CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 125 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 20 septembre 2018

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le jeudi 20 septembre 2018

● (1635)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Mesdames et messieurs, nos témoins sont ici. Reprenons nos travaux.

Je crois que nos témoins ont l'expérience des comités parlementaires. Je souhaite donc la bienvenue à Scott et à Rajiv. Nous allons essayer d'être aussi informels que possible, mais il faut ce qu'il faut.

Le premier intervenant peut prendre la parole.

M. Scott Jones (chef adjoint, Sécurité des technologies de l'information, Centre de la sécurité des télécommunications): Bonjour, monsieur le président et membres du Comité.

Je m'appelle Scott Jones. Je suis heureux d'être de retour. Je suis le chef adjoint de la sécurité des TI au Centre de la sécurité des télécommunications et le chef désigné du futur Centre canadien pour la cybersécurité.

Je suis accompagné aujourd'hui de Rajiv Gupta, directeur des Normes, Architecture et atténuation des risques. Merci de nous avoir invités à discuter de ce sujet très important.

[*Français*]

Le Centre de la sécurité des télécommunications est la principale autorité technique et opérationnelle responsable de la cybersécurité au gouvernement du Canada. On lui a confié le mandat de protéger les renseignements et les infrastructures d'information d'importance pour le gouvernement du Canada.

Cette expertise est l'aboutissement de plus de 70 années d'existence. La protection des communications du gouvernement fait en effet partie de la mission du CST depuis sa création en 1946. À l'époque, le Centre se nommait la Direction des télécommunications du Conseil national de recherches du Canada.

[*Traduction*]

Il va sans dire que le monde de 1946 était bien différent du monde d'aujourd'hui. Ce qui n'a pas changé, cependant, c'est la nécessité d'un leadership innovateur et compétent pour relever les défis d'un monde en évolution.

Annoncée en juin 2018, la nouvelle Stratégie nationale de cybersécurité du Canada tient compte de cette réalité et reflète la vision du Canada pour la sécurité et la prospérité dans l'ère numérique. La création du Centre canadien pour la cybersécurite, qui sera chapeauté par le Centre de la sécurité des télécommunications, faisait partie des nouvelles mesures proposées dans la Stratégie.

Combinés aux investissements prévus au budget de 2018, ces efforts nous permettront de faire preuve de résilience face aux cybermenaces et de continuer de protéger la sécurité des Canadiens. Et bien des choses valent la peine d'être protégées.

[*Français*]

Les récentes innovations technologiques ont donné lieu à de formidables occasions d'assurer la croissance économique au Canada. Il ne faut pas sous-estimer les nombreux avantages offerts par la numérisation grandissante de notre société.

Internet a considérablement simplifié la vie des Canadiens. Le gouvernement fédéral offre plusieurs services en ligne. Les investissements prévus au budget de 2018 pour le renforcement des services numériques constituent un signe probant que le gouvernement entend miser sur des technologies nouvelles et innovantes.

Or, pour pouvoir tirer avantage du commerce électronique, les Canadiens doivent être en mesure de mener de telles activités en toute confiance. Les risques ne devraient pas nous dissuader d'adopter les nouvelles technologies, mais être pris en compte et atténués.

[*Traduction*]

Malheureusement, nous savons tous comment les cybercompromissions peuvent entraîner d'importantes pertes financières, mener au vol de propriété intellectuelle et causer des dommages à la réputation d'une entreprise ou d'un individu. Par exemple, les récentes attaques par rançongiciels ont mis en evidence la menace grandissante que représente la cybercriminalité, de même que les répercussions d'une cybercompromission.

De nos jours, les auteurs de cybermenaces sont animés par de multiples motivations et disposent de capacités diverses. Parmi eux, on retrouve les auteurs parrainés par des États, les hacktivistes et les terroristes capables de commettre une vaste gamme d'activités perturbatrices allant des attaques par déni de service à l'exposition des renseignements personnels.

Le CST joue un rôle essentiel pour ce qui est de les empêcher d'atteindre leurs objectifs. Son expertise lui permet de détecter, d'endiguer et de contrer les graves cybermenaces visant les réseaux et les systèmes du Canada.

[*Français*]

Les trois clés de son succès sont les partenariats, l'attribution de pouvoirs appropriés et les compétences.

Commençons par les partenariats.

La sécurité, c'est l'affaire de tout le monde. Nos relations avec l'industrie sont primordiales pour protéger le Canada et les Canadiens contre les cybermenaces.

Toutes aussi importantes sont nos relations avec les autres ministères et organismes du gouvernement, notamment Sécurité publique Canada, Services partagés Canada, la GRC et le Service canadien du renseignement de sécurité.

En plus de tisser des partenariats avec le gouvernement et le secteur privé, le CST conclut des partenariats avec des universités et des groupes de recherche de pointe.

● (1640)

[*Traduction*]

Le Centre canadien pour la cybersécurité améliorera grandement notre capacité de collaborer avec le secteur privé, les autres partenaires du gouvernement et le milieu universitaire, puisqu'il rassemblera les principales unités opérationnelles de cybersécurité du gouvernement du Canada. II proposera une source unifiée de conseils, d'orientations, de services et de soutien spécialisés concernant les questions opérationnelles liées à la cybersécurité. Ainsi, les Canadiens pourront compter sur une source bien établie et fiable de conseils sur la cybersécurité.

II importera également d'assurer la continuité des fonctions assumées par le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique une fois que ses responsabilités auront été confiées au Centre pour la cybersécurité. Plus particulièrement, un élément essentiel du travail effectué par le CCRIC est d'aviser les victimes advenant une cybercompromission. II s'agit d'un rôle important que nous continuerons d'exercer par l'entremise du Centre pour la cybersécurité.

[*Français*]

Deuxièmement, j'aimerais parler des pouvoirs du CST.

Comme il a été établi lors des débats sur le projet de loi C-59, le CST conservera son mandat actuel de cybersécurité et d'assurance de l'information et se verra confier, en vertu de la loi proposée, un nouveau pouvoir afin de défendre les réseaux essentiels autres que ceux du gouvernement du Canada.

La Loi sur le Centre de la sécurité des télécommunications qui est proposée permettra également au CST d'échanger des informations concernant les cybermenaces avec les propriétaires de systèmes autres que ceux du gouvernement du Canada de manière à ce qu'ils puissent protéger adéquatement leurs réseaux ainsi que les informations qui y sont conservées. Par exemple, le CST pourra communiquer davantage d'informations sur des cybermenaces précises aux propriétaires d'infrastructures essentielles, comme les entreprises de communications ou le secteur bancaire.

[*Traduction*]

Enfin, la Loi sur le CST conférera au CST les pouvoirs nécessaires pour prendre des mesures en ligne pour défendre les réseaux importants du Canada et pour arrêter de façon proactive les cybermenaces avant qu'elles n'atteignent ces réseaux. Ces nouveaux pouvoirs permettront d'assurer une protection accrue des renseignements et des réseaux informatiques essentiels contre les compromissions, et de renforcer les mesures de cyberdéfense du Canada.

Troisièmement, les gens. Parmi les nouvelles mesures introduites dans la Stratégie nationale de cybersécurité, on retrouve la nécessité de financer le perfectionnement des compétences canadiennes liées à la cybersécurité. Le CST a la chance de pouvoir compter sur des Canadiens incroyablement brillants et talentueux pour s'attaquer aux enjeux complexes de la cybersécurité. Pour continuer dans cette voie, nous devrons toutefois tirer parti de ces compétences et investir l'exceptionnelle force intellectuelle du Canada dans la cybersécurité.

[*Français*]

Grâce à de solides partenariats, à l'attribution de pouvoirs appropriés et à un effectif compétent, le CST pourra s'efforcer de contrer les cybermenaces visant le Canada. Par contre, la cybersécurité est la responsabilité de tous. Pour assurer notre résilience, il faudra pouvoir compter sur l'expertise et sur l'esprit d'innovation de chacun d'entre nous.

Nous vous remercions de votre invitation. Nous serons heureux de répondre à vos questions.

[*Traduction*]

Le président: Merci, monsieur Jones.

[*Français*]

Monsieur Picard, vous disposez de sept minutes.

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

Ma question sera d'ordre plus général, pour vous permettre de nous fournir une réponse plus détaillée.

La création de ce nouveau centre survient alors que vous avez clairement établi le niveau de risque auquel nous faisons face en matière de cybersécurité, toutes menaces confondues. Ce nouveau centre est donc mis sur pied pour répondre à un problème bien établi, c'est-à-dire pour faire face à des menaces précises et en constante évolution.

À son premier jour d'existence, de quelle expertise et de quels instruments de qualité disposera ce centre pour faire face à la réalité actuelle? Comme les menaces auxquelles il devra faire face sont déjà bien enclenchées, ce centre accusera-t-il un certain retard? Quels buts visera-t-il à court terme et quels seront vos besoins pour les atteindre?

M. Scott Jones: Merci de votre question.

La première étape est d'établir le centre. Comme vous l'avez dit, c'est une tâche un peu bureaucratique.

● (1645)

[*Traduction*]

À mon avis, les principales priorités du cybercentre consisteront à établir la confiance et la crédibilité nécessaires pour travailler avec le secteur privé. Nous devons nous faire entendre haut et fort pour accroître nos attentes—dans le secteur privé et gouvernement—alors que nous examinons les défis en matière de sécurité auxquels nous sommes tous confrontés et que nous commençons à avoir des discussions plus ouvertes sur les menaces. Trop souvent, nous nous concentrons sur la menace après et non sur l'activité menaçante et sur la façon d'améliorer notre effort.

La première chose à faire est d'accroître la résilience. La résilience du Canada, en général, est faible. Nous ne parlons pas des choses les plus simples à faire, au moment où nous cherchons à nous défendre contre la menace la plus sophistiquée. En réalité, quelques choses simples peuvent nous permettre d'améliorer notre effort à tous et nous rendre plus immunisés et plus résilients face à des menaces fondamentales comme la cybercriminalité, alors cela peut être aussi simple que de réparer nos systèmes. L'un des premiers objectifs est de communiquer ce message, et d'obtenir des conseils simples et directs que tous les Canadiens peuvent prendre et utiliser.

La deuxième chose à faire concerne évidemment l'établissement d'un centre où, s'il y a un incident, nous sommes capables de gérer la situation. Nous avons fait un certain nombre d'exercices au cours de l'été pour nous assurer que nous sommes prêts à gérer tout incident, qu'il soit important ou petit, de portée internationale ou nationale, au sein du gouvernement fédéral ou dans le secteur privé, pour veiller à être prêts à faire notre part afin de pouvoir, dès le départ, exercer un leadership fédéral, en travaillant avec la victime ou avec d'autres administrations pour nous assurer que nous sommes prêts à gérer un incident.

Je pense que ce sont les deux éléments clés.

M. Michel Picard: Vous venez de parler de réparation. Est-ce que la réparation d'un système est une approche temporaire de la solution que vous envisagez, ou est-ce une façon permanente de travailler, en fonction du système que nous avons actuellement, plutôt que de repenser notre système?

M. Scott Jones: À l'heure actuelle, avec l'environnement que nous avons, la réparation est l'un des aspects clés de l'amélioration de notre cybersécurité. Les entreprises distribuent des correctifs. Le modèle dans l'industrie consiste à « commercialiser rapidement et corriger ensuite ce qui ne fonctionne pas ». Il en va de même pour les éléments de sécurité. À mesure qu'ils découvrent de nouvelles failles et de nouvelles façons de compromettre les systèmes, les fournisseurs publient des mises à jour logicielles. Il est important de les appliquer très rapidement et avec diligence à nos systèmes.

M. Michel Picard: Il a été mentionné que nous autoriserons des tactiques offensives afin de mieux protéger notre système.

D'un point de vue diplomatique, comment voyez-vous l'impact d'une attaque offensive plutôt que d'une approche défensive? Nous en avons parlé avec je ne me souviens plus quel commissaire. Je lui ai demandé s'il considérait une attaque offensive comme un acte de guerre.

M. Scott Jones: Je pense que l'élément clé est que des cyberopérations défensives sont proposées dans le projet de loi C-59. C'est un outil que nous pouvons utiliser pour contrer toute cyberactivité malveillante.

Il y a plusieurs éléments. La première concerne l'autorisation d'entreprendre cette activité. Il incombe au {ministre de la Défense nationale, en consultation avec le {ministre des Affaires étrangères, de veiller à ce qu'il soit tenu compte des relations extérieures.

Mais ce ne serait pas la première mesure, si vous preniez une mesure défensive. Vous voudriez augmenter les défenses de votre réseau. Vous devriez essayer d'accroître votre résilience face à l'activité malveillante. S'il n'y avait pas d'autre option, vous vous tourneriez vers ce genre d'activité au fur et à mesure que la situation s'aggraverait.

Il y a un certain nombre d'autres choses que nous pourrions faire. Si l'activité provenait d'un acteur étranger, nous mobiliserions la communauté internationale du CCRIC. Le Centre canadien de réponse aux incidents cybernétiques entretient des relations partout dans le monde avec les équipes nationales d'intervention en cas d'urgence informatique. Nous pourrions leur demander de l'aide. Nous nous tournerions certainement vers l'application de la loi, si c'était une meilleure option.

M. Michel Picard: Cette semaine, nous avons reçu le Comité de la justice de la Norvège. Une de leurs préoccupations était le manque d'expertise, de capacité de répondre aux menaces.

Comment évaluez-vous l'expertise réelle qui permet de composer avec la situation dès le début? Comment répondez-vous au besoin d'une plus grande ou d'une meilleure expertise?

Le président: Soyez très bref, s'il vous plaît.

M. Scott Jones: L'expertise est un aspect relativement auquel nous devons faire deux choses.

À court terme, nous devons regarder au-delà des domaines traditionnels de l'informatique et du génie. Il y a d'autres compétences à mettre à profit. Il y a des compétences qui sont très proches des capacités d'analyse en cybersécurité.

À long terme, il s'agit de bâtir une coalition avec les universités et les collèges, afin d'attirer plus de gens dans le domaine. Il subsiste une sous-représentation des femmes en sciences, en technologie, en génie et en mathématiques. Il y a là un vaste marché inexploité.

Les inscriptions dans ces domaines sont en baisse dans les universités, et pourtant, un impressionnant nombre d'emplois sont créés. Comment attirer des gens dans ce domaine? C'est l'un des objectifs de l'enseignement supérieur, mais j'aimerais assurément que les inscriptions augmentent et que plus de gens participent, à long terme.

● (1650)

Le président: Merci, monsieur Picard.

Monsieur Motz, vous avez sept minutes.

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

Merci d'être ici aujourd'hui.

Nos alliés du Groupe des cinq, par exemple, se sont prononcés contre Huawei, et je suppose que beaucoup de gens se demandent pourquoi le Canada n'en fait pas autant. Comme nous le savons, leurs activités au Canada pourraient évidemment créer des atteintes à la vie privée qui pourraient avoir une incidence sur notre réseau du Groupe des cinq.

Notre pays, ou votre établissement, a-t-il l'obligation d'emboîter le pas à nos alliés en matière de cybersécurité?

M. Scott Jones: Il est important, lorsque nous examinons nos réseaux de télécommunications, d'adopter l'approche selon laquelle nous voulons vraiment les considérer comme un système complet et nous défendre contre toutes les formes de cyberrisques. Nous abordons la question sous différents angles. Premièrement, il faut s'assurer que nous augmentons la résilience partout, peu importe d'où vient le produit. Nous voulons intégrer des mesures de sécurité, quoi qu'il arrive.

Comment vous assurez-vous que la chaîne d'approvisionnement est adéquatement protégée, par exemple, en vous assurant que vous importez des produits qui ont de bonnes pratiques de sécurité, qui sont intégrés à la fabrication du produit? Comment utiliser la technologie de façon sécuritaire? Vous pourriez prendre un produit très sûr, par exemple, mais si vous l'ouvrez au monde, vous pouvez rendre vulnérable notre technologie très rapidement.

Nous avons une relation très bien établie avec tous les fournisseurs de services de télécommunications au Canada. Je pense qu'il est important de relever la norme de résilience, peu importe le fournisseur, peu importe d'où vient l'équipement, et de travailler en collaboration dans cet objectif commun. Il s'agit vraiment de s'attaquer à tous les risques, et pas seulement à un seul.

M. Glen Motz: Je vous en remercie.

Nous avons entendu les experts au cours de la première heure. Je veux poser la question qu'ils ont soulevée, je crois. Il serait bon d'avoir votre point de vue là-dessus.

Comment le CST concilie-t-il la tension, la tension dans les relations, entre les tactiques défensives et offensives en ce qui concerne notre programme de cybersécurité et son incidence sur notre infrastructure ou sur tout aspect de notre pratique et de notre programme canadiens?

M. Scott Jones: Nous en parlons. Nous veillons à ce que la décision soit dans l'intérêt de la sécurité du Canada. Nous examinons le portrait d'ensemble. Nous voulons nous assurer que le Canada dispose de réseaux sûrs et résilients qui sont capables de fonctionner d'une manière qui inspire confiance. En même temps, l'on se rend compte qu'il y a des outils qui sont nécessaires pour recueillir des renseignements et qu'il y a des techniques qui sont nécessaires. Nous devons trouver un équilibre entre ces deux aspects.

Au bout du compte, cependant, notre système est conçu pour... Nous nous en remettrons à la défense, c'est-à-dire protéger le Canada et prendre la décision qui s'impose. En réalité, les décisions sont beaucoup plus claires que cela. Il est très rare que nous ayons des questions à nous poser. Les décisions sont très évidentes. S'il s'agit de la sécurité du Canada, c'est-à-dire la divulgation de renseignements à des fins de défense—la protection de la cybersécurité, les mises à jour, et ainsi de suite—nous n'hésitons pas une seconde.

Si c'est une mesure qui nous permet de protéger le Canada contre le terrorisme et d'obtenir des renseignements étrangers adéquats, nous allons prendre cette décision, mais nous savons toujours que, quoi qu'il arrive, il y aura un examen. Nous allons devoir rendre compte immédiatement au commissaire du CST et, au bout du compte, au tribunal de l'opinion publique, si nous prenons la mauvaise décision. Nous tenons compte d'un certain nombre de facteurs de cette façon.

M. Glen Motz: Nous avons entendu dans les échanges sur le projet de loi C-59 que comme au hockey, l'entraîneur est important. L'on dit que la meilleure défensive est l'attaque. Je suis intrigué par la façon dont nous nous en remettons toujours, ou implicitement, à une position défensive, quand cette position défensive pourrait être offensive.

M. Scott Jones: Cette analogie a ses limites. Ensuite, si nous parlons d'une vulnérabilité systémique, nous nous en remettons à la défense, mais la protection du Canada par le biais du renseignement étranger nous tient beaucoup à coeur. Nous voulons nous assurer d'avoir les renseignements dont nous avons besoin.

● (1655)

M. Glen Motz: Comme nous l'avons vu lors des élections aux États-Unis—la question a été soulevée au cours de la première heure —, nous sommes toujours exposés à la désinformation en provenance d'acteurs étrangers. Dans le cadre de nos élections qui auront lieu d'ici un an, comment pouvons-nous nous protéger de cet aspect tout en préservant notre liberté d'expression?

M. Scott Jones: Je pense qu'une partie de la solution consiste à en parler. Nous sommes désormais conscients de ce problème. C'est le fait que c'est maintenant dans la conscience. Nous pouvons maintenant en parler et, comme consommateurs d'information, nous pouvons commencer à devenir des connaisseurs, des consommateurs d'information qui ont un peu plus de jugement, et qui ne croient pas seulement ce qu'ils lisent dans les médias sociaux.

Je pense que le deuxième élément consiste à poser des questions ou à rechercher des sources multiples. J'accorde peut-être un peu trop de crédit à notre consommation des médias sociaux. Par ailleurs, le rapport que nous avons publié l'an dernier sur la menace qui pèse sur le processus démocratique du Canada en est un petit élément qui nous permet de lancer le dialogue.

Au bout du compte, il s'agit de notre littératie, de nos connaissances civiques, mais aussi, pouvons-nous commencer à en parler et à ne pas croire tout ce que nous lisons?

M. Glen Motz: J'ai deux questions, très rapidement.

Pour ce qui est de la première, vous devez répondre essentiellement par oui ou par non. Est-ce que le partage des données par les médias sociaux exige une réglementation? C'est un aspect de la question. L'autre élément est celui que vous avez mentionné dans votre exposé. Comment pouvons-nous procéder pour les petites entreprises qui ne pensent pas à la cybersécurité parce qu'elles ont un million d'autres choses à faire? Elles sont de petite taille, et comptent peut-être 100 employés. Quelle que soit leur taille. Comment les amener à penser différemment de ce qu'ils pensent maintenant?

Je sais. Ce sont deux questions différentes. J'essaie de les présenter toutes les deux, avec l'indulgence du président.

Le président: Le président ne sera pas très indulgent, car il ne vous reste que 30 secondes.

M. Scott Jones: En ce qui concerne la réglementation des médias sociaux, je ne suis probablement pas la bonne personne pour répondre à cette question. Je n'ai pas vraiment évalué cette question.

Pour ce qui est des petites et moyennes entreprises, il faut notamment relever la norme de la résilience générale. Je pense qu'il est déraisonnable de s'attendre à ce que les entreprises puissent lancer une initiative de cyberdéfense comme, par exemple, celle que nous dirigeons pour le gouvernement du Canada. C'est inabordable pour toutes les petites et moyennes entreprises.

Comment pouvons-nous améliorer notre effort? Comment pouvons-nous améliorer la cybersécurité générale de l'industrie, de façon à ce qu'elle puisse en profiter? Deuxièmement, comment établir des partenariats avec les grands fournisseurs de services, ceux qui fournissent ces services aux petites et moyennes entreprises? Troisièmement, l'industrie de l'assurance a une capacité remarquable de faire bouger les petites et moyennes entreprises, et je pense que cela s'ajoute au programme des petites et moyennes entreprises qui a été annoncé dans le cadre de la stratégie de cybersécurité.

Tout cela peut aider, mais au bout du compte, nous devons y accorder une certaine valeur.

Le président: Merci, monsieur Motz.

Monsieur Dubé, vous avez sept minutes.

M. Matthew Dubé (Beloeil—Chambly, NPD): Merci beaucoup, monsieur le président, et merci à vous deux d'être ici.

J'aimerais poser quelques questions au sujet de la transparence.

Premièrement, parce que le sujet qui préoccupe tout le monde, pour de bonnes et de mauvaises raisons, ce sont les élections, y a-t-il des protocoles en place pour la divulgation d'une vulnérabilité potentielle, d'une infiltration ou d'une tentative d'influence après l'émission du bref? Autrement dit, si nous sommes en plein milieu d'une campagne—j'ai entendu parler du dilemme James Comey—, comment vous assurez-vous que les Canadiens sont au courant qu'on tente de s'ingérer dans une élection tout en évitant de révéler cette nouvelle et en influençant ensuite l'élection de cette façon?

M. Scott Jones: Cela concerne la convention de transition, mais aussi la collaboration avec Élections Canada. Nous en parlons avec Élections Canada, parce qu'au bout du compte, le scénario cauchemardesque pour un fonctionnaire serait de faire quoi que ce soit qui nuirait à l'élection. Je ne saurais trop insister sur le fait que c'est un scénario cauchemardesque pour moi en ce moment.

Des voix: Oh, oh!

M. Scott Jones : Nous en parlons avec Élections Canada, pour nous assurer de respecter cela, et aussi pour le commissaire aux élections fédérales, pour nous assurer que nous respectons l'indépendance. Ce serait peut-être la meilleure solution. Nous discutons actuellement de la façon dont nous allons aborder cette question.

C'est un peu un monde nouveau. Normalement, dans la fonction publique, nous avons tendance à nous tenir en retrait. Nous nous concentrons sur le service public et nous faisons simplement les choses normales. La cybernétique a changé cela.

M. Matthew Dubé: Il n'y a pas de lignes directrices existantes sur la façon de procéder en cas d'événement de ce genre pendant une campagne.

M. Scott Jones: Nous examinons actuellement les scénarios envisageables.

M. Matthew Dubé: D'accord. Élections Canada a-t-il l'expertise nécessaire pour régler ce genre de problème ou compte-t-il uniquement sur vous?

M. Scott Jones: Nous avons commencé avant les dernières élections de 2015 à travailler en collaboration avec Élections Canada pour renforcer la cybersécurité et commencer à discuter de ces questions. Nous sommes en train de travailler là-dessus et de trouver aussi un moyen de collaborer avec les partis politiques au cas où nous découvririons un problème. Comment pouvons-nous communiquer l'information qui nous permet de déterminer si un parti politique en particulier est visé par des activités? Je pense que cela fait partie de l'élaboration de ce protocole.

● (1700)

M. Matthew Dubé: Il y a Services partagés et ensuite Sécurité publique, mais Élections Canada est absent de ce centre. N'a-t-on pas songé à confier un rôle quelconque à Élections Canada?

M. Scott Jones: Nous cherchons à assurer la liaison avec eux, mais nous respectons leur indépendance. Comme ils ne font pas partie de l'administration publique à proprement parler et qu'ils sont plutôt un agent du Parlement, nous cherchons à travailler en partenariat avec eux, à suivre un protocole strict et à le respecter.

M. Matthew Dubé: L'autre question que j'aimerais poser concerne le processus d'équité des vulnérabilités qui existe au sein de la NSA aux États-Unis. Toujours au sujet de la transparence, je m'interroge à ce sujet. De plus en plus, surtout compte tenu de l'existence du centre, je suppose que l'on fera davantage de travail pour cerner ces vulnérabilités.

Dans le projet de loi C-59, beaucoup de mesures prévoient la collaboration avec le secteur privé pour cerner les vulnérabilités et, dans certains cas, même les étudier dans une certaine mesure. Je ne veux pas reprendre le débat que nous avons longuement eu au Comité, mais y a-t-il un protocole précis qui existe ici, au même titre que celui qu'a élaboré la NSA, pour divulguer au public et aux parlementaires, et ainsi de suite, l'existence de vulnérabilités dans les logiciels et autres problèmes?

M. Scott Jones: Tout à fait, il existe un processus pour ces cas. Notre processus normal est de travailler avec l'entreprise pour essayer de procéder de façon responsable et de ne pas créer une vulnérabilité que quelqu'un pourrait exploiter. Chaque entreprise prend le temps de préparer des correctifs logiciels, et ainsi de suite. Nous voulons nous assurer qu'elle est en mesure de mettre ces correctifs en place avant toute divulgation publique afin que nous n'ayons pas de cybercriminels ou d'acteurs qui—

M. Matthew Dubé: Sans entrer dans les détails d'une vulnérabilité particulière, le processus et la façon dont il se déroule sont-ils rendus publics?

M. Scott Jones: Pas encore. C'est une chose dont nous avons parlé—comment pouvons-nous communiquer cela?

M. Matthew Dubé: D'accord. Je vous demanderais d'essayer de faire mieux que la dernière réponse que j'ai reçue, qui m'a renvoyé à Twitter. La dernière fois que nous avons reçu des représentants du CST, ils m'ont dit: « Nous procédons maintenant par gazouillis », alors j'espère simplement avoir quelque chose d'un peu plus robuste au même titre qu'à la NSA. Je n'arrive pas à croire que j'accorde du crédit à la NSA, mais elle mérite qu'on lui en donne dans ce dossier, alors si vous pouviez suivre cet exemple, ce serait grandement apprécié.

J'avais une autre question concernant les infrastructures privées, même si j'estime que c'est devenu un mot tabou. Il est intéressant de constater que, dans le cas de ces questions liées à des entreprises particulières, et pour certaines des préoccupations, qu'il s'agisse de Huawei ou d'autres, en ce qui concerne l'infrastructure privée, vous parlez évidemment de la liaison avec l'entreprise privée. L'on peut s'inspirer des réseaux électriques privés ou des cliniques privées en ce qui concerne l'information sur la santé ou quelque chose du genre.

Que se passe-t-il lorsqu'une infrastructure privée peut appartenir à des intérêts étrangers ou ne pas être clairement définie comme appartenant à des intérêts canadiens et s'il y a une sorte de zone grise? Comment fonctionnez-vous dans ce contexte particulier, surtout en ce qui concerne le spectre et ce genre de choses pour les télécommunications?

M. Scott Jones: Nous cherchons toujours à fournir des conseils et des directives pour aider à relever la norme de départ afin que ce soit plus sûr. Lorsqu'il est question d'infrastructure, peu importe la propriété, s'il s'agit d'une infrastructure canadienne, au Canada, nous la traiterions comme une infrastructure canadienne dans le cadre de notre travail avec elle. Si cette infrastructure était victime d'un incident, nous l'encouragerions certainement à se présenter au Centre canadien pour la cybersécurité afin que nous puissions essayer de l'aider. En même temps, la technologie qu'elle utilise, la façon dont elle la met en oeuvre et la nécessité d'équilibrer les facteurs—la cybersécurité, mais aussi l'abordabilité et d'autres facteurs, demeurent toujours des choix d'entreprise.

En fait, c'est une combinaison de plusieurs choses. Il s'agit d'offrir des conseils et des directives et d'aider à rendre l'infrastructure plus sûre. Nous essayons de publier de plus en plus de conseils et de guides pratiques. Je dirais que dans le passé, certains de nos outils étaient—

M. Matthew Dubé: Désolé de vous interrompre, mais mon temps est écoulé.

Lorsque des évaluations de la sécurité nationale sont établies dans les cas de prises de contrôle d'entreprises par des intérêts étrangers, je suppose qu'il y a une composante cybernétique plus importante à notre époque. Nous avons souvent parlé des ressources naturelles au cours des 10 à 15 dernières années. Est-ce une chose à laquelle vous participerez à l'avenir, lorsque ces évaluations seront faites par le {ministre de l'Innovation, des Sciences et du Développement économique, ISDE?

M. Scott Jones: Nous sommes désignés dans le cadre du processus prévu par la Loi sur Investissement Canada. Nous donnons des conseils au ministre de la Sécurité publique, qui travaille ensuite avec le {ministre de l'Innovation, des Sciences et du Développement économique.

Pour ce qui est des entreprises canadiennes, cependant, nous cherchons également des moyens d'accroître leur résilience afin qu'elles puissent se défendre contre ce genre de cyberactivités. Cela fait également partie de l'équation. C'est assurément une considération.

M. Matthew Dubé: Merci.

● (1705)

Le président: Merci, monsieur Dubé.

Madame Damoff, vous avez sept minutes.

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

Merci à vous deux d'être ici.

M. Motz et M. Dubé ont tous deux parlé de Huawei. Ma question est peut-être un peu plus générale. Il s'agit des risques que posent certaines des préoccupations qui ont été exprimées au sujet de cette entreprise, mais aussi au sujet de l'industrie des télécommunications en général et des risques auxquels nous sommes confrontés. Est-ce quelque chose que le Comité pourrait examiner dans le cadre d'une étude? Est-ce que cela en vaudrait la peine?

M. Scott Jones: L'élément clé pour nous, quand on parle de fournisseurs, c'est que presque tout est fabriqué partout dans le monde. L'endroit où le produit final est assemblé ne correspond pas nécessairement à l'endroit où le logiciel est conçu, et ainsi de suite. Nous travaillons dans un marché mondial. C'est l'une des choses sur lesquelles nous nous penchons vraiment, c'est-à-dire comment assurer la sécurité lorsque le produit d'origine, ou l'entreprise qui le fournit, ne fournit qu'une petite partie de ce qui est réellement intégré au produit?

Du côté des entreprises de télécommunications, c'est difficile pour nous, parce que nous travaillons en vertu... Elles fournissent beaucoup d'information pour que nous puissions travailler de façon très proactive sur ce qui s'en vient, de sorte qu'il s'agit de renseignements de nature concurrentielle pour eux. En même temps, je les ai vus faire des investissements substantiels dans la cybersécurité sans avoir besoin de publicité ou d'intervention gouvernementale, et ainsi de suite. Ils prennent la sécurité très au sérieux. Je suis vraiment fier de cette relation. Nous avons trouvé un bon modèle canadien de collaboration entre le gouvernement et l'industrie pour tenter de relever certains des défis en matière de cybersécurité, non pas à partir d'une menace très étroite à la sécurité nationale, mais de façon plus générale. Comment pouvons-nous nous assurer de bâtir un réseau de télécommunications très résilient d'un océan à l'autre? C'est un aspect sur lequel nous insistons beaucoup.

C'est une question complexe. Dans le cas de la cybersécurité, malheureusement, comme nous le disions, il est très difficile de la définir en 240 caractères. C'est l'un des plus grands défis dans le secteur des télécommunications. C'est très compliqué et très vaste.

Mme Pam Damoff: L'autre question que j'aimerais poser, qui a été soulevée à quelques reprises, concerne les élections et la désinformation. Vous avez dit qu'à votre avis, le public est devenu plus conscient. Je dirais que c'est vrai dans une certaine mesure, sauf qu'il est toujours possible de diffuser des renseignements erronés sur les médias sociaux, où on en trouve beaucoup. Je m'inquiète en particulier des faux comptes qui ont surgi au cours de l'été. Il semble s'agir d'un représentant du gouvernement, et ses messages sont partagés 5 000 fois, mais c'est en fait un faux compte.

Ce genre de choses est vraiment troublant, parce qu'il y a de la désinformation qui circule encore. Des gens sont venus à mon bureau, comme nous tous probablement, pour parler de ce qu'ils ont lu. Lorsque je leur dis que ce n'est tout simplement pas vrai et que je leur demande d'où viennent ces renseignements, ils disent en avoir entendu parler par un ami, qui l'a lu sur les médias sociaux.

Comment composez-vous avec cela lorsque ces renseignements viennent d'un autre pays, ou même à l'interne?

M. Scott Jones: Pour ce qui est de s'en occuper directement, c'est l'un des défis que nous devons relever dans une démocratie ouverte qui encourage la communication. Nous ne surveillons tout simplement pas ce genre de choses. Nous ne dirigeons pas nos activités vers les Canadiens, et sur Internet, il est difficile de distinguer les Canadiens de tous les autres.

L'essentiel, c'est que les plateformes de médias sociaux elles-mêmes essaient de régler ce problème. Par exemple, si je voyais quelqu'un essayer de se faire passer pour moi—je ne vois pas pourquoi, mais si jamais c'était le cas—, je profiterais certainement des outils de signalement qu'offrent ces plateformes. L'on a essayé de régler ce problème, et c'est donc un peu connu du public.

Mme Pam Damoff: Je vais vous interrompre un instant, cependant, parce que nous avons reçu des représentants de Twitter au Comité de la condition féminine, et c'est exactement ce dont nous parlions, et des outils de signalement. Les représentants de Twitter nous ont dit que Google avait, en Irlande seulement, le même nombre d'employés qu'eux ont dans le monde, et qu'ils n'arrivaient même pas à régler le problème.

Il y a un petit problème lorsque les médias sociaux—en particulier Twitter, parce que je pense que Facebook a probablement mieux réussi à régler certains de ses problèmes—n'ont tout simplement pas le personnel nécessaire. Ils peuvent signaler des problèmes, mais ils ne s'en occupent pas, alors c'est un problème. C'est une question de sécurité publique, en ce qui concerne les élections, si la société privée ne s'occupe pas de cette question.

M. Scott Jones: Le défi auquel nous faisons face, c'est que, pour nous, le problème est très explicite. Nous ne dirigeons pas nos activités vers les Canadiens.

Lorsque nous avons affaire à de faux comptes de médias sociaux ou à des comptes de parodie—et c'est une autre chose que nous avons vue cet été, par exemple—et qu'on cherche à savoir où se situe la ligne entre un faux compte et un compte de parodie, le problème, c'est que ces comptes ne font tout simplement pas partie de notre mandat. Nous essayons d'accroître la résilience cybernétique de base de ces systèmes, mais je pense que l'utilisation des médias sociaux et les contraintes que nous aimerions y imposer sont probablement des aspects qu'il vaudrait mieux laisser à des organisations comme le ministère du Patrimoine canadien, qui examinerait les médias numériques et l'interaction en ligne.

En ce qui concerne le renseignement de sécurité, nous chercherions certainement les auteurs de menaces étrangères pour voir s'ils en tirent profit, et nous prendrions des mesures. Nous examinons les activités étrangères qui cibleraient le Canada, mais l'examen des comptes à proprement parler, et ainsi de suite, surtout quand on commence à entrer dans un contexte national, ne relève tout simplement pas du mandat du CST.

● (1710)

Mme Pam Damoff: Comment savez-vous qu'un pays étranger ne s'ingère pas dans les médias sociaux?

M. Scott Jones: C'est un défi pour le gouvernement. Nous nous tournerions vers nos organismes d'application de la loi, qu'il s'agisse de la GRC ou du Service canadien du renseignement de sécurité, où ils ont des pouvoirs nationaux, mais aussi, peut-être, vers la façon de composer avec ce genre de problème de façon plus générale. De plus, malheureusement, avec une seule personne, nous avons ce type de caisse de résonance dans laquelle les gens créent l'apparence d'information réelle.

Nous essayons de sensibiliser les gens à ce qui se passe et d'attirer leur attention sur certains éléments, mais au bout du compte, il ne nous appartient pas de commencer à nous occuper des faux comptes.

Le président: Monsieur Paul-Hus, vous avez cinq minutes.

C'est à vous.

[*Français*]

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

Je remercie les témoins d'être ici.

Récemment, le Groupe des cinq a entamé des procédures contre la compagnie Huawei. Je voudrais savoir pourquoi le Canada n'a pas suivi.

[*Traduction*]

M. Scott Jones: Lorsque nous examinons cette question du point de vue canadien, il m'est difficile de commenter certaines décisions internes. Nous ne voyons pas toujours les débats internes du gouvernement de nos partenaires du Groupe des cinq, mais de notre point de vue, nous avons vraiment essayé de nous concentrer sur les grands défis en matière de cybersécurité dans l'espace des télécommunications. Nous pensons avoir un programme vraiment efficace pour ce qui est de la façon dont nous gérons les risques liés à la cybersécurité auxquels nous sommes confrontés comme pays, comme les vulnérabilités propres à chaque produit de télécommunication et la façon dont nous commençons à les atténuer.

Voulez-vous ajouter quelque chose?

M. Rajiv Gupta (directeur, Normes, architecture et atténuation des risques, Centre de la sécurité des télécommunications): Oui.

Comme Scott l'a dit, au Canada, nous adoptons une approche fondée sur le risque, alors nous examinons le même ensemble de risques. Nous les évaluons au Canada. Nous évaluons notre relation avec les exploitants de sociétés de télécommunications et le type d'influence que nous y exerçons, et nous travaillons ensemble pour appliquer une approche fondée sur le risque.

Nous avons parlé un peu du programme que nous avons appliqué au cours des dernières années, et nous croyons toujours qu'il est efficace pour atténuer les risques. C'est en évaluant ce programme que nous déterminons si nous pensons que c'est une bonne façon de procéder en prévision de l'avenir.

[*Français*]

M. Pierre Paul-Hus: Ne pensez-vous pas que le fait de permettre à cette compagnie de faire des affaires au Canada puisse diminuer la confiance au sein du Groupe des cinq? Si les quatre autres pays membres sont unanimes dans leur choix, mais que nous décidons de garder cette compagnie, cela ne pourrait-il pas créer une brèche dans la confiance de nos partenaires?

Comme on le sait, il n'existe aucun document écrit qui définisse ce qu'est ce groupe. Il repose sur une entente fondée sur la confiance mutuelle. Ce pourrait-il que nous perdions la confiance de nos partenaires?

[*Traduction*]

M. Scott Jones: L'une des choses que nous essayons de partager avec nos partenaires du Groupe des cinq, c'est de nous assurer qu'ils connaissent notre programme et notre approche, qui sont très complets pour ce qui est de gérer tous les risques dans le spectre des télécommunications. De plus, nous avons établi une relation productive avec tous les fournisseurs de services de télécommunications du Canada pour ce qui est de l'échange d'information, du partage des risques et de la recherche de solutions concertées aux problèmes de cybersécurité. Ce ne sont pas tous les pays qui profitent de cela, et c'est une très bonne force canadienne. Je suis très fier du travail accompli par l'équipe. Nous examinons les risques pour tous les fournisseurs, mais aussi pour tous les produits, pour ce qui est de la façon dont nous superposons les couches de cybersécurité et nous nous assurons que le problème est considéré comme systémique.

Au bout du compte, nous avons des réseaux de télécommunications très sécuritaires en raison de ces relations, mais c'est un aspect compliqué de la question.

À long terme, nous devons chercher des moyens d'accroître systématiquement notre cyberrésilience, peu importe d'où vient notre produit. C'est une façon durable de commencer à vraiment examiner la question.

● (1715)

[*Français*]

M. Pierre Paul-Hus: Comme l'ont mentionné les analystes, le Canada retire de nombreux bénéfices de la présence des États-Unis, qui lui fournissent beaucoup d'information.

En proportion de son poids économique, le Canada apporte-t-il une contribution juste? Les Américains ont-ils l'impression de trop en donner et de ne pas assez en recevoir?

[*Traduction*]

M. Scott Jones: Je ne peux pas vraiment parler au nom des Américains à ce sujet, mais de notre point de vue, nos relations avec nos fournisseurs de services de télécommunications sont très avancées. D'après ce que j'ai vu, elle est assurément différente de celle qui existe dans la plupart des autres pays.

Nous avons un programme très étoffé qui vise à accroître la résilience, surtout dans le contexte de la prochaine génération de réseaux de télécommunications, pour nous assurer que nous sommes en mesure de faire évoluer ce programme et de trouver des façons d'innover en cybersécurité, mais aussi d'accroître la cybersécurité de base de chaque produit acheté, peu importe d'où il vient dans le monde.

Je pense que c'est l'un de nos plus grands défis. Il ne s'agit pas d'un seul élément; il s'agit de la façon de rendre tout le système résilient. L'environnement des communications est très complexe et nous devons l'aborder dans son ensemble.

[*Français*]

M. Pierre Paul-Hus: J'ai une dernière question. Est-ce que j'ai le temps de la poser?

[*Traduction*]

Le président: Il vous reste 20 secondes.

Ça va, M. Motz va prendre votre relève.

M. Glen Motz: Bien sûr.

Le président: Monsieur Spengemann, vous avez cinq minutes.

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

Messieurs, merci d'être venus.

Je veux revenir au paradigme selon lequel une bonne cybersécurité se traduit par une bonne sécurité économique et une bonne compétitivité économique.

Dans nos circonscriptions, nous recevons beaucoup de questions de la part des entreprises, même des entreprises en démarrage qui s'intéressent aux mégadonnées. Ils nous demandent ce que fait le Canada dans ce domaine.

Vous semblez dire que vous êtes relativement satisfait du modèle que nous appliquons actuellement. Parliez-vous en particulier des télécommunications, ou de l'ensemble des secteurs qui utilisent les mégadonnées?

M. Scott Jones : Nous avons commencé par le secteur des télécommunications. Nous avons tout de suite abordé cette question. Nous pensons avoir un modèle que nous pourrons développer pour l'appliquer à d'autres secteurs, en particulier dans les infrastructures essentielles. De façon plus générale, cependant, nous devons commencer à nous pencher sur des questions comme la politique numérique, et des consultations sont en cours à ce sujet. Je pense qu'il est important de commencer à... la cybersécurité en est un élément, et nous nous efforçons de la renforcer, mais je pense aussi que nous devons diffuser plus d'information sur des aspects pratiques afin que les petites et moyennes entreprises puissent innover afin de protéger leur propriété intellectuelle contre les cyberintrusions. Nous devons essayer de développer cette relation. Il faut renforcer la résilience. Le fonctionnement du cybercentre reposera sur un modèle de « sécurité par la collaboration ».

Nous manquons d'expertise dans certains domaines. Nous sommes experts des menaces et de la cryptographie et nous savons très bien atténuer les risques. Par exemple, dans le cas de l'infrastructure essentielle du secteur de l'énergie, nous devons collaborer avec les experts de ce domaine. Par exemple pour régler des problèmes de mégadonnées, nous nous occuperions des mégadonnées en demandant quels sont les plus grands problèmes afin de sécuriser les données.

M. Sven Spengemann : Du point de vue économique, des coûts d'exploitation ou même des dépenses en capital, y a-t-il encore moyen de mettre en commun les ressources des entreprises canadiennes en partenariat avec les directions générales du gouvernement du Canada afin de créer une base commune de cybersécurité dont nous pourrions tous profiter?

M. Scott Jones : Tout à fait. C'est justement l'un de nos objectifs. Par exemple, le Canadian Cyber Threat Exchange est un organisme sans but lucratif créé par des entreprises canadiennes. Nous collaborons et, en fait, nous allons bientôt signer une entente afin de transmettre l'information à toutes les entreprises canadiennes. Nous pourrons ainsi mettre des ressources en commun dans un esprit non concurrentiel. Nous ne devrions pas nous faire concurrence pour accroître la sécurité, mais comment y parvenir?

Nous cherchons également des moyens d'encourager l'innovation. Le cybercentre permettra aux entreprises de collaborer à des projets qui encourageront l'innovation en matière de sécurité.

Nous nous efforçons de créer des occasions pour rassembler ces éléments. Il nous arrivera de ne pas avoir le temps d'aborder certains problèmes qui ne nous concerneront peut-être même pas, mais nous nous ferons un plaisir de jumeler des entreprises. Nous pourrons présenter aux entreprises qui ont des problèmes celles qui y ont déjà trouvé de bonnes solutions.

M. Sven Spengemann : Je comprends. Merci, c'est très utile.

Avez-vous constaté d'autres pays qui ont un peu d'avance sur nous et que le Comité pourrait examiner plus en détail pour éclairer son étude?

M. Scott Jones : Je tiens à féliciter mes collègues du Royaume-Uni d'avoir créé le National Cyber Security Centre...

M. Sven Spengemann : C'est vrai.

M. Scott Jones : ...et tout ce qu'ils ont fait pour innover. Nous travaillons en étroite collaboration avec eux. Ils seraient donc les premiers.

Il y a aussi mes collègues en Australie. L'Australian Cyber Security Centre vient de changer de modèle. Le Royaume-Uni est un peu plus avancé, mais ce sont là les deux exemples les plus éloquents.

Il y a aussi quelques bons exemples en Europe.

● (1720)

M. Sven Spengemann : J'ai une dernière question pour la minute et demie qu'il me reste.

Pour ce qui est de la capacité des candidats du bassin de talents de se déplacer librement entre le secteur privé et le secteur public, vous semblez dire qu'il y a des catégories ou des mandats qui ne sont pas bloqués par des cotes de sécurité, donc que les gens peuvent se déplacer assez librement. Dans quelle mesure est-ce le cas à l'heure actuelle, et que pouvons-nous faire pour que le bassin de talents profite vraiment aux secteurs public et privé?

M. Scott Jones : C'est l'un des objectifs du cybercentre : l'ouverture et la transparence. En fait, nous visons à ce que les gens puissent venir travailler dans ce centre. À l'heure actuelle, quand les gens visitent le CST, nous leur retirons tous leurs appareils électroniques, parce qu'ils entrent dans un immeuble très secret. Ce ne sera pas le cas du cybercentre. Les gens pourront venir dans nos installations physiques pour y collaborer et y apporter carrément leurs appareils pour que nous puissions voir comment ils fonctionnent et développer des choses ensemble.

À mon avis, il faut que nous soyons plus souples. La collaboration nous ouvre des occasions d'apprendre d'autrui.

Le secteur public pose certaines entraves — notre mission, un peu d'altruisme, etc. Cependant, le secteur privé en pose aussi dans les domaines de l'innovation, des profits et des choses de ce genre. Tout dépend des gens.

M. Sven Spengemann : On pourrait même détacher des employés les uns chez les autres.

M. Scott Jones : J'aimerais beaucoup cela. Je pense que ce serait très créatif.

M. Sven Spengemann: Merci, monsieur le président.

Le président : Chers collègues, il nous faudrait dix minutes pour les questions, mais nous n'en avons que sept.

Je trouve cette conversation fascinante, et nous avons commencé un peu en retard, alors je pense que nous pourrions dépasser 17 h 30, si vous êtes tous d'accord. Les analystes ont aussi deux ou trois questions à poser, et j'aimerais les aborder à la fin. Est-ce que cela vous irait?

C'est très bien. Je dois poser les questions des analystes, alors il n'y a pas de panique.

Monsieur Eglinski, vous avez cinq minutes.

M. Jim Eglinski (Yellowhead, PCC) : J'ai deux questions qui sont en quelque sorte reliées.

En vertu du projet de loi C-59, vous avez le pouvoir de diriger le cybercentre, et vous parlez des autres organismes gouvernementaux, soit Sécurité publique, Services partagés, la GRC, le Service canadien du renseignement de sécurité et les forces armées.

Je suis un ancien policier et j'ai enquêté sur des crimes graves dans de très grands centres. Je sais qu'il y a toujours des conflits, causés peut-être par l'entêtement d'un ministère face à un autre.

Un certain temps s'est écoulé depuis la déposition du projet de loi C-59, et nous en avons discuté à la Chambre et ailleurs. Vos organismes se réunissent-ils déjà pour collaborer? Pensez-vous que la transition sera relativement facile et les efforts conjoints, ou prévoyez-vous des obstacles et des pressions dans les deux sens, peut-être parce qu'on vous en a confié la direction?

M. Scott Jones : Quand il sera en place, dans une dizaine de jours, le cybercentre sera un centre relativement nouveau. Cependant, nous entretenons des relations depuis longtemps pour éliminer les conflits. Par exemple, la cybercriminalité est le fléau d'Internet. Nous voudrions vraiment y appliquer la loi. Je voudrais vraiment voir des poursuites couronnées de succès afin de commencer à dissuader les cybercriminels. Pour ce qui est de notre collaboration avec l'unité de coordination de la lutte contre la cybercriminalité que la GRC va mettre sur pied, par exemple, nous espérons nous installer dans un même immeuble et partager les locaux.

Depuis très longtemps, un de nos organismes collabore avec la Gendarmerie royale du Canada et avec le Service canadien du renseignement de sécurité afin d'éliminer les conflits opérationnels et de choisir les meilleurs dirigeants possible. Par exemple, dans le cas d'une enquête sur la sécurité nationale, je veux que le SCRS agisse sur le terrain, mais nous appuierons ses activités d'atténuation. Nous savons contrer les menaces. Nous savons comment travailler avec l'entreprise et nous voulons que les poursuites soient couronnées de succès. Nous tenons à ce que les gens dénoncent la cybercriminalité.

Nous corrigeons le problème. D'expérience, je sais qu'il y aura des ratés et aussi probablement des manoeuvres politiques, mais nous mettons cette stratégie à l'essai.

M. Jim Eglinski : Vous m'avez amené à ma deuxième question.

Au Canada, un certain nombre de services de police accrédités ont des services de cybersécurité et de renseignement. J'imagine que comme vous, ils collaborent très étroitement avec la GRC. Envisagez-vous de créer un programme pour collaborer avec les autres corps policiers — les services de police municipaux de Vancouver, d'Edmonton et de Calgary, par exemple — qui ont déjà établi ces services?

Pensez-vous que, d'une manière ou d'une autre, votre organisme fédéral pourrait aider financièrement ces services de police? Bon nombre d'entre eux sont municipaux, mais en fait, ils protègent le pays. Voyez-vous un rôle qui vous permettrait peut-être d'aider ces autres services partout au Canada en leur procurant des fonds, de l'aide ou de la formation?

● (1725)

M. Scott Jones : Il est certain que nous envisagerions de collaborer avec la GRC afin de mobiliser tous les organismes d'application de la loi et que nous suivrons son exemple pour le faire.

Quant aux contributions financières, nous ne sommes pas vraiment habilités à faire ce genre de choses, mais nous offrons de la formation. Nous gérons actuellement le centre d'apprentissage en sécurité des TI, où nous offrons de la formation. Par exemple, je sais que quelques services de police provinciaux ont suivi des programmes de formation, etc., sur la sécurité des TI. Je pense que nous chercherions vraiment à tirer parti de notre relation avec la GRC et avec le Collège national de police et à faire notre possible pour soutenir la formation.

Nous misons certainement sur une relation de ce genre avec les forces policières. Il faut collaborer. Il faut aussi que nous sachions quand laisser les forces policières faire leur important travail sans altérer la preuve, n'est-ce pas? En fin de compte, j'encourage beaucoup cela.

M. Jim Eglinski : Je ne sais pas lequel d'entre vous a mentionné cela plus tôt, mais comment former les Canadiens afin qu'ils possèdent les connaissances et les compétences requises pour travailler dans votre ministère et dans d'autres ministères? Je voudrais savoir ce que vous en pensez. Comment nous y prendre? Il ne faut pas tarder.

M. Scott Jones : Pour ce qui est de la formation et de l'aide...?

M. Jim Eglinski : Oui.

M. Scott Jones : À mon avis, il y a plusieurs facteurs. C'est dans la cyberculture. Il s'agit de démystifier la TI. Les gens pensent que c'est domaine d'experts, et pourtant ils l'utilisent quotidiennement. La plupart des gens ont peur d'y toucher en cas de panne, etc. Elle ne devrait pas paraître si difficile. Notre secteur devrait corriger cette perception.

Deuxièmement, à mon avis, il faut que nous attirerions les gens vers les programmes. Personne ne s'y inscrit. Nous sommes allés visiter l'université qui, en 1999, recrutait le plus de candidats de toutes pour le CST. Le nombre des étudiants en informatique est tombé au quart de ce qu'il était cette année-là. Nous aurons bien de la peine à recruter des gens en cybernétique, au gouvernement comme dans le secteur privé. Voilà selon moi sur quoi nous devrions vraiment nous concentrer.

Le président : Merci, monsieur Eglinski.

Madame Dabrusin, vous avez cinq minutes.

Mme Julie Dabrusin (Toronto—Danforth, Lib.) : Une grande partie de la conversation que nous avons eue aujourd'hui portait sur la collaboration avec le secteur privé. Vous avez parlé à quelques reprises de la faible résilience et de la nécessité de la renforcer. Dans votre site Web, j'ai remarqué qu'il y a un peu moins d'un an, vous avez lancé une plateforme qui s'appelle Assemblyline. D'après ce que je comprends, les utilisateurs privés peuvent aussi s'en servir. Pourriez-vous la décrire brièvement pour que je ne m'embrouille pas en le faisant moi-même?

M. Scott Jones : Bien sûr. Assemblyline est le système que nous utilisons pour analyser des logiciels malveillants. Disons que vous obtenez un fichier malveillant. Comment allons-nous le décomposer et essentiellement effectuer toute la cyberanalyse? Nous l'automatisons. C'est ce que nous faisons pour le gouvernement. Nous ne confions pas cela à des personnes, nous automatisons et nous profitons de certains éléments créatifs. Nous avons offert le code gratuitement au monde entier.

Mme Julie Dabrusin : À la lumière de cette expérience, quelles sont les leçons apprises sur ce qui a fonctionné ou pas en le lançant ainsi gratuitement? Vous l'avez fait il y a environ un an.

M. Scott Jones : Son grand succès est le fait qu'il s'adressait aux professionnels de la cybersécurité, aux gens qui font ce travail pour gagner leur vie, et nous avons constaté qu'il a été adopté partout dans le monde. De plus, ces utilisateurs le développent continuellement.

Il faut beaucoup de travail pour maintenir un projet en exploitation libre. En le lançant ainsi, nous devons continuellement investir pour le gérer, etc.

Je pense que dans l'ensemble, cela nous a réussi, non seulement en plaisant au public qui recevait ainsi un logiciel gratuit, mais en cherchant à offrir un nouvel outil à la communauté cybernétique.

Je désire qu'un plus grand nombre de gens y contribue et l'améliore. Je voudrais trouver un moyen de l'utiliser partout au Canada... Les gens commencent à l'adopter. Comment partager maintenant certaines des composantes analytiques qui s'y rattachent?

Mme Julie Dabrusin : Les gens qui l'utilisent craignent-ils de vous transmettre leurs renseignements personnels? On entend souvent ce genre de questions, et cela semble revenir quand nous parlons de données et de protection des données. Le problème touche aussi la confidentialité de ces données.

M. Scott Jones : Nous avons offert l'outil. Nous n'avons pas offert notre utilisation de cet outil. Les gens peuvent télécharger le logiciel, l'installer dans leur système et l'exécuter dans leur propre environnement en toute sécurité. Il n'y a pas de lien, alors ils n'utilisent pas notre utilisation de l'outil, et nous ne recueillons pas... Ce n'est pas une plateforme de collecte de données ou quoi que ce soit du genre.

Mme Julie Dabrusin : Au début, en parlant de renforcer la résilience, vous avez dit qu'il y a des choses simples que nous pourrions faire. Vous avez mentionné brièvement les correctifs, mais quelles sont ces choses simples que nous pourrions faire pour renforcer la résilience?

● (1730)

M. Scott Jones : L'application de correctifs est la toute première, réellement.

La deuxième, suivant l'infrastructure que vous utilisez, est d'éviter à tout prix d'ouvrir une session en tant qu'administrateur, de profiter de super privilèges, etc. C'est tout simple. Cela ne fait que ralentir votre utilisation.

Il y a aussi la sauvegarde de vos données. Sauvegardez toutes vos données cruciales, parce que si un rançongiciel rentre dans votre ordinateur, il vous suffira alors de faire une restauration et de réinsérer vos données, et d'autres petites choses. Je simplifie un peu les choses par rapport à la pratique, mais ce sont des mesures fondamentales sur le plan de la résilience.

Nous avons dressé la liste de nos 10 priorités. Elles s'appliquent surtout aux grands organismes, mais je peux les traduire en mesures personnelles. Il s'agit aussi de déterminer ce que vous trouvez important afin de le protéger, par exemple en faisant des sauvegardes. Pour moi, les photos de famille et ce genre de choses me tiennent à coeur. Honnêtement, je ne me soucie pas d'un courriel que je ne lirai plus jamais et que j'ai reçu dans ma boîte personnelle.

Mme Julie Dabrusin : C'est assez simple. Ce que vous venez de suggérer est vraiment simple. Par exemple, vous parlez de faible résilience et de la nécessité de renforcer la résilience, et ce que vous venez de dire est assez fondamental. Alors, qu'est-ce qui vous qui empêche de divulguer ces renseignements pour que les gens soient moins vulnérables à différents types de cybercrimes ou à ceux dont vous avez parlé, comme les rançongiciels et autres?

M. Scott Jones : Dans certains cas, ce n'est pas commode. La mise à jour est un peu embêtante à faire. Il n'est pas pratique de faire fonctionner les correctifs, etc. Dans d'autres cas, les gens ne voient tout simplement pas le besoin. Ils se disent que tout va bien chez eux, ou encore qu'il n'ont pas les compétences pour le faire. Cette attitude a malheureusement été créée par notre industrie.

Dans certains cas, c'est le produit lui-même. Il ne se met pas à jour assez souvent. Lorsqu'on achète, disons, un téléphone intelligent, on rentre dans un écosystème, alors si c'est le fournisseur qui le met à jour, l'appareil peut être vraiment bon marché avec un mauvais soutien. Tous ces facteurs entrent en ligne de compte. Certains systèmes exigent beaucoup d'efforts manuels pour la mise à jour alors que d'autres sont plus conviviaux : une petite bulle rouge apparaît, vous appuyez sur *Installer*, et tout est prêt. Tous ces facteurs sont important. Nous compliquons souvent beaucoup les choses dans notre industrie.

Mme Julie Dabrusin : Merci.

Le président : Merci.

Monsieur Dubé, vous avez trois minutes, et je vous suivrai.

M. Matthew Dubé : Merci, monsieur le président. Je vous remercie de votre indulgence.

J'ai une question que je regrette vraiment de ne pas vous avoir posée tout à l'heure, au sujet du communiqué que l'alliance des *Five Eyes* a récemment diffusé. Il traite du chiffrement par des moyens détournés et de l'accès légal. Ce communiqué inquiète les défenseurs de la vie privée. Est-ce que votre organisme coopère avec le secteur privé au sujet de l'un ou l'autre de ces problèmes? J'en reviens aux questions de M. Eglinski sur la capture de criminels et autres. S'efforce-t-on à l'heure actuelle de trouver moyen d'entraver le chiffrement effectué par une « porte dérobée » ou de ranimer le débat sur l'accès légal que nous avons tenu dans le passé?

M. Scott Jones : Nous avons en fait un programme de validation des modules cryptographiques, que nous utilisons pour renforcer le chiffrement et être sûrs qu'il est bien fait. Nous collaborons avec le secteur commercial pour que non seulement les produits que nous utilisons au gouvernement, mais aussi les produits qui sont à la disposition de tous soient sûrs et adéquatement installés.

L'un des débats porte sur la façon dont les forces de l'ordre font leur travail dans le monde moderne des communications, maintenant que les ordinateurs sont assez puissants pour effectuer le chiffrement. Avant, c'était difficile. C'était lent. De quels outils les forces de l'ordre ont-elles besoin? Je pense que c'est une question de politique que nous préférerons vous laisser le soin de régler.

M. Matthew Dubé : J'en suis sûr.

Je n'aime pas vous demander de répondre au commentaire de quelqu'un d'autre, mais le porte-parole du ministre Goodale parle de données déchiffrées, d'accès à des données déchiffrées. Comme vous en êtes spécialiste, que signifie « accès aux données déchiffrées »?

M. Scott Jones : Je pense que si l'on considère cela du point de vue des fournisseur, certains d'entre eux sont en mesure d'obtenir ces données, alors comment peut-on fournir cet accès, en vertu de quels pouvoirs légaux, etc.? On se le demande, parce que les données ne sont pas chiffrées, par exemple, dans le serveur d'un fournisseur. Voilà ce qui cause le problème et la façon d'accéder aux données. C'est un problème complexe, surtout si le chiffrement vise une communication entre vous et moi et non un point central où il est stocké. Cela dépend vraiment des circonstances.

M. Matthew Dubé : Je crois comprendre que les fournisseurs de services de télécommunications, comme nous l'avons vu même dans le cas de l'iPhone d'Apple à San Bernardino, hésitent à donner un accès, quel qu'il soit. Que faire, alors? Si les ministres de la Sécurité publique de l'alliance *Five Eyes* affirment qu'ils ont besoin d'un meilleur accès et que ces fournisseurs hésitent à l'accorder, y aurait-il d'autres façons de les convaincre à le faire?

● (1735)

M. Scott Jones : Je ne sais pas ce qu'on pourrait faire. À mon avis, les solutions dépendent des technologies que l'on met sur pied. Parfois le fournisseur peut fournir l'information, ou il peut la concevoir. Dans bien des cas, les fournisseurs la conçoivent de façon à ce qu'on ne voie pas les données qui traversent le réseau et ils choisissent des conceptions particulières. La solution dépend du problème qu'on cherche à résoudre. Dans certains cas, ce sera technologiquement très complexe sur le plan technologique, mais très facile pour ce qui est de l'accès légal.

M. Matthew Dubé : Merci.

Le président : Merci, monsieur Dubé.

J'ai deux questions. D'abord, ne créez-vous pas effectivement une dépendance entre le secteur privé et le secteur public par l'entremise du CST ou de ce cybercentre? Au fil du temps, et peut-être même très bientôt, la dépendance sera permanente. Ce sera la nouvelle façon de faire des affaires et d'analyser la sécurité.

M. Scott Jones : Je pense que c'est déjà le cas, en effet. Nous comptons sur l'infrastructure privée qui gère notre infrastructure essentielle, qui est construite dans l'espace commercial. L'époque de l'équipement produit par le gouvernement est révolue. Nous ne réussissons pas à suivre le rythme rapide des innovations que le secteur privé produit. C'est l'un des plus grands défis actuels du secteur de la cybersécurité. L'innovation dépasse la sécurité. Comment établir des relations collaboratives? Ce serait la seule façon de régler ce problème.

Le président : Vous nagez en fait dans l'interdépendance. Elle va durer à perpétuité.

M. Scott Jones : Je ne vois pas comment nous pourrions régler ce problème sans collaborer avec le secteur privé.

Le président : Nous n'avons pas du tout parlé du rôle du milieu universitaire. Cette question est réapparue avec les gens de la société Huawei. Ils travaillent très activement en 5G et probablement avec d'autres technologies que nous ne connaissons même pas. Vous avez dit que vous effectuez une analyse du risque pour déterminer où vous devez intervenir et où vous en abstenir. Honnêtement, j'ai l'impression qu'une fois sortis de l'écurie, vous essayez de déterminer si votre cheval est un bon coureur.

La société Huawei participe à la création du réseau 5G, qui sera la plateforme pour tout. Cela fait-il partie de votre mandat? Sinon, devrait-il en faire partie?

M. Scott Jones : Dans le cas précis de la 5G, les réseaux de télécommunications de cinquième génération, la meilleure solution de sécurité pour tout ce qui y est lié est d'établir un environnement où plusieurs fournisseurs peuvent installer des protocoles de sécurité ou des dispositifs de sécurité à différents niveaux. On appuie cela par une approche de multiples fournisseurs. Les organismes internationaux de normalisation établissent certains des éléments émergents de la 5G. Bien sûr, la 5G n'existe pas encore. Il y a des prototypes et des choses de ce genre. Par où commencer pour intégrer ces éléments dans des éléments de cybersécurité?

Le plus important, à mon avis, est d'éviter à tout prix de n'avoir qu'un fournisseur, car nous serions vulnérables à tous les niveaux, et toutes les entreprises de télécommunications le seraient aussi. Il faut intégrer divers fournisseurs. Il faut divers fournisseurs à différents niveaux. On crée ainsi une sécurité énorme, parce qu'il devient difficile de traverser toutes les couches de cette pile de télécommunications. C'est l'un des éléments clés de la 5G.

Avez-vous quelque chose à ajouter, Rajiv?

M. Rajiv Gupta : Vous avez à peu près tout dit.

Nous cherchons des réseaux hétérogènes. Il est toujours très important, du point de vue de la continuité des activités, de mettre en place les contrôles et de comprendre les technologies à venir. Nous collaborons toujours avec tous les fournisseurs.

Vous avez parlé d'un cheval qui n'a pas encore franchi la barrière. Nous essayons de prévoir ce que la 5G nous réserve et de mettre en place des mesures d'atténuation dès maintenant, avant que les entreprises de télécommunications ne commencent à déployer leurs réseaux. Il est très important pour nous de comprendre ces technologies et de fournir des conseils et des directives dès le début afin d'atténuer les risques aussitôt que possible dans le processus, avant le déploiement des réseaux.

Le président : Au nom du Comité, je vous remercie tous les deux.

C'est incroyablement complexe. Vous nous avez certainement donné matière à réflexion.

Encore une fois, merci d'être venus témoigner devant le Comité et merci de votre réflexion.

Sur ce, la séance est levée.