation publique parce qu'elle n'est pas disposée à investir des ressources pour corriger la vulnérabilité.

Nous savons tous que cela met les Canadiens en danger. À votre avis, que devrait faire le gouvernement pour encourager les organisations à mettre en oeuvre des politiques de divulgation responsable afin d'empêcher ce genre d'activités?

M. Benoît Dupont: Le gouvernement pourrait peut-être offrir des déductions fiscales pour couvrir ces primes. Cela aiderait peut-être ces organisations à prendre ces primes plus au sérieux. Sinon, il pourrait réglementer ce domaine d'activité.

M. Glen Motz: Allez-y, monsieur Hewie.

M. John Hewie: Je dirais que Microsoft possède une assez grande expérience dans ce domaine précis. Nous serions certainement heureux de participer à des consultations et d'éclairer certains points de vue sur ce sujet particulier après votre séance.

Nous favorisons certainement la divulgation confidentielle des vulnérabilités. Nous collaborons avec une communauté et nous avons favorisé la création d'une communauté avec des chercheurs en sécurité du monde entier. Nous disposons de vastes programmes de primes aux bogues pour essayer d'orienter ces recherches vers les domaines de nos produits et services que nous estimons les plus sensibles ou dans lesquels nous aimerions voir davantage d'inspections. Bien honnêtement, nous avons constaté que cela fonctionne généralement très bien.

Il y a évidemment des situations où… Techniquement, ces correctifs sont des mises à jour visant à remédier à ces vulnérabilités et ils prennent du temps. Nous ne voulons pas déployer un correctif avant qu'il soit prêt, au risque de perturber l'infrastructure existante ou d'avoir des incidences négatives sur celle-ci.

Le président: Merci, monsieur Motz.

Les cinq dernières minutes iront à MM. May et Fisher.

M. Bryan May: Merci, monsieur le président.

Monsieur Hewie, je suis vraiment un néophyte, alors j'espère que vous pourrez simplifier vos explications et me guider. Vous avez parlé de la somme de travail nécessaire, du point de vue de Microsoft, pour détecter ces brèches et, évidemment, les colmater.

Pourriez-vous nous en dire un peu plus sur la brèche elle-même? Est-ce généralement Microsoft qui la découvre, plutôt que l'organisation ou un gouvernement?

M. John Hewie: Oui, absolument. Je dirais que les techniques les plus utilisées sont de deux ordres. Premièrement, les attaquants utilisent et exploitent des vulnérabilités dans les logiciels qui, pour la plupart, ont été corrigées par le fournisseur, mais le client, l'organisation ou l'agence n'a simplement pas encore eu l'occasion de déployer ce correctif.

M. Bryan May: Mais vous vous en apercevez en premier, non? Est-ce que c'est vous qui détectez ces brèches peut-être avant le gouvernement, ou même avant l'entreprise en question?

● (1730)

M. John Hewie: Dans le modèle de responsabilité partagée dans lequel nous fonctionnons pour les services en nuage, il y a une responsabilité en matière de sécurité à la fois pour le fournisseur du nuage et pour l'utilisateur final ou le client. Dans le cas d'attaques contre les identités, c'est-à-dire lorsque des personnes essaient d'accéder au nom d'utilisateur d'une autre personne, autrement dit son identifiant et son mot de passe, nous avons certainement vu des acteurs russes utiliser des mots de passe piratés et d'autres types de techniques, y compris l'hameçonnage, pour accéder à ces comptes.

Nous travaillons avec ces clients pour les avertir d'une activité suspecte lorsque nous voyons des tentatives de compromettre des comptes particuliers ou si nous détenons des renseignements qui nous permettent de détecter qu'ils ont été compromis.

M. Bryan May: À quoi ressemble cet arbre de décision? Je me demande à quel moment vous communiquez avec le gouvernement pour lui dire: « Nous avons détecté ceci. C'est un élément que nous devrions communiquer à l'ensemble de la communauté ».

M. John Hewie: Dans la grande majorité des cas, parce que ces systèmes sont massifs et étendus, l'outillage a été habilité de manière à ce que des alertes soient générées. C'est la responsabilité de l'utilisateur ultime, du client ultime, de surveiller lui-même ces alertes et ces activités suspectes.

M. Bryan May: Merci.

Je vais céder le reste de mon temps à M. Fisher si vous voulez bien.

M. Darren Fisher: Merci beaucoup, monsieur May, de partager votre temps avec moi.

Je dois dire que les deux témoins sont étonnants. Les renseignements que nous obtenons sont absolument étonnants. Je vous remercie tous les deux de votre présence.

Je n'ai pas beaucoup de temps, donc je suppose que ce sera une sorte de question éclair. En supposant que les bons et les méchants recherchent les jeunes cybercompétents d'aujourd'hui et de demain, qui a l'avantage pour obtenir cet ensemble de compétences? S'agit-il d'une guerre d'enchères pour que les personnes les plus intelligentes et les plus brillantes se rangent du côté du bien plutôt que du côté du mal?

J'ai regardé de votre côté par hasard, madame Gallant...

Mme Cheryl Gallant: Le mal.

Des voix: Oh, oh!

M. Benoît Dupont: Je pense que le côté du bien paie mieux que le côté du mal, donc je dirais qu'il y a un avantage pour les pirates au chapeau blanc.

M. John Hewie: Je serais du même avis que M. Dupont sous ce rapport.

Je pense que la communauté de la recherche sur la sécurité est un domaine où il y a une ligne éthique. Les chercheurs en sécurité qui recherchent des vulnérabilités peuvent faire essentiellement l'une des deux choses suivantes. Ils peuvent les transmettre au fournisseur, ce qui fait partie du programme de divulgation responsable et confidentiel des vulnérabilités, et les faire corriger ou ils peuvent les vendre à l'industrie cybercriminelle ou à d'autres.

Nous essayons d'offrir des programmes de « prime aux bogues » et d'autres structures d'encouragements pour encourager ces chercheurs en sécurité à se ranger du côté des bons.

M. Darren Fisher: Merci.

Cela m'amène en quelque sorte à ma dernière question, pour laquelle il me reste environ 45 secondes.

Monsieur Hewie, vous avez parlé du coût des violations de données. Comment les groupes, ces acteurs étatiques ou ces réseaux criminels, en tirent-ils profit autrement qu'en vendant les données?

M. John Hewie: Malheureusement, ils font preuve de beaucoup de créativité pour trouver des moyens de monétiser les données volées à des organisations.

Dans le cas des rançongiciels — je suis sûr que c'est un terme que la plupart des gens connaissent — il y a le cryptage conventionnel de vos fichiers et la demande de rançon en vue de vous remettre une clé pour les décrypter. Puis, il y a la deuxième étape où ils volent des données et les rendent publiques.

Au cours des dernières années, je pense que nous avons assisté à une professionnalisation de cette industrie criminelle, où ce n'est pas seulement un ou deux acteurs qui agissent, mais toute une économie d'acteurs.

Un autre exemple est celui des comptes compromis où un nom d'utilisateur et un mot de passe pour une organisation canadienne donnée sont compromis. Ils sont offerts sur le Web clandestin et vendus au plus offrant comme moyen d'accéder à cette organisation. Ils ont peut-être plus d'expérience dans le domaine des infrastructures essentielles ou de l'industrie minière et savent monétiser davantage les attaques contre ces organisations.

Le président: Merci, monsieur Fisher.

Voilà qui met fin à nos questions. Je tiens à remercier MM. Dupont et Hewie pour cet aperçu très éclairant et quelque peu inquiétant de ce nouveau monde. Je prendrai soin de ne plus parler à ma femme devant notre réfrigérateur.

Des voix: Oh, oh!

Le président: Sur ce, chers collègues, en supposant que je vive assez longtemps, nous aurons une autre séance mercredi prochain. Nous terminerons ainsi notre dernière heure. Au cours de la deuxième heure, nos estimés analystes nous présenteront au moins quelques chapitres d'un rapport. Si nous pouvions réfléchir à ce que nous voulons voir dans un rapport, ce sera très utile.

Nous allons lever la séance.