CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

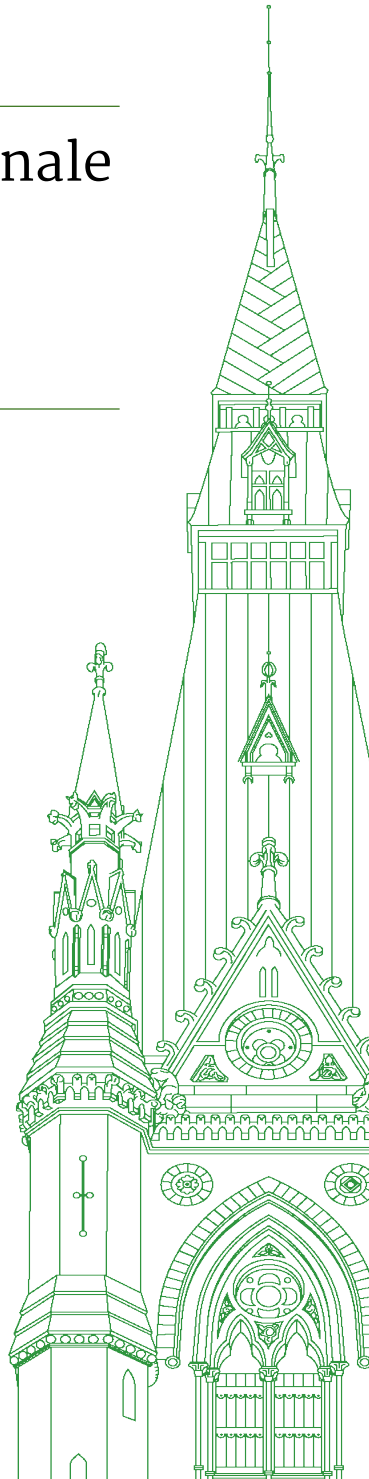
44e LÉGISLATURE, 1re SESSION

Comité permanent de la défense nationale

TÉMOIGNAGES

NUMÉRO 053

Le vendredi 10 mars 2023



Président : L'honorable John McKay

Comité permanent de la défense nationale

Le vendredi 10 mars 2023

● (0845)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Chers collègues, la séance est ouverte. Il est 8 h 45. Nous avons le quorum. Nos témoins sont prêts et nous avons effectué tous les tests de son.

Chers collègues, au cours de la première heure, nous suivrons l'horaire normal, puis je compte prendre quelques minutes à la fin de la deuxième heure pour adopter le budget des déplacements. J'espère que vous utiliserez ces deux heures pour parvenir à un accord sur les déplacements de ce comité. Je vis peut-être dans un monde où l'espoir est faible, mais bon...

Sur ce, je vais donner la parole à Christyn Cianfarani, qui aura cinq minutes pour formuler ses observations. Ensuite, M. Callan, qui semble être en ligne et qui a effectué les tests de son, se joindra à nous par vidéoconférence.

Bon retour au Comité. Nous sommes impatients d'entendre ce que vous avez à dire, madame Cianfarani.

Mme Christyn Cianfarani (présidente-directrice générale, Association des industries canadiennes de défense et de sécurité): Bonjour. Merci de m'avoir invitée à comparaître devant le Comité.

Aujourd'hui, je vous donnerai le point de vue de l'industrie canadienne de la défense et de la sécurité, et du sous-ensemble des entreprises qui forment l'industrie canadienne de la cybersécurité.

L'industrie canadienne de la cybersécurité est de classe mondiale. Selon des études effectuées par ISDE et Statistique Canada, entre 2018 et 2020, ce secteur a connu une croissance de plus de 30 % pour ce qui est de l'emploi, de la recherche et du développement et des revenus. Il s'agit d'un secteur mondial qui croît rapidement et qui devrait dépasser rapidement les TI traditionnelles pour ce qui est des dépenses.

Toutefois, seuls 8 % des revenus du secteur de la cybersécurité sont dérivés des contrats du gouvernement. Les ventes du secteur sont trois fois plus importantes auprès de nos alliés du Groupe des cinq qu'auprès du gouvernement du Canada. Ces chiffres reflètent une difficulté centrale à laquelle notre pays est confronté en matière de cyberdéfense: nos alliés voient plus de valeur dans le secteur de la cybersécurité que le Canada. Quelque chose cloche dans cette situation.

D'un côté, le Canada a besoin de faire plus d'acquisitions auprès de sa propre base industrielle, en utilisant l'approvisionnement comme levier politique pour stimuler l'innovation et pour faire croître les entreprises canadiennes. D'un autre côté, le Canada a besoin de faire des acquisitions à la vitesse de la cybernétique. Un processus d'acquisition lent est le moyen parfait pour acheter des cybertechnologies désuètes, voire obsolètes. Les cycles d'innovation dans ce domaine se mesurent en mois et même en semaines.

La résolution de ces problèmes se résume en un mot: collaboration. Le Canada a besoin d'un degré plus élevé de coopération, de partage de connaissances et de développement en collaboration entre le gouvernement et le secteur privé.

Nous avons pris des mesures concrètes en ce sens, mais nous ne sommes absolument pas rendus là où nous devrions l'être. Des agences comme le Communications Security Establishment ont les capacités voulues, mais la recherche de l'Association des industries canadiennes de défense et de sécurité a montré que notre gouvernement est loin derrière nos alliés lorsqu'il est question de collaboration avec le secteur d'une manière institutionnalisée. En Ukraine, nos alliés collaborent en temps réel avec l'industrie.

Le gouvernement du Canada doit établir un forum permanent pour le dialogue et la discussion sur les questions cybernétiques avec tous les principaux intervenants: l'industrie, le ministère de la Défense nationale et les Forces armées canadiennes, le Centre de la sécurité des télécommunications du Canada, Affaires mondiales Canada, et Sécurité publique Canada.

Le Canada doit également créer des systèmes améliorés de partage des menaces qui conjuguent les sources de données ouvertes sur les effractions, les indicateurs et les réponses possibles à celles du gouvernement et de l'industrie. Il s'agira de rationaliser ce qui n'est pas classifié et ce qui reste classifié et qui a accès à quoi. Encore une fois, nos alliés sont à l'avant-garde de ce type d'activité.

Nous devrions envisager d'utiliser les bacs à sable et les laboratoires collaboratifs pour tester ensemble les nouvelles technologies et les capacités à l'échelle et l'échange de talents entre les secteurs public et privé comme le fait le programme Industry 100 au Royaume-Uni et le nouvel échange de talent qui vient d'être lancé par le Centre de la sécurité des télécommunications. Nous pourrions ainsi remédier aux pénuries de cybertalents qui sévissent partout, parce que le fait de se cannibaliser mutuellement ne fonctionnera pas. Le recours aux réservistes ayant des compétences en cybernétique embauchés par des entreprises pourrait constituer un moyen attrayant de soutenir la reconstitution des Forces armées canadiennes, pour autant que le gouvernement ne réclame pas la propriété intellectuelle et les brevets des réservistes pour la période où ils étaient embauchés par le secteur privé.

Il convient également de souligner que l'infrastructure industrielle de défense en général, qui englobe les entreprises qui fabriquent tout, des satellites aux navires, est devenue une cible de choix pour les cybermenaces. De plus en plus, les entreprises intègrent des technologies comme l'intelligence artificielle dans leurs produits. On sait que la Chine et la Russie peuvent s'intéresser à l'intelligence artificielle du Canada par tous les moyens disponibles.

L'infrastructure industrielle de défense canadienne est étroitement intégrée dans les Forces armées canadiennes et l'infrastructure industrielle de défense américaine. Ce que nous faisons dans ce secteur revêt une grande valeur et nous sommes extrêmement vulnérables, étant donné que 90 % des entreprises de défense canadiennes sont des petites ou moyennes entreprises. Bon nombre d'entre elles n'ont pas la capacité de se défendre contre une cyberattaque parrainée par un État. Le besoin de sécuriser les entreprises canadiennes de défense, petites et grandes est croissant. Les Américains sont, sans surprise, en avance sur nous. Une norme contraignante et obligatoire sera bientôt appliquée à tous les contrats de défense du Pentagone. Il s'agit du Cybersecurity Maturity Model Certification, la CMMC. L'Association des industries canadiennes de défense et de sécurité a déjà affirmé que le Canada devrait adopter cette norme comme référence. La CMMC deviendra fort probablement de fait la norme de référence du Groupe des cinq, voire une norme mondiale, des entreprises de défense. Le fait de prendre le temps d'envisager d'adopter une autre norme au Canada pourrait s'avérer être un désavantage pour les entreprises canadiennes et un obstacle au commerce libre de tarifs douaniers.

Et bien que la CMMC soit nouvelle, d'autres réglementations liées à la cybernétique doivent aussi être modernisées en collaboration avec l'industrie puisque nous sommes à la pointe de la technologie et que nous possédons la plus grande partie de l'infrastructure.

● (0850)

En conclusion, l'assurance d'une cyberdéfense efficace au niveau national est un sport d'équipe. Si nos alliés peuvent le faire, pourquoi pas nous?

Merci. Je vais maintenant répondre à vos questions.

Le président: La parole est à M. Callan pour cinq minutes. Allez-y.

M. Tim Callan (directeur de l'expérience client, Sectigo): Bonjour. Je remercie les députés de m'avoir donné l'occasion de comparaître devant le Comité aujourd'hui.

Je m'appelle Tim Callan et je suis directeur de l'expérience et directeur de la conformité chez Sectigo, qui est un leader mondial en matière de solutions d'identité numérique, d'infrastructure à clés publiques et de certificats numériques. Il s'agit d'éléments fondamentaux pour sécuriser les opérations et les écosystèmes numériques. Mon expérience dans cet espace technologique a débuté en 2004. Auparavant, j'ai été vice-président et dirigeant chez Verisign et Symantec, et membre du conseil d'administration de DigiCert. Je suis co-créateur et co-animateur d'un balado populaire sur la sécurité informatique intitulé *Root Causes*, qui se concentre sur l'identité numérique, le cryptage et l'infrastructure à clés publiques.

Aujourd'hui, presque tous les organismes dépendent des processus numériques. Même les entreprises les plus traditionnelles et les plus déconnectées ne peuvent fonctionner correctement sans l'aide de services numériques internes et axés sur le client, qui dépendent de réseaux interconnectés complexes de serveurs, d'appareils, de flux de travail, de programmes automatisés, etc. Ces systèmes se sont développés pour s'alimenter mutuellement dans des réseaux complexes d'interdépendance et, par conséquent, le concept de défaillance isolée d'un système devient de plus en plus rare, et est remplacé par des défaillances en cascade qui peuvent interrompre un ensemble complet de services.

La panne cellulaire multinationale du 6 décembre 2018 en est un parfait exemple. Ce jour-là, environ 40 millions d'utilisateurs de O2, SoftBank et d'autres fournisseurs de services cellulaires ont subi une panne qui a duré près d'une journée. Celle-ci était due à une défaillance unique d'un seul système survenue chez un seul fournisseur de services tiers. Cette panne s'est propagée en cascade jusqu'à ce que l'ensemble des réseaux de données de plusieurs grands fournisseurs de services mobiles soient indisponibles.

Cette défaillance particulière concernait un certificat numérique, c'est-à-dire une composante qui prouve l'identité d'un élément d'un système en réseau. En l'absence d'une identité numérique adéquate, les acteurs malveillants peuvent utiliser toute une série de techniques pour s'introduire dans le système afin de voler des renseignements, de rendre des services inaccessibles ou de corrompre des processus. L'identité numérique est irremplaçable pour les stratégies de défense en profondeur, comme l'accès au réseau à confiance zéro et l'authentification sans mot de passe. L'identité numérique est nécessaire pour exploiter en toute sécurité les architectures informatiques modernes, comme DevOps, le nuage public et l'Internet des objets.

La sécurisation des identités numériques est assurée par l'infrastructure à clés publiques. Cette dernière est une méthode éprouvée d'échange de clés cryptographiques pour vérifier les systèmes connectés et crypter les données. Elle empêche les tiers de lire ou de modifier les données en transit et de se faire passer pour des acteurs légitimes au sein d'écosystèmes numériques. La plupart des mises en œuvre de l'infrastructure à clés publiques dépendent des certificats numériques, qui renferment les fonctions cryptographiques de base d'une manière qui permet des capacités essentielles, comme la gestion du cycle de vie, les données d'identité lisibles par les êtres humains et l'expiration automatique.

Le Comité doit aujourd'hui déterminer comment protéger les Canadiens contre des cybermenaces de plus en plus sophistiquées. Les événements de ces dernières années ont prouvé à maintes reprises qu'une utilisation adéquate et complète de l'identité numérique est essentielle pour fournir des processus numériques sécurisés aux entreprises, aux gouvernements, aux infrastructures, au secteur de la finance, aux transports, aux soins de santé, à l'éducation et pour presque tous les autres aspects de la vie. Malheureusement, des organismes de tous types présentent des lacunes importantes en matière de mise en œuvre. Il pourrait s'agir d'une mauvaise mise en œuvre de l'infrastructure à clés publiques, d'une cryptographie faible ou de l'incapacité de déployer une gestion automatisée des certificats pour s'assurer que tous les certificats sont à jour et exacts. Ces lacunes peuvent entraîner des interruptions de service ou des failles de sécurité de toutes sortes.

De plus, les enjeux augmentent avec l'avènement des ordinateurs quantiques. Ces derniers seront capables de vaincre facilement plus de 99 % des systèmes de cryptage du monde. Plus particulièrement, les algorithmes RSA et de cryptographie à courbe elliptique pourront être cassés en beaucoup moins de temps, ce qui rendra les données cryptées susceptibles d'être exposées par tout attaquant ayant accès à un ordinateur quantique. Pour répondre à cette menace, de nouvelles primitives cryptographiques, appelées cryptographie post-quantique, sont déployées. De nouveaux algorithmes cryptographiques post-quantiques sont nés d'un effort mondial conjoint des gouvernements, des universités et de l'industrie, et les organismes de normalisation travaillent actuellement à leur intégration. À terme, les fournisseurs de logiciels, de matériel et de services proposeront des produits compatibles avec la cryptographie post-quantique, qui pourront être déployés dans tous les systèmes informatiques.

Le gouvernement et l'industrie devraient commencer à se préparer pour la cryptographie post-quantique en dressant l'inventaire de leur cryptographie, en mettant en œuvre des solutions de déploiement et de gestion automatisées et en assurant la souplesse cryptographique. La souplesse cryptographique est la capacité de surveiller, de comprendre et de mettre à jour l'ensemble de la cryptographie dans tous les processus et environnements, aujourd'hui et demain. Nous devons agir dès aujourd'hui.

● (0855)

Merci.

Le président: Merci, monsieur Callan.

Madame Gallant, vous avez six minutes. Allez-y.

Mme Cheryl Gallant (Renfrew—Nipissing—Pembroke, PCC): Monsieur Callan, l'identifiant numérique que vous avez mentionné, les certificats, sont-ils uniquement destinés au travail, ou proposez-vous de les utiliser pour les Canadiens ordinaires et à des fins personnelles? Le gouvernement exigerait-il des Canadiens qu'ils possèdent ces certificats pour accéder aux prestations et aux services?

M. Tim Callan: C'est une question légèrement différente. Les certificats numériques sont à la base de tous nos processus numériques, de sorte que les citoyens canadiens en dépendent, qu'ils le sachent ou non.

Si vous me demandez si le pays devrait exiger un identifiant numérique, comme le font de nombreux pays européens, je répondrais que le monde se dirige assurément dans cette direction. Cette mesure présente de nombreux avantages. Elle permet de vérifier facilement que vous êtes une personne bien réelle et que votre identité n'a pas été usurpée. Lorsqu'on utilise correctement cette technologie, l'interaction est beaucoup plus facile pour le citoyen moyen qui ne possède pas nécessairement un diplôme en informatique. Un certain nombre de pays européens obtiennent de bons résultats avec ces systèmes.

Il existe également une norme paneuropéenne appelée eIDAS, qui est largement utilisée dans l'Union européenne et au Royaume-Uni à cette fin. La mise en place de ce genre de système au sein d'organismes gouvernementaux n'est pas une mince affaire, mais le gouvernement est un bon point de départ.

Mme Cheryl Gallant: Ce système est donc principalement destiné à l'industrie, mais certaines personnes l'utilisent à des fins personnelles...

Madame Cianfarani, quelles sont les ressources dont disposent vos entreprises et dont le gouvernement ne dispose pas ou qu'il ne connaît pas?

Mme Christyn Cianfarani: Lorsque vous parlez de ressources, je suppose que vous parlez à la fois de services et de produits. La difficulté actuelle réside dans le fait qu'une grande partie des... Assurément, au sein des organismes, les ressources sont utilisées au sein des organismes et ont été créées par ceux-ci. Il n'y a donc pas beaucoup de correspondances entre les lacunes en matière de capacités et l'exposition de ces lacunes à l'industrie, car il n'est pas dans la nature du Centre de la sécurité des télécommunications d'exposer ses lacunes en matière de capacités. C'est l'un des principaux problèmes, à savoir que nous ne savons pas quels sont les renseignements qui nous manquent. Ils ne savent pas ce que nous avons, et nous ne savons pas où se situent leurs lacunes en matière de capacités.

Cependant, je peux dire que l'industrie même, environ 60 % de l'industrie, a la capacité de sécuriser les réseaux et l'infrastructure des données, ce qui signifie généralement que nous nous accomplissons l'assurance des missions. Cette dernière peut concerner les réseaux situés dans des environnements menaçants, mais aussi les capteurs et les actifs, comme les avions, les navires et les chars qui opèrent dans des environnements en réseau, comme au sein des Forces armées canadiennes, ainsi que l'infrastructure — comme le nuage, par exemple — que les Forces armées canadiennes elles-mêmes utilisent dans le cadre de leurs activités.

Nous sommes également très forts dans des secteurs stratégiques, comme le cryptage, les tests de pénétration et la surveillance des menaces, et les actifs spatiaux que nous entretenons, exploitons et déployons, comme le satellite RADARSAT-2, servent à la collecte de renseignements et au ciblage.

Je peux vous dire ce dont nous disposons, mais je ne peux pas vous dire où se situent les lacunes des organismes en matière de capacité.

● (0900)

Mme Cheryl Gallant: C'était ma prochaine question.

De quelle manière le Canada s'expose-t-il à des menaces lorsqu'il choisit d'expatrier ces travaux au lieu de soutenir son infrastructure nationale?

Mme Christyn Cianfarani: Je pense que les pays déploient actuellement des efforts considérables pour sécuriser leurs chaînes d'approvisionnement. J'ai mentionné la CMMC, grâce à laquelle les Américains essaient en fait de sécuriser l'ensemble de leur chaîne d'approvisionnement. Nous estimons que le fait de ne pas adopter ce type de normes ou de méthodologies pour garantir la sécurité de la chaîne d'approvisionnement accroît notre vulnérabilité.

Nous pensons également que ce que vous devez obtenir dans ce secteur particulier, le meilleur moyen de réduire vos vulnérabilités dans ce secteur particulier, est d'employer des citoyens canadiens possédant des habilitations de sécurité canadiennes au sein des entreprises canadiennes qui paient des impôts canadiens et qui ont des chaînes d'approvisionnement canadiennes. C'est probablement la meilleure façon de réduire les vulnérabilités au minimum.

Mme Cheryl Gallant: Pourquoi pensez-vous que le gouvernement soutient les entreprises étrangères au lieu d'utiliser les industries canadiennes?

Mme Christyn Cianfarani: Je pense que le problème... Ce n'est pas nécessairement l'adoption de technologies étrangères. Je crois que c'est le fait d'investir la majorité des fonds, pour des ressources ou des technologies, dans sa propre organisation. Le SCRS augmente son bassin de ressources et augmente le nombre de logiciels et de technologies qu'il crée à l'interne pour ses propres besoins. C'est bien. Nous ne sommes pas contre ce genre de comportement ou d'activité. Ce que nous disons, c'est que l'apport du secteur privé — le secteur privé canadien assurément — peut être beaucoup plus important si on regarde la situation dans son ensemble.

Nos alliés s'en sont rendu compte très rapidement. Dans notre rapport 2020, je crois, nous avons interrogé des experts en sécurité de divers pays, en particulier au Royaume-Uni et aux États-Unis, et ils ont déterminé que plus de 50 % de leurs cyberopérations sont menées actuellement à parts égales par des fournisseurs et par les organismes eux-mêmes. Ils prennent donc cette direction.

Le président: Je vous remercie, madame Gallant.

Monsieur Sousa, vous avez six minutes. Allez-y, s'il vous plaît.

M. Charles Sousa (Mississauga—Lakeshore, Lib.): Je vous remercie, monsieur le président.

Je vous remercie tous les deux de votre témoignage.

Madame Cianfarani, j'ai trouvé très encourageant ce que vous avez dit dans votre déclaration liminaire au sujet de l'expertise canadienne, même si les Canadiens ne l'utilisent pas nécessairement autant que nos alliés et le Groupe des cinq. J'ai été frappé aussi par votre commentaire au sujet de la chaîne d'approvisionnement et du fait que tout va tellement vite dans le cyberunivers qu'il est difficile de suivre le rythme.

Comment faites-vous pour y arriver? Vous enseignez dans ce domaine et sur ce sujet en particulier.

Mme Christyn Cianfarani: Eh bien, je passe beaucoup de temps à essayer de me tenir à jour. En fait, j'ai toute une industrie autour de moi qui me tient informée. Nous échangeons de l'information et des connaissances. Il faut être ouvert à la collaboration.

M. Charles Sousa: Je pense que cela fait partie de la solution que vous mettez de l'avant. C'est exactement ce que vous voulez proposer que les autres fassent dans ce domaine, et que le Canada joue un rôle plus important à cet égard.

Le risque lié à la chaîne d'approvisionnement que vous avez évoqué est important. À propos de ce que vous avez dit, quelle serait votre préoccupation la plus pressante?

Mme Christyn Cianfarani: Il y a quelques éléments. Le premier est de sécuriser la chaîne d'approvisionnement, ce qui veut dire, d'une part, adopter des normes réglementaires au fur et à mesure qu'elles deviennent accessibles. Nous sommes inquiets. Cinquante pour cent de la base industrielle de défense sont des exportations, et la moitié de ces exportations sont destinées aux États-Unis. Si nous voulons être un partenaire fiable dans la chaîne d'approvisionnement aux États-Unis, nous allons devoir avancer de pair avec eux pour nous assurer de pouvoir être des partenaires de confiance et qu'ils pourront s'approvisionner chez nous. C'est le premier élément. C'est un enjeu économique pressant pour notre pays.

Le deuxième élément est l'échange de l'information sur les menaces. Vous avez sans doute vu dans les journaux dernièrement qu'il y a eu des brèches via le secteur privé, via les fournisseurs d'infrastructures essentielles ou via la base industrielle de défense. Nous devons nous assurer d'avoir des liens beaucoup plus étroits et de divulguer de manière proactive ces brèches, afin de pouvoir profiter des technologies et des organismes pour obtenir la meilleure protection possible. C'est le quid pro quo, et il faut un mécanisme institutionnel. Cela ne peut se faire chaque fois qu'une incursion se produit. Il faut qu'un système soit déjà en place afin de pouvoir en tirer parti si et quand, potentiellement, les cyberattaques se multiplient, comme nous pouvons le constater dans le théâtre de la guerre en Ukraine en ce moment.

● (0905)

M. Charles Sousa: C'est un bon point.

Monsieur Callan, nous venons de parler d'une solution globale concernant l'architecture en collaboration avec le secteur privé. Vous avez parlé des enjeux numériques. Pouvez-vous nous en dire plus sur la souplesse nécessaire, les cyberinnovations...? Comment devons-nous procéder pour rester à l'avant-garde des cyberinnovations et mieux travailler en collaboration avec le secteur privé pour réussir?

M. Tim Callan: Nous avons un secteur privé très solide, très actif du côté des organismes de normalisation dans l'industrie et des organismes coopératifs. Je mentionne encore une fois la cryptographie post-quantique, qui en est un excellent exemple. Des gens du monde entier se sont réunis pour construire une nouvelle architecture de défense contre une menace émergente identifiée. Des universités et des sociétés canadiennes y ont joué un rôle très important. J'ose même dire que les Canadiens se sont distingués dans le cadre de cet effort particulier.

C'est exactement ce dont nous avons besoin. Rien ne peut exister uniquement à l'intérieur des frontières d'un pays. L'Internet et la technologie voyagent bien au-delà des frontières. Nous devons établir des partenariats pour obtenir ce qu'il y a de mieux, car c'est ce que font les attaquants. Ils font fi des frontières. Tout ce qui les intéresse, c'est d'arriver à leurs fins.

C'est en travaillant ensemble avec d'autres organismes — gouvernementaux ou privés — dans le monde que les fournisseurs de technologie peuvent le mieux protéger les entreprises et le gouvernement, etc.

M. Charles Sousa: Madame Cianfarani, on mentionnait dans un des rapports que le secteur manufacturier était le plus à risque, en particulier pour ce qui est de l'approvisionnement. Comme les entreprises canadiennes sont principalement des PME, et que la masse critique existe aux États-Unis et ailleurs dans le monde, mais pas chez nous, comment pouvons-nous surmonter cet obstacle?

Mme Christyn Cianfarani: Comme nous l'avons mentionné, il faut disposer de ce qui ressemble à un mécanisme institutionnel dans le cadre duquel on peut créer des liens de collaboration entre l'industrie, le secteur privé et les organismes ou les organes gouvernementaux.

Le CCC, le Centre canadien pour la cybersécurité, a pris une bonne initiative en commençant à mobiliser une équipe au sein de son organisation. Je pense qu'ils sont six actuellement, mais qu'ils pourraient sans doute être beaucoup plus nombreux, étant donné le très grand nombre d'entreprises. Il a commencé à mobiliser une équipe qui est responsable de sécuriser des secteurs de la base industrielle. On met l'accent actuellement sur les infrastructures critiques, mais, si on comprend bien, le centre commence à se pencher sur la base industrielle de défense, ce qui comprend le secteur manufacturier dont vous avez parlé.

L'idée commence lentement à circuler qu'il faut mobiliser les entreprises, mieux les sensibiliser à la responsabilité qu'elles ont d'avoir une meilleure cyberhygiène, en échange de quoi, nous allons les inclure un peu plus dans le cercle du secret.

M. Charles Sousa: Oui, c'est un bon point.

Je vous remercie tous les deux.

Je vous remercie aussi, monsieur le président.

Le président: Je vous remercie, monsieur Sousa.

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

[*Français*]

Mme Christine Normandin (Saint-Jean, BQ): Je remercie les deux témoins d'être avec nous aujourd'hui.

Monsieur Callan, j'aimerais parler du recours à l'identité numérique par les gouvernements. Il peut parfois y avoir une panne d'un système informatique, même sans l'intervention d'acteurs externes malveillants. Au Québec, récemment, nous avons vu que la simple implantation d'un système a causé des difficultés à la Société de l'assurance automobile du Québec.

Quand il y a un acteur malveillant, comme cela s'est produit en Albanie, qui a été la cible d'une cyberattaque de l'Iran, c'est problématique. L'être humain semble souvent être le premier maillon faible.

Au Canada, la cyberhygiène des Canadiens est-elle suffisamment bonne pour assurer que la mise en vigueur d'un nombre croissant de services gouvernementaux numériques se déroule bien?

J'aimerais aussi avoir vos commentaires sur l'Internet des objets. Dans quelle mesure cela peut-il être une porte d'entrée pour des individus ayant des intentions malveillantes?

● (0910)

[*Traduction*]

M. Tim Callan: Oui, l'être humain est toujours un maillon faible dans tout système numérique. On peut très facilement mettre au point des solutions cryptographiques mathématiquement pures qui sont sans failles. Il est plus difficile d'enseigner aux gens à ne pas tomber dans les pièges. On appelle cela l'ingénierie sociale. C'était un problème avant l'avènement des ordinateurs, et cela demeure une forme d'attaque très importante.

Nous pouvons construire des systèmes informatiques pour aider à protéger les gens de ce genre de pièges avec des outils comme la cryptographie. En mettant cela en place, je peux vous dire qu'il est très difficile, voire impossible, à un travailleur de donner un accès sans le vouloir à un criminel, dans la mesure où les bons systèmes sont mis en place. C'est le genre de solutions que le gouvernement et les entreprises peuvent examiner et mettre en place. C'est l'un des domaines où l'on voit que les entreprises et le gouvernement continuent de manquer à leur devoir en ne faisant pas tout ce qu'ils peuvent faire.

Au sujet de l'Internet des objets, c'est un autre domaine où l'on pourrait renforcer beaucoup la sécurité. Nous pouvons construire des systèmes cryptographiquement sécurisés pour empêcher que les appareils soient la cible d'intrusion ou une source possible de perturbation de nos systèmes, de nos infrastructures, du secteur manufacturier, de nos réseaux de transport, etc. Encore une fois, nous constatons souvent que les appareils ne sont pas les mieux protégés contre les intrusions, et cela est lié à des problèmes comme le coût, la forme, la taille, l'alimentation et la bande passante disponibles, qui amènent les entreprises ou les fabricants à lésiner sur la sécurité. Ce qui a pour conséquence d'ouvrir la porte à des attaques. Il y en a eu beaucoup sur les automobiles et beaucoup sur les infrastructures.

[*Français*]

Mme Christine Normandin: Merci, monsieur Callan.

Comme je n'ai pas beaucoup de temps de parole, j'aimerais aussi poser des questions à Mme Cianfarani.

Madame Cianfarani, j'aimerais avoir vos observations sur la rigidité dont le gouvernement fait parfois preuve en matière de certificats de sécurité. Par exemple, des gens m'ont dit avoir postulé pour un poste au Centre de la sécurité des télécommunications et que c'était à la dernière étape de la vérification qu'ils étaient bloqués, parce que la Gendarmerie royale du Canada, ou GRC, était un peu stricte sur la délivrance de certificats de sécurité.

Ne pourrions-nous pas nous permettre d'être un peu plus ouverts pour qu'il y ait une meilleure collaboration entre le secteur privé et le secteur public, de telle sorte que les gens puissent plus facilement faire le saut de l'un à l'autre?

Les normes de sécurité fédérales sont-elles trop strictes? Ne sont-elles pas tout simplement inappropriées?

Qu'est-il possible de corriger pour assurer une meilleure collaboration?

[*Traduction*]

Mme Christyn Cianfarani: Je présume que vous parlez des cotes et des classifications de sécurité. Je ne peux pas vous parler des méthodes utilisées par les organismes pour les accorder. Ce que je peux vous dire, c'est que, comme nous sommes aux prises avec ce problème dans le secteur de la défense, l'idée au pays est qu'il y ait le moins de cotes de sécurité possible. On pense que moins il y en aura, plus on sera en sécurité, moins il y aura de gens qui auront accès à ce genre d'information et de connaissances, plus le pays sera en sécurité, car il y aura sans doute moins de fuites ou choses du genre.

D'autres pays ont adopté une approche très différente et commencent à déclassifier de plus en plus d'information. Nous pouvons voir cela en temps réel en Ukraine lorsque le GCS britannique, le service de communication du gouvernement, déclassifie de l'information en temps réel pour montrer à tous ce qui se passe. C'est le cas également dans la stratégie de sécurité nationale qui vient d'être mise à jour aux États-Unis et dans laquelle on dit que plus d'information sera déclassifiée pour rendre la population plus consciente de ce qui se passe.

Qu'il s'agisse des contrôles de sécurité, ou des organismes ou du Programme de sécurité des contrats qui s'en occupe pour la Défense nationale, il faut que notre optique change. Je pense que l'idée voulant qu'il faille tenir les gens à l'écart, au lieu de les inclure et de mieux les informer, doit changer.

[*Français*]

Mme Christine Normandin: Merci beaucoup.

Jusqu'à quel point le fait que les ministères travaillent en vase clos empêche-t-il la collaboration avec le secteur privé?

● (0915)

[*Traduction*]

Mme Christyn Cianfarani: Je pense que cela nuit beaucoup à nos efforts de coopération. On le voit régulièrement au sein des entités gouvernementales: entre la Défense nationale et les Forces armées canadiennes et les organismes de sécurité, entre les organismes de sécurité et le gouvernement. Je ne veux pas revenir sur ce qui s'est dit hier, mais on l'a vu en temps réel lors de l'ingérence étrangère au sein du gouvernement, entre les ministères, les Affaires étrangères et la Sécurité publique. On l'a vu lors de la présence du convoi à Ottawa, lorsque les organismes gouvernementaux provinciaux et municipaux, et en fait, l'ensemble du gouvernement fédéral n'étaient pas coordonnés dans leurs stratégies ou l'échange d'information face aux menaces. On le voit et le sent de notre côté dans le secteur privé, où très souvent on se demande ce qui se passe, si on doit être informé, si la menace croît ou décroît.

Je pense que notre façon de fonctionner en vase clos nous nuit au pays, et c'est regrettable, car nous sommes un si petit pays.

Le président: Nous allons devoir en rester là.

Nous passons à Mme Mathyssen pendant six minutes.

Mme Lindsay Mathyssen (London—Fanshawe, NPD): Je vous remercie, monsieur le président.

Je remercie aussi les témoins d'être avec nous aujourd'hui.

Madame Cianfarani, vous avez parlé de normes institutionnalisées, et bien entendu, nous avons vu beaucoup d'allers-retours d'un gouvernement à l'autre au sujet de l'approvisionnement, parce qu'il n'y a pas de plans à long terme neutres et non partisans, et cela a beaucoup nui à ce dont vous parlez, je crois, au sujet de ce que l'industrie peut faire, ce qu'elle peut fournir, comment elle peut planifier, construire, en particulier quand on sait, comme vous l'avez mentionné, que la majorité des entreprises canadiennes sont des PME.

Pourriez-vous nous parler du fait que, encore une fois, il semble que nous changions de direction? Nous avions un gouvernement qui a opté, pour certains projets d'approvisionnement, pour le fournisseur unique, puis cela a été rejeté par un autre gouvernement qui disait qu'on avait besoin d'un processus d'appels d'offres ouvert. Cela a pris beaucoup de temps et coûté beaucoup d'argent. Il semble maintenant qu'on revienne à l'idée des exigences opérationnelles urgentes, et beaucoup de projets d'approvisionnement sont axés sur cela pour passer outre au processus ouvert.

Pourriez-vous nous parler des répercussions que cela a sur l'industrie dans son ensemble, du point de vue de la cybersécurité, de même que de l'approvisionnement militaire dans son ensemble?

Mme Christyn Cianfarani: On parle beaucoup de ce sujet, qui relève de l'examen de la politique de défense, de sa mise à jour, et du concept de maintien continu des capacités ou d'approvisionnement agile.

Il y a un lieu et un moment pour la concurrence. Habituellement, les pays ouvrent la porte à la concurrence lorsqu'il y a deux fournisseurs étrangers et aucun fournisseur titulaire canadien. C'est la façon normale de procéder dans le monde. Lorsqu'il y a un fournisseur titulaire canadien — et ce dont nous parlons ici dans le domaine cyber, c'est d'avoir une entreprise canadienne déjà fiable, sélectionnée, avec qui on est prêt à faire affaire, et dans ce cas particulier, le modèle du fournisseur unique n'est pas et ne doit pas être vu comme le fait de court-circuiter le processus. Au contraire, cela doit être vu comme une solution d'agilité.

Le problème, c'est lorsqu'on ne comprend pas que la plupart des pays utilisent le processus du fournisseur unique ou de l'approvisionnement agile pour maintenir et faire croître les entreprises au sein même de leur pays, et assurer leur viabilité, ce qui veut dire que la sécurité nationale est la sécurité économique. On comprend que, fondamentalement, en investissant dans une entreprise canadienne, et en le faisant d'une façon agile avec des sources de confiance ou des personnes de confiance, on peut investir, en fait, dans notre économie.

Mme Lindsay Mathyssen: Dans ce cas, les grandes entreprises n'auraient-elles pas systématiquement déjà un avantage qui, de plus, rendrait impossible pour les PME de leur livrer une réelle concurrence?

Mme Christyn Cianfarani: Eh bien, elles ne jouent pas dans la même ligue. Les petites entreprises font habituellement partie de la chaîne d'approvisionnement.

Les petites entreprises obtiennent habituellement des contrats prescrits de deux façons. Soit il s'agit d'une technologie de créneau — ce que les organismes recherchent habituellement, et ce sont des marchés prescrits, très ciblés —, soit il s'agit de plateformes ou de grands projets où il y a le fournisseur d'un produit — un navire, un avion, peu importe —, et ce fournisseur, cet équipementier, a toute une chaîne d'approvisionnement. Dans ces cas, ce que l'on veut, c'est être un partenaire dans la chaîne d'approvisionnement, un partenaire de confiance pour ces équipementiers. Cela veut dire positionner sa base industrielle de défense ou sa base industrielle comme acteurs dans la chaîne d'approvisionnement.

D'où l'idée qu'il faut être des partenaires de confiance dans la chaîne d'approvisionnement, et veiller à avoir les règlements appropriés en place pour qu'on ne finisse pas par ériger des barrières commerciales non tarifaires, en d'autres mots, que les équipementiers disent qu'on ne peut pas jouer dans leur carré de sable parce que nous n'avons pas de certification. C'est ainsi qu'on s'assure que les petites entreprises ont leur part du gâteau, si on veut.

● (0920)

Mme Lindsay Mathyssen: D'accord. On voit beaucoup cela dans l'approvisionnement. Une entreprise ne peut tout faire. Elle sous-traite toutes ces pièces. Elle s'efforce, en particulier s'il y a des exigences d'achats canadiens, d'achats autochtones, par exemple, de répondre à certaines normes, certains pourcentages, etc.

Mais, encore une fois, comment peut-on s'assurer que les produits sont principalement canadiens, si ce sont les pièces du casse-tête pour créer une norme générale globale, et que ce n'est pas simplement accaparé, comme on le voit dans l'industrie des télécommunications, par les grandes entreprises?

Mme Christyn Cianfarani: On peut le faire. Ce n'est pas un modèle unique. Divers incitatifs peuvent être utilisés. Au Canada, nous avons ce qu'on appelle une politique de contreparties ou une politique des retombées industrielles et technologiques qui s'applique au moment de l'approvisionnement. Cela incite les entrepreneurs principaux à utiliser des entreprises canadiennes au sein de leurs chaînes d'approvisionnement afin d'obtenir des contrats du gouvernement canadien. Ce sont de moyens que l'on peut utiliser.

On peut aussi dicter les exigences et dire qu'on veut que l'entreprise travaille avec tel fournisseur parce qu'il possède telle technologie. On peut préciser cela. Dans le cas du cyberapprovisionnement et de l'approvisionnement agile, nous pensons que si vous avez des firmes canadiennes en qui vous avez déjà confiance, vous pourriez simplement acheter directement auprès d'elles, ce qui accélère le processus. Vous avez déjà des partenaires de confiance qui possèdent les classifications dont vous avez besoin, et vous pouvez les utiliser encore et encore.

Le président: Je vous remercie, madame Mathyssen.

Chers collègues, nous avons encore une fois le même problème. Nous allons tenter d'avoir une série complète de questions de 25 minutes. Il se pourrait que nous débordions sur la deuxième heure, mais je pense que c'est une bonne chose de le faire.

Monsieur Kelly, vous avez cinq minutes.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Merci, monsieur le président.

Dans le rapport de CADSI, on souligne que, contrairement au Canada qui peut prendre des années, voire des décennies pour déployer de nouvelles cybercapacités, nos adversaires et alliés ont tous montré leur aptitude à le faire en quelques mois ou semaines. À quel point SPAC est-il dysfonctionnel?

Mme Christyn Cianfarani: Eh bien, nous essayons d'appliquer à l'approvisionnement agile un modèle qui n'a pas été conçu pour celui-ci. Ce que nous avançons, ce n'est pas que le modèle actuel est dysfonctionnel, mais plutôt qu'il est inadéquatement appliqué aux technologies.

M. Pat Kelly: Donc, le modèle de SPAC est un modèle inapproprié en matière de cybersécurité.

Mme Christyn Cianfarani: Oui.

M. Pat Kelly: D'accord. Merci.

Dans votre rapport, vous dites que l'urgence émane du fait que les cybermenaces sont beaucoup plus rapides que les processus décisionnels du gouvernement. Que doit faire le gouvernement pour être en mesure de vraiment prendre des décisions rapides pour protéger les Canadiens dans le domaine de la cybersécurité?

Mme Christyn Cianfarani: Eh bien, dans un modèle, le temps est le nerf de la guerre. Dans notre rapport, dans celui auquel vous faites référence, j'imagine, soit celui de 2021 intitulé *Procurement at Cyber Speed*, il y a essentiellement trois choses qui pourraient être faites. Sachez que, si vous avez ce rapport en main, la page 18 est fort intéressante.

Donc, vous commencez par créer des projets-cadres qui viennent assurer la capacité. Comme je l'ai proposé, vous éliminez les obstacles, de sorte que vous avez des partenaires de confiance et qu'il y a acquisition et perfectionnement des compétences ici même au pays, puis vous affectez des fonds à l'échelon du projet-cadre.

L'autre chose que vous pourriez faire serait d'avoir un financement plus souple. Actuellement, il y a énormément de processus d'approbation. La demande passe par le Conseil du Trésor où il y a environ 200 étapes à franchir selon le vieux modèle. Vous devriez vous débarrasser de toute cette chaîne de production, si je puis dire, et envisager des fonds qui bénéficient de la souplesse du crédit 1 et de la possibilité d'acquérir de nouvelles capacités du crédit 5.

Ensuite, la dernière chose que vous pourriez faire serait d'accélérer les processus d'approbation et de conclusion de marchés, par exemple, comme je l'ai dit, en établissant des lignes directrices, dans lesquelles vous pouvez exiger de la technologie et des services conçus par des Canadiens possédant une autorisation de sécurité canadienne et par des entreprises canadiennes de confiance qui paient leurs impôts au Canada et dont la propriété intellectuelle reste au pays. Et vlan! Voilà quelque chose que je peux acheter.

● (0925)

M. Pat Kelly: D'accord. Merci.

Il y a plusieurs années, le comité des opérations gouvernementales a étudié l'approvisionnement auprès des petites et moyennes entreprises. Vous avez parlé des différences et du fait qu'énormément de fournisseurs en cybersécurité et en cyberdéfense sont de petites entreprises. On a dit au comité des opérations gouvernementales que les petites entreprises ne peuvent tout simplement pas répondre aux exigences du système d'approvisionnement actuel, qu'il est hyper compliqué et qu'il est impossible de transiger avec SPAC, ce qui fait que seulement les fournisseurs spécialisés s'y collent, des fournisseurs spécialisés qui ont pour tout modèle d'affaires de trouver une façon de déjouer le système d'approvisionnement. Vous avez donc de fait des marchés d'exclusivité, puisqu'il n'y a tout simplement pas de concurrence.

Est-ce un problème dans le cas de l'approvisionnement en cybersécurité?

Mme Christyn Cianfarani: Les organismes qui ont témoigné vous ont probablement dit que, dans les faits, ils ne fournissent pas de produits et services. Il me semble qu'ils étudient le système et se disent que, ouf!, s'ils devaient l'appliquer à l'approvisionnement en cybertechnologie, ce ne serait pas de la tarte, ce qui est probablement l'une des raisons pour lesquelles ils ne le font pas. Est-ce que le système est lourd et plus ou moins rigide, et y a-t-il autour de celui-ci toute une industrie artisanale qui se consacre à la façon de l'utiliser? Tout à fait. C'est pour cette raison que nous sommes souvent présents ici pour vous dire qu'il peut être grandement amélioré. Surtout dans le cas du cyber, il y a beaucoup de façons dont on pourrait grandement améliorer le système et le rendre beaucoup plus agile.

Le président: Il vous reste 20 secondes, monsieur Kelly.

M. Pat Kelly: D'accord.

Pendant les 20 secondes à venir, aimeriez-vous fournir des précisions sur la recommandation dans votre rapport sur la modernisation en cyberapprovisionnement?

Mme Christyn Cianfarani: Eh bien, comme je l'ai dit, il y a ces trois choses. Je ne veux pas les répéter plus que je ne l'ai déjà fait, mais, encore une fois, il y a le concept des projets-cadres, où se trouve une bonne partie des fonds que vous pouvez ensuite affecter à des projets secondaires, ce qui signifie que je pourrais acheter diverses technologies, les mettre à l'essai, puis les intégrer à mon entreprise de façon très rapide, et que le financement n'aurait pas à constamment passer par le Conseil du Trésor et ses divers échelons d'approbation. Une fois que j'ai un bon financement de base, je peux procéder à son affectation sous forme de projets.

Enfin, il y a ce processus accéléré, selon lequel un projet secondaire qui répond à divers critères, que nous estimons bons sur les plans de l'économie et de la sécurité, peut faire l'objet d'un approvisionnement agile sans avoir à passer par les 200 étapes nécessaires pour y arriver.

Le président: Merci, monsieur Kelly.

Madame O'Connell, vous avez cinq minutes. Je vous en prie, allez-y.

Mme Jennifer O'Connell (Pickering—Uxbridge, Lib.): Merci, monsieur le président.

Je vais commencer par Mme Cianfarani.

Vous avez parlé du secteur privé et des gouvernements travaillant avec le secteur privé, mais des témoins nous ont également dit qu'il peut y avoir des difficultés parce que le secteur privé n'est pas forcément enclin à communiquer ses renseignements au gouvernement quand il y a une brèche de sécurité. Il peut y avoir une raison pour cela. Des secrets commerciaux peuvent être en jeu ou l'entreprise souhaite cacher à ses clients ou aux membres du conseil d'administration qu'il y a des vulnérabilités.

Cela dit, si le gouvernement peut jouer un rôle pour favoriser cette coordination ou mieux s'en charger, de quelle façon recommandez-vous ou proposez-vous que nous amenions le secteur privé à faire davantage preuve d'ouverture et de transparence à propos de possibles brèches? Procéder de la sorte aiderait aussi le gouvernement à se préparer à ce qui l'attend et aux menaces existantes.

Mme Christyn Cianfarani: Vous avez tout à fait raison. Il y a le bâton et la carotte. C'est ainsi que j'aime voir les choses. Dans certains cas, le bâton pourrait pousser certaines entreprises à divulguer leurs brèches. La majorité des entreprises auxquelles nous parlons affirment que tant qu'elles sont incluses dans le processus établissant la façon de faire et la transmission de l'information, tant que tout est fait de façon proactive de sorte que leur marque ou leur entreprise n'en souffre pas... En d'autres mots, vous adoptez l'optique inverse et affirmez que la divulgation proactive est une bonne chose. Personne ne devrait avoir honte d'avoir subi une brèche, car ce n'est qu'une question de temps. Présentez les choses ainsi, puis déclarez que lorsque ces entreprises vous les divulguent de façon proactive, elles gagnent l'accès aux vulnérabilités des autres afin qu'elles puissent devenir de meilleures entreprises. C'est une relation donnant-donnant, si vous voulez.

Je crois que ce sont les pièces manquantes du puzzle. Si vous voulez les obliger à le faire, vous devez inclure les entreprises et trouver une façon de faire efficace qui ne nuit pas à leurs activités. Dans un même ordre d'idées, vous devrez partager cette information en retour, ce qui est quelque chose que nous souhaitons et qui nous permettra de nous améliorer et de rendre l'écosystème en général plus sûr.

● (0930)

Mme Jennifer O'Connell: C'est super. Merci.

Dans votre déclaration liminaire, je crois que vous avez fourni un exemple du Royaume-Uni.

Mme Christyn Cianfarani: C'était Industry 100, au Royaume-Uni.

Mme Jennifer O'Connell: Oui. Merci.

Je suis intriguée. Pourriez-vous nous dire un peu à quoi cela ressemble? Depuis quand cela existe-t-il? Est-ce tout nouveau? De quelle façon pourrions-nous nous inspirer de certains de ses meilleurs aspects? Pourriez-vous nous fournir plus de détails sur cet exemple?

Mme Christyn Cianfarani: Oui. C'est un modèle collaboratif qui n'est plus tout à fait nouveau. En somme, c'est un programme qui contribue à remédier à court terme à la pénurie de main-d'œuvre spécialisée.

Les entreprises du programme affectent du personnel de leur équipe au National Cyber Security Centre. Un peu comme si nous avions certains de nos employés qui travaillaient au sein du Centre de la sécurité des télécommunications. Elles le font à temps partiel. Il n'y a pas de séparation entre ces partenaires industriels, ce qui veut dire qu'ils peuvent être en concurrence à un moment donné, mais quand il est question de travailler aussi au National Cyber Security Centre, elles le font toutes ensemble de pair avec les fonctionnaires dans un nouvel environnement neutre et sur une base non transactionnelle, ce qui veut dire qu'elles ne sont pas payées pour œuvrer ensemble à la sécurité nationale du Royaume-Uni.

Ces personnes du secteur privé peuvent faire de tout, qu'il s'agisse de rédiger des livres blancs ou de concevoir des logiciels, voire d'assurer la liaison entre leur entreprise et l'entité gouvernementale sur les menaces et incursions qui se produisent. C'est une activité de type national.

Mme Jennifer O'Connell: Merci.

Pour continuer dans cette veine, quand je siégeais au comité des finances, nous nous sommes rendus au Royaume-Uni dans le cadre de notre examen annuel de l'étude sur la lutte contre le blanchiment d'argent. On nous a dit que la culture y est différente quand il est question de cette ouverture et de la sécurité, car il y a assez souvent des attaques terroristes plus ciblées là-bas. Donc, au sein de la population, il y a une plus grande acceptation... Par exemple, même les registres pour les hypothèques sont très courants. Au Canada, toutefois, et je dirais même en Amérique du Nord, la culture à propos de ces renseignements est un peu plus délicate. Il est plus difficile de convaincre les Canadiens d'être aussi ouverts.

Avez-vous des réflexions à faire là-dessus?

Mme Christyn Cianfarani: Je crois que c'est une affirmation fort judicieuse. Nous constatons ce type d'urgence tout le temps. L'Union européenne est le théâtre d'une guerre à l'heure actuelle, et bien que les Canadiens en ressentent en quelque sorte les effets, ceux-ci ne sont pas très grands. C'est l'une des raisons pour lesquelles nous disons que, s'il y a une partie de la population ou de la communauté d'affaires qui est disposée à être un peu plus ouverte par rapport à ce genre de choses, c'est bien l'infrastructure industrielle de défense canadienne, vu sa nature.

Le président: Malheureusement, nous devrons nous en tenir à cela. Nous ne pourrons tout simplement pas respecter le temps alloué.

Madame Normandin, vous avez deux minutes et demie.

[*Français*]

Mme Christine Normandin: Merci beaucoup.

Madame Cianfarani, j'aimerais que nous revenions à la norme relative à la certification du modèle de maturité de la cybersécurité des États-Unis, dont vous avez parlé. L'une de vos recommandations est que le Canada ne travaille pas à sa propre norme, mais adopte plutôt celle-là.

Disposez-vous d'information indiquant que le Canada est en train de travailler sur sa propre norme ou est-ce qu'aucun travail n'est fait en ce sens?

[*Traduction*]

Mme Christyn Cianfarani: Le Canada étudie en ce moment même la norme relative à la certification du modèle de maturité de la cybersécurité. L'ambassade canadienne aux États-Unis et, dans une certaine mesure, le ministère de la Défense nationale, le ministère de la Sécurité publique et SPAC suivent de près le dossier et s'intéressent à cette norme.

Ce qui est difficile, c'est qu'ils essaient d'établir si la norme doit être « canadianisée » de quelque façon. Nous estimons que, si nous procédons ainsi et développons des parties canadianisées de la norme, nous allons créer une norme différente. Les entreprises canadiennes se retrouveraient ainsi avec deux normes, ce qui augmenterait leurs coûts. Si nous ne faisons pas les choses correctement, les Américains pourraient aller de l'avant pendant que les entreprises canadiennes attendent la norme nationale et seraient donc laissées en plan en matière d'approvisionnement. Il y a ce sentiment d'urgence.

Ils travaillent là-dessus. Nous avons actuellement un programme exploratoire qui tente d'amener les entreprises canadiennes à concrètement participer à la norme américaine alors qu'elle est en cours d'adoption.

● (0935)

[*Français*]

Mme Christine Normandin: Merci beaucoup.

Monsieur Callan, vous avez parlé des ordinateurs quantiques qui sont capables de déjouer la cryptographie. En raison de cette capacité, il faudrait investir dans la cryptographie post-quantique.

J'aimerais que vous nous parliez de la rapidité avec laquelle il faut acquérir le matériel informatique pour maintenir notre capacité de défense constamment à jour. J'aimerais que vous compariez cela au processus d'acquisition public.

Ce processus est-il beaucoup trop lent?

[*Traduction*]

M. Tim Callan: Il est sans doute déjà trop tard, puisqu'il existe une attaque de type « stocker maintenant, décrypter plus tard », ce qui signifie que si quelqu'un a accès à votre système, il peut en extraire de grands pans de données chiffrées et simplement les stocker, puis à un moment donné, quand il aura accès à un ordinateur quantique, il pourra y accéder.

Dans le cas de secrets qui auront encore de la valeur dans 10 ans, comme les secrets militaires ou les secrets industriels de pointe, par exemple, il est probablement trop tard. Peut-être pas pour d'autres secrets, mais il est très urgent de passer dès que possible à la cryptographie post-quantique.

Le président: Merci, madame Normandin.

Madame Mathyssen, vous avez deux minutes et demie.

Mme Lindsay Mathyssen: Évidemment, la main-d'œuvre et les ressources humaines du point de vue du développement sont une chose qui affecte toutes les industries au pays et ailleurs dans le monde.

Ma question s'adresse à vous, madame Cianfarani: est-ce que le Canada en fait assez au niveau postsecondaire pour offrir une formation axée sur ces besoins futurs? Vous avez parlé du modèle britannique, et justement, du point de vue du partage de personnel, qui fait ainsi la navette, en faisons-nous assez au sein des collèges et des universités pour veiller à ce que, à l'avenir, nous ayons les personnes pour concrètement concevoir ces systèmes et travailler au sein de ceux-ci? Que pourrions-nous faire pour améliorer les choses?

Mme Christyn Cianfarani: C'est difficile, parce que je déborde un peu de mon cadre ici. Je ne suis plus vraiment dans un modèle universitaire ni à l'école secondaire, mais je crois que, partout au pays, nous comprenons qu'il y a pénurie de talent. Nous comprenons également, il me semble, que nous avons quelques réserves à offrir directement des incitatifs pour favoriser certaines catégories d'études ou certains secteurs où nous voulons développer les talents dont nous avons besoin, ce qui veut dire que nous ne faisons essentiellement rien comme de dire aux étudiants qu'ils peuvent obtenir une plus grosse bourse d'études s'ils se dirigent dans un domaine en particulier. Nous voulons inciter tous les Canadiens à avoir un accès égal à l'éducation, à l'éducation postsecondaire, à l'éducation universitaire, et nous n'indiquons pas très clairement dans quelles filières nous souhaitons que cette éducation ait lieu afin de pouvoir développer les talents pour l'avenir.

Je crois que nous pourrions faire plus comme nation en matière de programmes d'incitatifs, possiblement en orientant l'éducation et les talents vers un éventail de possibilités, si vous voulez, pour créer une nouvelle génération dans les domaines qui, selon nous, sont cruciaux pour le pays, mais, pour cela, il faut établir les priorités nationales quant aux domaines où l'on veut faire émerger le talent.

Le président: Merci, madame Mathyssen.

Monsieur Bezan, vous avez cinq minutes.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président.

Merci aux témoins d'être des nôtres. Je suis heureux de revoir Mme Cianfarani.

J'aimerais poursuivre dans la lignée de ce que Mme Mathyssen vient de dire. Vous avez parlé de la difficulté pour les gens d'obtenir une autorisation de sécurité nationale et une cote de sécurité de niveau très secret. Quand il y a pénurie de main-d'œuvre, cela devient encore plus difficile. Nous avons actuellement des discussions sur le projet de loi C-26 et le Conseil canadien des affaires affirme qu'il manque 26 000 personnes dans le secteur de la cybersécurité en ce moment même. Il y a beaucoup de postes vacants.

Mis à part essayer d'obtenir plus de main-d'œuvre ici par l'intermédiaire de notre réseau de l'éducation, serait-il approprié d'employer des ressortissants étrangers qui viennent des pays partenaires du Groupe des cinq et qui ont été approuvés dans le cadre de leur processus?

● (0940)

Mme Christyn Cianfarani: Vous devriez à mon avis procéder aux vérifications de diligence raisonnable qui s'imposent pour confirmer qu'ils peuvent être des partenaires de confiance. D'abord, avant de s'aventurer dans cette voie, je soulignerais que beaucoup d'anciens combattants qui ont une autorisation de sécurité quittent la Défense nationale et les organismes de sécurité et, le jour où ils passent le pas de la porte, ils perdent cette autorisation et doivent attendre deux ans ou un an et demi pour la récupérer.

Peut-être pourrait-on avant toute chose regarder à l'interne et accélérer les processus et éliminer les obstacles présents. Ensuite, oui, il pourrait tout à fait être possible de se tourner vers des personnes provenant de nos partenaires du Groupe des cinq plus particulièrement pour obtenir la compétence et le talent nécessaires dans notre pays.

M. James Bezan: J'adore cette idée. Nous devons absolument donner cette possibilité à nos vétérans lorsqu'ils quittent les Forces armées canadiennes. Je suis d'accord avec vous pour dire que c'est pour eux l'endroit idéal pour amorcer leur nouvelle vie publique en tant que simples citoyens, nommément dans le cybermonde — en contexte industriel —, dans les entreprises de télécommunications, mais aussi dans les industries du domaine de la défense.

Vous avez parlé d'une approche holistique et d'une cybersécurité collective. Par le passé, des sources américaines nous ont raconté que certaines technologies ont été percées lorsque des fournisseurs tiers ont été piratés — des fournisseurs qui auraient pu avoir accès à des schémas pour des choses comme les F-35 ou les missiles de croisière —, et que les renseignements ainsi obtenus ont ensuite été disséminés à l'échelle mondiale par nos adversaires.

Le gouvernement du Canada a-t-il pris suffisamment au sérieux ce type de défense collective pour s'assurer de fournir un système aussi sûr que possible à tout le monde — depuis le lieu de travail du gouvernement et de l'entrepreneur principal jusqu'aux sous-traitants et à tous les employés —, et que nous faisons tout en notre possible pour protéger ces renseignements?

Mme Christyn Cianfarani: Je pense, comme nous l'avons dit, que nous avons été assez lents à le faire. Il est certain que les organismes et même, dans une certaine mesure, la Défense nationale... Notre approche cloisonnée signifie que nous nous occupons de nous-mêmes. Les organismes s'occupent du gouvernement. Les FAC s'occupent des FAC, et l'industrie s'occupe d'elle-même. Ce que nous constatons, c'est que l'approche que nous utilisons ne fonctionne pas.

Si nous voulons sécuriser les chaînes d'approvisionnement à partir du plus petit dénominateur commun — et c'est là que se produisent la plupart des intrusions, parce que le chaînon le plus vulnérable est la petite entreprise ou le petit fournisseur qui n'a pas forcément l'équipement ou les compétences nécessaires pour assurer le niveau de cybersécurité requis —, nous devons créer ces institutions, ces organismes ou les sensibiliser afin de les amener à se soucier davantage de la cybernétique et à se munir des protections adéquates. Nous devons mettre ces protections à leur disposition. Nous devons aider ces entreprises à se protéger et les inciter à prendre les moyens nécessaires en ce sens. L'incitation peut prendre la forme du bâton et de la carotte. Par exemple, elles pourraient être informées que si elles veulent faire des affaires avec le gouvernement canadien, si elles veulent faire des affaires qui touchent aux chaînes d'approvisionnement, elles doivent obtenir leur certification CMMC.

Pour nous améliorer en la matière, nous devons imposer des règles aux entreprises, avec la contrepartie suivante: « Une fois que vous êtes à l'intérieur, c'est pour de bon. »

M. James Bezan: Combien de fournisseurs canadiens de cybersécurité, tant du côté des services que du côté de l'infrastructure, sont actuellement concurrentiels sur la scène mondiale? Vous avez mentionné que nous maîtrisons bien le cryptage et la pénétration. Quelles sont nos autres forces? Y a-t-il des choses qui sont prisées par nos partenaires, en particulier au sein du NORAD, mais aussi, bien entendu, au sein du Groupe des cinq?

Le président: Répondez très brièvement, s'il vous plaît.

Mme Christyn Cianfarani: Comme je l'ai dit, environ 25 % de l'industrie... et 60 % de ce chiffre concerne l'assurance de la mission, soit 60 % de 25 %. Ne me demandez pas de faire des maths, parce que j'ai étudié l'anglais, mais cette partie est activement engagée dans les contrats gouvernementaux de nos partenaires du Groupe des cinq.

Le président: Merci, monsieur Bezan.

Monsieur Fisher, vous avez les cinq dernières minutes.

M. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Merci, monsieur le président.

Je remercie nos témoins d'être ici aujourd'hui.

Nous avons examiné les risques de cybersécurité pour les infrastructures essentielles dans le contexte de la cyberguerre et des menaces pour la défense et la sécurité du Canada. L'industrie manufacturière fait partie des 10 infrastructures essentielles recensées par Sécurité publique Canada.

Monsieur Callan, en quoi la fabrication en matière de défense représente-t-elle une cible pour les tentatives de cyberintrusions soutenues par des États étrangers?

● (0945)

M. Tim Callan: Absolument. La fabrication en matière de défense est essentielle aux infrastructures de la défense, et si vous pouvez empoisonner ces processus, vous pouvez lui nuire. En outre, vous pouvez voler des secrets. Le vol de secrets est un problème de taille. Il y a beaucoup à gagner à cet égard, et les gains touchent au long terme. Les secrets percés concernent les plans pour l'avenir et la capacité d'approvisionnement existante. Toutes ces choses sont des cibles de choix pour ce que nous appelons les « menaces sophistiquées et persistantes »: un acteur parrainé par un État, quelqu'un qui pourrait vouloir nuire au Canada. Nous pouvons imaginer de qui il s'agit.

Dans la mesure où le gouvernement est une cible, il l'est, mais les entreprises, les entrepreneurs privés qui fournissent le gouvernement peuvent également être des cibles, et c'est une autre façon pour les acteurs parrainés par des États autres d'obtenir les renseignements qu'ils tentent de se procurer.

M. Darren Fisher: Pouvez-vous me donner quelques exemples de la manière dont l'industrie travaille ou prévoit de travailler à l'atténuation de ce risque?

M. Tim Callan: Il y a un grand nombre de stratégies et de technologies qui sont nécessaires. L'une des choses à comprendre, c'est qu'il faut vraiment construire une forteresse de sécurité, et que toute entrée est une entrée. Il faut donc rechercher une couverture complète, alors que l'attaquant n'a qu'à trouver une faille, un trou ou une vulnérabilité. Comme nous l'avons dit, il peut s'agir d'attaques par piratage psychologique. Il peut s'agir d'un cryptage inadéquat. Il peut s'agir de pare-feu ou de protections de messagerie qui ne sont pas tout à fait au point.

C'est très complexe. Des professionnels consacrent leur vie entière à comprendre ces activités et à se tenir au courant des avancées dans ce domaine. Il y a des départements entiers qui se concentrent là-dessus, et il faut qu'il y en ait.

M. Darren Fisher: Madame Cianfarani, soyez la bienvenue.

Vous avez dit que la cybersécurité est un « sport d'équipe ». Je suis un grand défenseur des partenariats. Je suis un fervent partisan de la collaboration. Vous en avez un peu parlé, mais vous pourriez peut-être y mettre la touche finale: de quelles façons les entreprises canadiennes de cybersécurité, les partenaires traditionnels de l'industrie de la défense et le gouvernement pourraient-ils travailler ensemble pour mieux protéger la fabrication et nos chaînes d'approvisionnement?

Mme Christyn Cianfarani: Comme nous l'avons dit, 85 % des infrastructures névralgiques de ce pays sont en fait détenues et exploitées par le secteur privé, et nous avons donc un rôle très important à jouer pour ce qui est de sécuriser nos propres infrastructures afin d'assurer la sécurité de tous.

Deuxièmement, nos organismes disposent de talents et de savoir-faire, et nous misons constamment sur le développement et l'innovation afin d'apporter ces compétences aux organismes et de maintenir ces derniers au courant de ce qui fait de plus pointu pour protéger le Canada et la société canadienne. C'est cet échange collaboratif qui nous permet de nous améliorer en tant que nation, pour peu que nous soyons disposés à nous ouvrir un peu les uns aux autres.

M. Darren Fisher: Vous avez abordé beaucoup de choses dans vos cinq minutes liminaires. Vous avez parlé de la norme de cybersécurité, de la norme mondiale ou de la nécessité d'une norme mondiale...

Mme Christyn Cianfarani: Oui, c'est la CMMC.

M. Darren Fisher: C'est exact.

Mme Normandin en a parlé un peu, je crois. Le Canada envisage-t-il d'adhérer à une norme mondiale ou de suivre la norme américaine? Est-ce que c'est ce que vous suggérez que nous fassions?

Mme Christyn Cianfarani: Ils étudient la norme américaine, qui est en train de devenir une norme. Elle nous sera imposée. Dans un avenir plus ou moins proche, elle sera imposée à tous ceux qui voudront obtenir une part des contrats du ministère de la Défense. Nous l'envisageons sous l'angle de... Nous faisons partie de cette chaîne d'approvisionnement, alors nous allons devoir l'utiliser de toute façon. Nous devrons nous assurer que l'industrie est en phase avec cette norme et qu'elle l'a adoptée.

Deuxièmement, voulons-nous adopter cette norme au Canada et faire en sorte que la Défense nationale, par exemple, puisse l'évoquer lors de ses propres achats de produits et de services? Doit-il s'agir d'une « norme par renvoi », c'est-à-dire une reproduction exacte de ce qu'ont les Américains, ou devons-nous y ajouter quelque chose de particulier au Canada?

M. Darren Fisher: Je vous remercie.

Le président: Merci, monsieur Fisher.

Avant de suspendre la séance, j'aimerais obtenir quelques éclaircissements sur ce que vous avez dit concernant la déclassification. J'ai eu le privilège d'être informé de choses secrètes et il m'est arrivé de me demander si je ne les avais pas déjà lues quelque part dans le *Globe and Mail*. Il me semble que nous avons une vision excessivement prudente de ce qui constitue une information classifiée. Je ne sais pas si vous avez beaucoup réfléchi à la question, mais j'aimerais que vous me disiez, en 30 secondes, où en sont vos réflexions sur le sujet.

● (0950)

Mme Christyn Cianfarani: Je n'ai pas approfondi la question, mais je suis d'accord avec vous. Je pense que la classification des choses a d'abord été un moyen pour les personnes possédant ces renseignements de détenir quelque chose qui a de la valeur. Lorsqu'ils transfèrent cette valeur, ils doivent se demander: « Qu'est-ce que j'apporte à la table? »

Au Canada, nous craignons également ce que les gens feront de ces renseignements et le fait que ces derniers pourraient être utilisés contre nous. Je pense que les Canadiens, de même que nos institutions gouvernementales, sont par nature un peu plus réticents à prendre des risques que nos alliés. Cela vient peut-être du fait que nous n'avons pas souvent l'impression d'être dans des situations épineuses où nous devons prendre des risques.

Je pense qu'il s'agit d'un modèle qui se perpétue de lui-même et qui ne nous permet pas d'aller aussi loin qu'il le faudrait. Je crois qu'une réflexion s'impose. Avons-nous besoin de classifier toutes les choses que nous classifions? Un plus grand nombre de personnes peuvent-elles avoir accès à l'information, et devrions-nous permettre la déclassification d'une plus grande quantité de renseignements pour faire en sorte que les Canadiens deviennent plus lucides, plus efficaces et plus nuancés face à ce qui se passe? Il ne s'agit pas de nous effrayer, mais de nous éduquer.

Le président: Vous présentez bien la chose. Nous connaissons un climat de menaces très différent de ce à quoi nous sommes habitués, même en ne considérant que les 12 derniers mois. Je serais curieux de savoir comment votre point de vue évoluera avec le temps.

Madame Cianfarani et monsieur Callan, je vous remercie d'avoir accepté de venir devant le Comité. Vous nous avez tous deux fait part de vos réflexions, et sachez qu'elles alimenteront nos études.

Sur ce, nous allons suspendre la séance et passer au groupe d'experts suivant dès que le professeur Leuprecht sera disponible.

● (0950)

_____(Pause)_____

● (1000)

Le président: Très bien, distingués collègues, nous avons résolu tous les problèmes techniques qui devaient l'être. Le professeur Leuprecht est en ligne.

Il devrait normalement faire une déclaration liminaire de cinq minutes, mais étant donné son talent et les contraintes de temps, je vais lui demander d'être aussi condensé que possible à l'intérieur du temps qui lui est imparti.

[*Français*]

M. Christian Leuprecht (professeur, Collège militaire royal du Canada, à titre personnel): Merci, monsieur le président.

Je vais faire mon discours en anglais. Toutefois, c'est avec plaisir que je répondrai à vos questions en anglais ou en français.

[*Traduction*]

La déclaration vous a été distribuée à l'avance, je vais donc en sauter certaines parties.

Le Belfer Center Cyber Power Index, le CPI, de l'Université Harvard classe le Canada au 8e rang des cyberpuissances mondiales. Le CPI caractérise le Canada comme une cyberpuissance à forte intention et à faible capacité, dotée d'atouts notables en matière de cyberdéfense, d'initiatives d'élaboration de normes cybernétiques et de surveillance. En revanche, l'intention et la capacité du Canada à mener des opérations de renseignement étranger et des offensives cybernétiques le placent au milieu du peloton du CPI, derrière la Russie et la Chine et ses partenaires du Groupe des cinq — en particulier les États-Unis et le Royaume-Uni —, les Pays-Bas et Israël. L'évaluation du Canada par le CPI porte sur deux décennies d'initiatives canadiennes en matière de cybersécurité. Le classement montre par ailleurs que le Canada souffre d'un déficit stratégique sur le plan cybernétique.

Depuis 20 ans, la cyberdiplomatie a échoué à susciter une entente sur les normes internationales visant à limiter les comportements malveillants des acteurs étatiques ou tolérés par les États dans le cyberespace. Pour dissuader et limiter les mauvais comportements, les États occidentaux doivent intervenir en recourant à des cybermesures actives et offensives. C'est ce que la doctrine américaine d'engagement persistant s'efforce de faire depuis 2018. Toutefois, aucun allié des États-Unis n'est en mesure d'égaler les ressources et les capacités américaines.

En 2019, l'adoption du projet de loi C-59 a donné du poids au rôle et à l'incidence qu'avait le Canada dans le cyberespace en autorisant le Centre de la sécurité des télécommunications, le CST, à mener des cyberopérations offensives. L'ajout de ces capacités au mandat du CST a été salué comme une étape très importante. En théorie, la combinaison de mandats de renseignement étranger, de cyberopérations actives et de cyberopérations défensives permet l'éventail complet des opérations de cyberespionnage, de sabotage et de subversion. Le Canada a maintenant la capacité de faire preuve d'un leadership international indépendant pour réduire l'instabilité et l'incertitude dans le cyberespace, mais la volonté politique n'est pas au rendez-vous.

Je propose une « cyberdoctrine » d'engagement fonctionnel pour renforcer les cybernormes tacitement acceptées. L'utilisation assidue des cybercapacités est le moyen le plus efficace pour le Canada de réduire l'incertitude dans le cyberespace et de limiter les menaces qui pèsent sur ses intérêts nationaux.

En raison des contraintes de ressources du Canada et de ses ambitions limitées en matière de politique étrangère, l'engagement fonctionnel prescrit que le pays emploie toute la gamme de ses cybercapacités pour établir et renforcer un ensemble limité de points focaux clairement définis et communiqués afin de dissuader et de limiter les comportements inacceptables.

Au lieu d'utiliser continuellement et à l'échelle mondiale des cybercapacités pour modifier l'équilibre global des forces dans le système international, l'engagement fonctionnel demande au Canada d'employer ses cybercapacités de manière plus étroite, dans des cas précis lorsqu'un cyberacteur malveillant mène une activité délétère à l'endroit des choses qui nous sont chères. On pense, par exemple, à des activités qui mineraient directement la souveraineté du Canada et la sécurité de son peuple, dégraderaient ou subvertiraient le droit international et l'intégrité des institutions internationales, électorales ou démocratiques, ou porteraient atteinte à la sécurité économique, à la compétitivité et à la prospérité du Canada.

La cyberdoctrine d'engagement fonctionnel proposée vise à façonner le comportement nuisible de manière cumulative en renforçant les cybernormes tacitement acceptées dans le cadre des ressources limitées et du caractère particulier du leadership traditionnel que le Canada exerce en tant que puissance moyenne à l'égard de ses créneaux de politique étrangère.

[*Français*]

Je vous remercie de votre attention.

● (1005)

[*Traduction*]

Le président: Merci, professeur Leuprecht.

Madame Gallant, vous avez six minutes. Nous vous écoutons.

Mme Cheryl Gallant: Merci, monsieur le président.

Le Service canadien du renseignement de sécurité a identifié les villes dites intelligentes comme des menaces émergentes, en particulier pour la diaspora de la République populaire de Chine. Comment ces villes peuvent-elles mettre en danger notre défense nationale?

M. Christian Leuprecht: Le principe des villes intelligentes est leur interconnexion et leur capacité de suivre à la fois le contenu et les connexions des personnes qui y vivent.

Ce problème est similaire à celui que pose, par exemple, TikTok sur le plan microéconomique. Un acteur adverse peut apprendre beaucoup de choses sur les gens, même s'il ne peut pas lire le contenu qu'ils publient. Il s'agit de comprendre les liens qui relient les différentes notes, c'est-à-dire de savoir à quelle fréquence vous, madame Gallant, communiquez avec quelqu'un d'autre dans votre réseau. En outre, la capacité d'extraire ces données permettrait à un acteur apte à les décrypter — par des mesures quantiques ou plus élémentaires — de dresser un tableau très complet de votre comportement et de déployer des campagnes de désinformation délibérément et intentionnellement ciblées sur votre comportement particulier. En procédant de la sorte, il pourrait, par exemple, influencer votre comportement actuel, mais aussi collecter ces données sur plusieurs années pour influencer votre comportement futur.

C'est là le problème avec TikTok. Il s'agit pour les acteurs adverses d'influencer la génération actuelle et de conserver des données sur ces personnes afin d'être en mesure d'intervenir sur leur comportement une fois qu'elles seront en âge de voter.

Mme Cheryl Gallant: Un entrepreneur de Construction de Défense Canada a récemment été victime d'une attaque par rançongiciel. Le cas échéant, quel en serait l'effet sur notre défense nationale? Y a-t-il des mesures que nous devrions prendre pour mieux protéger nos organisations de défense et de sécurité?

M. Christian Leuprecht: Eh bien, madame Gallant, j'ignore quelle voiture vous conduisez. Moi, je conduis une mini-fourgonnette. Elle a une douzaine d'années. Voilà à quoi ressemblent la plupart des réseaux au sein du gouvernement du Canada: c'est un peu comme conduire une vieille voiture. Nous roulons sur une vieille infrastructure dans laquelle le gouvernement n'a pas suffisamment investi.

Voilà le volet cybersécurité du défi que nous devons relever. L'autre volet concerne le cyberdomaine, c'est-à-dire les comportements risqués des personnes qui cliquent sur des liens — comme c'était probablement le cas dans ce contrat de Construction de Défense Canada — et qui finissent par divulguer par inadvertance des renseignements ou par rendre les réseaux vulnérables.

Dans la première partie de la réunion, vous avez parlé de la classification. Au Canada, nous avons tendance à surclassifier constamment et abondamment les documents: 90 % des documents que nous classifions n'ont probablement pas besoin de l'être. Les 10 % restants doivent être protégés à tout prix. À l'heure actuelle, nous effectuons une classification beaucoup trop vaste, au lieu de cibler notre protection, nos ressources pour nous assurer que les éléments qui ne doivent jamais être divulgués sont bel et bien protégés. Les discussions récentes sur les fuites montrent que nous avons certes encore beaucoup de travail à faire.

● (1010)

Mme Cheryl Gallant: Plus tôt dans la journée, nous avons appris que des plans et des messages technologiques cryptés pourraient avoir été volés à notre insu. À un moment donné dans l'avenir, lorsque l'informatique quantique sera disponible, le tout pourrait être décrypté. Des technologies et des plans secrets pourraient ainsi être dévoilés, notamment en ce qui concerne notre technologie des missiles, etc.

Que devrions-nous faire dans l'immédiat, et quelles mesures devrions-nous prendre entretemps pour protéger les données de nature délicate? Que pouvons-nous faire aujourd'hui pour que, le jour où ces réalités quantiques se concrétiseront, les vulnérabilités ne soient pas aussi exposées et pour que nous soyons mieux protégés dans l'ensemble?

M. Christian Leuprecht: C'est une très bonne question, madame Gallant, parce qu'on peut imaginer qu'un [*difficultés techniques*] hostile qui utilise un système de crédit social pour ses 1,4 milliard d'habitants aurait la capacité d'étendre ce système au reste de la population mondiale. Si j'avais à parier, je dirais que ce pays a déjà établi un profil assez sophistiqué de votre identité, ainsi que de vos communications numériques et de vos données.

Je pense qu'il est essentiel, comme vous le dites précisément, que nous réfléchissions très attentivement, par exemple, au type de données que nous risquons de divulguer par inadvertance. Tout récemment, l'Australie a décidé de retirer des dizaines de milliers de produits fabriqués en Chine des édifices et des réseaux gouvernementaux en raison des préoccupations liées aux capacités de surveillance qui pourraient s'y rattacher.

Il ne fait aucun doute que la technologie quantique constituera une avancée considérable. Ce n'est pas mon domaine d'expertise, mais à ma connaissance, ce sera un peu comme Big Blue. Nous n'allons pas disposer de cette capacité du jour au lendemain. Il y aura une sorte de transition, mais c'est certainement un avenir auquel nous devons nous préparer, car les mesures et les mécanismes de cryptage dont nous disposons aujourd'hui ne nous protégeront pas à l'avenir.

Le président: Merci, madame Gallant.

Avant de céder la parole à Mme Lambropoulos, professeur Leuprecht, pourriez-vous déplacer votre micro? Je vous remercie.

Allez-y, madame Lambropoulos.

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

J'aimerais vous remercier, professeur, d'être des nôtres aujourd'hui pour répondre à certaines de nos questions.

Tout d'abord, à quoi ressemble actuellement le régime international de cybergouvernance en ce qui concerne les lois et les normes internationales régissant le comportement des États? Vous avez mentionné dans votre déclaration liminaire qu'aucun autre pays n'arrive à la cheville des États-Unis pour ce qui est de la capacité à prendre des cybermesures offensives, et vous avez également dit que le Canada a la capacité nécessaire grâce au projet de loi C-59, mais que nous n'avons pas nécessairement la volonté politique.

Je me demande si vous pouvez nous dire, de votre point de vue, ce que le Canada peut faire, de concert avec ses alliés, pour renforcer cet ordre international fondé sur des règles dans le cyberdomaine.

M. Christian Leuprecht: C'est une excellente question. Cela fait 20 ans que nous essayons d'établir des normes et de dégager un consensus à ce sujet, mais nous n'avons guère progressé au sein des Nations unies et d'autres organismes.

Ce qu'il faut comprendre, c'est qu'il y a des gens qui croient en l'ordre international libéral fondé sur des règles — c'est-à-dire environ 57 pays —, puis il y a des pays qui sont agnostiques, mais il y a aussi un sous-ensemble de pays qui ne souscrivent tout simplement pas à cet ordre. Par conséquent, nous n'aurons jamais de régime international de cybergouvernance, du moins pas dans un avenir prévisible, mais nous pouvons forcer les acteurs hostiles [*difficultés techniques*]. Nous pouvons les dissuader de mal agir s'ils savent que les États-Unis et leurs alliés fixent des limites clairement définies, de sorte que tout manquement aura de graves répercussions sur l'acteur concerné, que ce soit dans le cyberespace ou dans le contexte cinétique, par l'entremise de sanctions ou par d'autres moyens. Dans ma déclaration liminaire, j'ai expliqué précisément en quoi consiste un tel mécanisme.

Toutefois, le gouvernement du Canada s'est montré extrêmement réticent à utiliser les pouvoirs conférés au Centre de la sécurité des télécommunications aux termes du projet de loi C-59, après l'obtention de la sanction royale. Le problème est donc le suivant: quel est l'intérêt d'accorder ces pouvoirs si nous ne les utilisons pas pour défendre nos intérêts? Le Canada s'est toujours enorgueilli d'être un pays qui établit et fait respecter des normes et des règles internationales, mais en matière de cyberespace, nous faisons exactement le contraire en refusant de nous servir de ces pouvoirs.

Maintenant que nous disposons de tels pouvoirs, nous devons également nous en prévaloir pour défendre nos intérêts et ceux de nos alliés. La raison pour laquelle nous devons y recourir, c'est que l'État a un rôle très particulier à jouer dans ce domaine, car les acteurs du secteur privé et d'autres acteurs du secteur public ne disposent pas de capacités actives et offensives. Seul l'État peut déployer ces capacités; par conséquent, seul l'État peut agir de façon proactive en interdisant ou, au besoin, dans le cyberespace, en sabotant les capacités des acteurs malveillants émanant d'un État ou tolérés par un État.

● (1015)

Le président: Je vous remercie.

Permettez-moi d'intervenir vite fait. Monsieur Leuprecht, pourriez-vous désactiver votre micro entre vos prises de parole? Je comprends que cela puisse être un peu difficile, mais si vous pouviez le faire, cela contribuerait à la qualité de la transmission.

Madame Lambropoulos, allez-y.

Mme Emmanuella Lambropoulos: Je vous remercie.

Je vous sais gré de votre réponse. Comme je ne connais pas très bien le projet de loi C-59, je me demande si vous pouvez nous dire s'il comporte actuellement des lacunes qui créent une différence, disons, entre nos capacités et celles des États-Unis. Si on devait le renforcer à l'avenir en cas de nécessité, de quelles façons pourrait-on s'y prendre?

M. Christian Leuprecht: Il ne s'agit pas de renforcer le projet de loi. Il s'agit plutôt de nous assurer que nous utilisons efficacement les capacités dont nous disposons. Les États-Unis disposent de vastes capacités qu'ils utilisent régulièrement, en partie pour empêcher un changement dans l'équilibre international des pouvoirs. Ce n'est pas l'objectif principal du Canada, bien que notre pays vise intrinsèquement à maintenir le statu quo.

Dans le dernier paragraphe de mon mémoire concernant le Canada, [*difficultés techniques*] définit clairement trois points focaux de comportements inacceptables que le Canada ne tolérera pas et pour lesquels les adversaires sauront que le Canada déploiera, seul ou avec ses alliés, les mesures actives ou offensives prévues dans le projet de loi C-59. Le problème, c'est que le Canada n'a pas voulu, dans l'ensemble, prendre part à ce genre d'exercices, à l'exception de quelques opérations de dépistage en ce qui concerne, par exemple, l'Ukraine.

Le Canada doit faire preuve d'un peu plus d'audace dans la manière dont il utilise les pouvoirs qui ont été accordés aux organismes pour défendre les intérêts canadiens.

Mme Emmanuella Lambropoulos: Diriez-vous qu'il y a un avantage à agir rapidement, avant que quelque chose d'important ne se produise? Est-ce que nous perdons une partie de notre capacité à répondre à une menace si nous attendons plus longtemps?

M. Christian Leuprecht: C'est une question formidable, qui touche vraiment le nœud du problème.

L'ennui avec les processus actuels de prise de décision politique — peu importe le gouvernement du pays —, c'est que, depuis des années, nous tergiversons trop longtemps avant de prendre des décisions clés dans des dossiers où nous devons assurer une autorité, une autorisation et une orientation politiques. Plus nous attendons, plus notre marge de manœuvre se réduit et moins nous avons d'options dans notre boîte à outils. Nous avons besoin de processus décisionnels plus agiles, et il nous faut aussi des processus décisionnels politiques plus rapides afin de maximiser les options politiques mises à la disposition du gouvernement et les instruments en matière d'opérations pour obtenir l'effet voulu par le gouvernement.

● (1020)

Le président: Merci, madame Lambropoulos.

Madame Normandin, vous avez six minutes.

[*Français*]

Mme Christine Normandin: Merci, professeur Leuprecht.

C'est toujours avec plaisir que nous vous recevons parmi nous.

Vous avez parlé de la cyberdiplomatie en mentionnant que des États s'entendent entre eux, que des États sont un peu plus agnostiques quant à la cyberdiplomatie et que des États sont carrément contre l'ordre global international. Par exemple, la Chine, la Russie, la Corée du Nord et l'Iran sont des acteurs malveillants, mais ils ont chacun leur façon assez indépendante de fonctionner selon des intérêts qui leur sont propres.

Pouvons-nous penser qu'il y a une certaine forme de collaboration entre ces pays présentement?

Pourrait-il se créer deux fronts plutôt que d'avoir un front réunissant les pays alliés et s'attaquant à différents acteurs ayant des vues différentes?

Pourrait-il y avoir une espèce de regroupement des façons de faire concernant les pays malveillants?

M. Christian Leuprecht: C'est une excellente question, madame, parce que cela concerne la culture politique et la culture stratégique de chacun de ces pays.

Par exemple, l'Iran vise de prime abord des fins stratégiques dans la région du Moyen-Orient. L'Iran ne vise pas d'abord le Canada, les États-Unis ou des alliés européens. Un des objectifs principaux de la Corée du Nord, c'est de voler de vastes sommes d'argent afin de financer ses activités malveillantes. La Russie a des capacités à l'échelle mondiale. Ce qui différencie la Chine et la Russie d'autres pays, c'est l'envergure des capacités et une patience stratégique pour développer ces capacités afin d'optimiser certains objectifs.

Par exemple, vous vous souvenez peut-être de l'infiltration informatique des systèmes de l'entreprise SolarWinds, il y a à peu près 18 mois ou deux ans. Il s'agissait d'une tentative de cyberattaque qui a pris probablement de 12 à 18 mois à planifier. Cela a probablement nécessité un millier de personnes pour réunir toutes les pièces nécessaires. Ces acteurs ont des capacités très différentes des autres États. Par conséquent, il faut prendre des mesures actives et offensives pour les dissuader de prendre des moyens qui vont à l'encontre de nos intérêts.

Mme Christine Normandin: Comme ces acteurs sont particulièrement différents l'un de l'autre, nous ne pouvons pas nous attendre à ce qu'il y ait nécessairement de la collaboration entre eux. Ce n'est pas quelque chose à considérer à court ou à moyen terme.

Est-ce bien cela?

M. Christian Leuprecht: Il y a toujours de la collaboration pour des raisons tactiques, c'est-à-dire pour remettre en cause l'ordre politique international, qui, selon la Russie et la Chine, ne sert pas leurs intérêts.

Les régimes autoritaires ne se font pas tellement confiance les uns envers les autres. C'est pourquoi je ne m'inquiète pas trop de cette collaboration à long terme, en particulier du côté de la Chine, car elle a les capacités voulues pour agir toute seule et favoriser ses intérêts malveillants.

Mme Christine Normandin: Merci beaucoup.

De notre côté, nous travaillons beaucoup en collaboration avec d'autres pays. Cela ne comporte-t-il pas le risque que nous devenions un peu dépendants d'eux? Pourquoi ne pas bâtir notre propre expertise?

À long terme, n'y a-t-il pas un danger, soit de ne pas être capables d'agir de façon autonome à force de travailler trop en collaboration avec d'autres pays alliés?

M. Christian Leuprecht: Madame Normandin, ce n'est pas un risque, c'est une réalité. C'est ce qui se passe.

Aujourd'hui, le Canada n'a pas les capacités nécessaires dans plusieurs domaines pour être pris au sérieux par les autres partenaires du Groupe des cinq, en particulier les États-Unis, le Royaume-Uni et l'Australie. Par conséquent, le Canada est exclu de certaines mesures de collaboration dans le domaine cinétique et dans le domaine de la cybersécurité. Cela réduit la capacité du Canada de veiller à ses intérêts à l'échelle mondiale.

Il est donc urgent de faire des investissements afin de développer et d'élargir les capacités étatiques dans le domaine de la cybersécurité.

● (1025)

Mme Christine Normandin: Merci beaucoup.

Au Québec, il y a un ministère de la Cybersécurité et du Numérique, qui est soutenu par un groupe de conseillers. J'aimerais savoir si l'équivalent existe au fédéral.

Y a-t-il des groupes de conseillers en cybersécurité qui soutiennent le travail des ministres que cela touche? Je pense principalement au ministre responsable de la défense nationale.

Si cette façon de faire n'existe pas, cela devrait-il être rapidement mis en place?

M. Christian Leuprecht: J'ai eu le plaisir d'avoir certaines interactions avec l'équipe du Québec, et je trouve très intéressants les efforts déployés par la province dans ces domaines. Le gouvernement fédéral pourrait apprendre plusieurs choses du Québec.

Le gouvernement fédéral a certainement des capacités plus importantes que celles de n'importe quelle province. Je crois qu'il pourrait y avoir beaucoup plus de collaboration intergouvernementale, comme c'est le cas en Australie, où l'Australian Signals Directorate, l'équivalent du Centre de la sécurité des télécommunications au Canada, ou CST, a des bureaux dans chacun des États australiens.

Il me semble aussi que le Canada pourrait être plus actif. Plusieurs pays ont des ambassadeurs de la cybersécurité. Le Danemark a été le premier à créer un tel poste, mais il y a aussi les États-Unis. Nous n'avons pas d'ambassadeur de la cybersécurité, ce qui montre que notre façon de concevoir le domaine de la cybersécurité pourrait être mise à jour.

[*Traduction*]

Le président: Nous allons devoir en rester là.

Merci, madame Normandin.

Vous avez six minutes, madame Mathyssen.

Mme Lindsay Mathyssen: Merci, professeur, de vous joindre de nouveau à nous au sein du Comité.

J'aimerais revenir un peu sur votre conversation avec Mme Gallant. Vous avez parlé en détail de TikTok, des algorithmes qui sont conçus et de leur capacité d'influence, ainsi que de l'exploitation de ce type de renseignements. Diriez-vous que cela existe sur toutes les plateformes de médias sociaux, qu'il s'agisse de Facebook, de Google ou de tout autre réseau?

M. Christian Leuprecht: Madame Mathyssen, j'ai écrit un livre sur ce sujet, intitulé *Intelligence as Democratic Statecraft*. C'est une excellente question.

Il y a des différences considérables. Pendant des années, j'ai averti les Canadiens, alors qu'ils se souciaient beaucoup de la surveillance exercée par l'État canadien, qu'ils devraient peut-être s'inquiéter davantage de la surveillance exercée par les entreprises du secteur privé que de celle exercée par l'État canadien. Il existe des garanties considérables, des processus de reddition de comptes et de transparence pour la surveillance de l'État, mais de telles mesures ne sont pas en place pour le secteur privé.

Dans le cas de TikTok, bien entendu, on parle d'un pays qui non seulement ne dispose d'aucune garantie pour la surveillance de l'État ou du secteur privé, mais qui a activement, encore tout récemment, renforcé ses lois pour obliger les entreprises du secteur privé à échanger des données sans aucune sorte d'autorisation légale ou judiciaire, simplement à la demande du gouvernement. De plus, la présence du parti communiste chinois a été renforcée dans toutes les entreprises chinoises.

En Chine, il n'est pas possible de faire la distinction entre le secteur privé et le secteur public comme on le ferait, par exemple, en Amérique du Nord. Dire que le risque est le même dans le secteur privé serait une méconnaissance fondamentale de l'écosystème dans lequel évoluent les entreprises du secteur privé en Chine et de leur relation avec le régime chinois.

Mme Lindsay Mathyssen: Je comprends parfaitement ce point de vue. Il s'agit plutôt des plateformes de médias sociaux en général et de leur appartenance au secteur privé. En fin de compte, elles ont un objectif précis que tout gouvernement doit surveiller.

Comment le gouvernement du Canada peut-il mieux élaborer des lois pour protéger les gens contre un grand nombre d'algorithmes, que ceux-ci visent à exploiter des secrets, à faire de l'argent ou à manipuler les gens? Il est certain que les gens peuvent s'enfoncer dans un trou de lapin sur Facebook à cause de la désinformation et de la mésinformation.

● (1030)

M. Christian Leuprecht: Facebook est un excellent exemple, madame Mathyssen. Regardez l'enquête conjointe menée par le commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et son pendant fédéral. Le problème, c'est que le gouvernement fédéral ne dispose actuellement que d'outils très limités pour appliquer des mesures à l'encontre des entreprises qui ne respectent pas les règles canadiennes.

Je pense que le Comité devrait se poser la question suivante: quelles sont les possibilités qui existent, et que faut-il faire en matière de mesures d'application gouvernementales? De même, quelles mesures d'encouragement, sous forme d'incitatifs fiscaux, de règlements, etc., peuvent permettre au gouvernement d'agir?

D'ici peu, le Conseil des académies canadiennes publiera un rapport sur la sécurité publique à l'ère numérique, qui fournira des mesures très concrètes sur certains de ces sujets.

Mme Lindsay Mathyssen: Je vous remercie.

Je reviens sur ce que vous avez dit à propos de la rationalisation des décisions clés prises par les gouvernements, des inefficacités et de la nécessité de veiller à ce que les gouvernements aient les pouvoirs nécessaires à cet égard. Pourriez-vous également parler du revers de la médaille en ce qui concerne certaines des garanties démocratiques qui existent pour une bonne raison?

L'une des choses qui me préoccupent, c'est qu'en essayant de nous en prendre aux mauvais acteurs étatiques qui nous inquiètent — et vous me direz si je me trompe —, nous risquions de devenir nous-mêmes de tels acteurs.

M. Christian Leuprecht: Je suppose qu'il y a toujours lieu de s'inquiéter de l'intervention de l'État dans ce domaine, surtout lorsqu'il s'agit de contenu.

Il est sans doute possible d'établir des règles plus claires et d'assurer une plus grande transparence pour le secteur privé, et peut-être — comme je l'ai proposé par le passé — de veiller à ce que le gouvernement établisse des mesures de certification volontaire en fonction desquelles les entreprises se comporteraient. Celles-ci peuvent alors obtenir cette certification auprès du gouvernement. En retour, les utilisateurs savent qu'une entreprise prend certaines mesures de cyberprotection ou de cybersécurité, par exemple, qu'elle respecte certaines normes et, en même temps, qu'elle n'utilisera pas les données à d'autres fins que celles prévues par le gouvernement.

Je pense qu'un mécanisme de certification volontaire donnerait beaucoup plus de confiance au consommateur et permettrait au gouvernement d'intervenir sans être [*difficultés techniques*].

Le président: Merci, madame Mathyssen.

Chers collègues, nous avons obtenu une prolongation de 10 minutes. Cependant, nous allons encore manquer de temps. J'aimerais consacrer les cinq dernières minutes au budget pour les déplacements. Cela nous laisse 25 minutes de questions.

M. Bryan May (Cambridge, Lib.): Monsieur le président, je suis désolé, mais un certain nombre d'entre nous devront participer à la période de questions d'ici là.

Le président: On nous a accordé ce temps supplémentaire en raison des difficultés techniques.

Le Comité souhaite-t-il siéger jusqu'à 10 h 55 ou lever la séance à 10 h 45?

M. Bryan May: Pouvons-nous faire un compromis entre les deux, monsieur le président?

Le président: Oui, nous le pouvons. Je n'y vois pas d'inconvénient.

Sommes-nous d'accord pour 10 h 50?

Des députés: D'accord.

Le président: Chers collègues, je vais devoir être assez sévère. Même à trois minutes, je serai très strict.

Sur ce, monsieur Kelly, vous avez trois minutes très courtes.

● (1035)

M. Pat Kelly: Nous avons entendu dire que nos alliés et nos adversaires peuvent déployer de nouvelles capacités en quelques semaines ou quelques mois, alors qu'il nous faut des années ou des décennies. Comment cela nuit-il à la capacité du Canada à utiliser, comme vous l'avez préconisé dans une intervention précédente, les capacités offensives et les pouvoirs existants en matière de cyberdéfense?

M. Christian Leuprecht: C'est ce qui se produit lorsqu'on n'établit pas de stratégie, et surtout lorsque la stratégie n'est pas tournée vers l'avenir. En 2017, des personnes comme moi ont affirmé que le slogan « Protection, sécurité, engagement » était déjà dépassé le jour de sa diffusion. Je pense que cette prémonition s'est avérée juste.

Ce dont nous avons besoin, c'est d'une stratégie bipartisane sur 15 ans pour reconstruire notre défense nationale, notre sécurité et, sans doute, nos capacités de renseignement. Je pense que nous devrions arrêter de faire de la politique et faire ce que font l'Australie et la France. Dans ces pays, tous les partis se réunissent, adoptent une stratégie commune et s'y tiennent. Ainsi, nous ne serions pas constamment à la traîne et nous n'aurions pas à essayer de rattraper notre retard sur un grand nombre de fronts.

M. Pat Kelly: Comment nos goulets d'étranglement en matière d'approvisionnement influent-ils sur notre capacité de gérer cette question?

M. Christian Leuprecht: La passation de marchés pose problème. Ce sont les personnes qui constituent la plus grande difficulté. Le personnel est le principal atout du gouvernement, en particulier dans ce domaine. Il faut beaucoup de temps pour développer ces ensembles de compétences. Elles sont très demandées et le secteur privé s'en empare régulièrement.

Je pense que le Comité ferait bien de réfléchir longuement à ce que le gouvernement peut faire pour garantir le maintien des capacités et les personnes que mes collègues du Collège militaire royal et moi-même, par exemple, avons passé de nombreuses années à développer des ensembles de compétences exceptionnels.

M. Pat Kelly: Vous avez dit que ce que faisait le Canada dans ce domaine revenait à conduire une voiture vieille de 12 ans. C'est une question de personnel et d'approvisionnement. Le problème est généralisé.

M. Christian Leuprecht: Nos capacités sont excellentes, mais elles sont très limitées, en raison de problèmes de personnel, de difficultés liées à l'équipement et à l'approvisionnement des réseaux structurels, ainsi que de défis relatifs à la mise à jour de la politique et de la réglementation. Comme vous pouvez l'imaginer, un organisme de défense nationale qui doit composer avec des lacunes de ce type n'a pas le temps de mettre à jour sa politique et sa réglementation.

Nous faisons face à une multitude de difficultés très diverses qui ne peuvent être résolues en quelques semaines ou quelques mois, ni même en quelques années.

Le président: Merci, monsieur Kelly.

Monsieur May, vous avez trois minutes.

M. Bryan May: Merci, monsieur le président.

Merci, monsieur Leuprecht. Je suis heureux de voir ici aujourd'hui.

Il y a environ un an, au début de l'invasion de l'Ukraine par la Russie, il y avait beaucoup de discussions et de crainte quant à la possibilité que l'Ukraine et les personnes qui la soutenaient soient la cible de cyberattaques de la part de la Russie, mais cela ne s'est pas vraiment concrétisé dans le volume que nous avions prédit, que ce soit pour le Canada ou pour l'Ukraine.

Comment expliquez-vous l'absence apparente de cyberguerre à grande échelle dans la guerre entre la Russie et l'Ukraine?

M. Christian Leuprecht: Je pense que si l'on consulte les rapports de source ouverte de Microsoft, la Russie a déployé ses capacités cybernétiques avec plus d'efficacité qu'on ne le croyait et a intégré ces capacités à des mesures offensives cinétiques sur le champ de bataille. Ce que la Russie a appris en Ukraine, c'est que l'on ne peut pas atteindre des objectifs politiques sur le champ de bataille par l'entremise du cyberespace. Il faut pouvoir agir de façon cinétique. C'est là que la Russie concentre ses ressources.

Cependant, comme l'indiquent les avertissements répétés du Centre de la sécurité des télécommunications, le Canada est exposé à un risque considérable émanant d'acteurs hostiles... non seulement des acteurs étatiques, mais, en particulier dans le cas de la Russie, des acteurs tolérés par l'État. On a mentionné les rançongiciels. Il s'agit d'une source majeure de revenus pour les milices tolérées par l'État, principalement concentrées en Russie.

● (1040)

M. Bryan May: Vous estimez que les efforts de la Russie dans le domaine de la cybernétique ont été efficaces.

M. Christian Leuprecht: Je pense qu'il ne faut pas sous-estimer la Russie, car il n'existe pas vraiment de secteur privé pour les nombreuses personnes hautement qualifiées que la Russie produit dans ce domaine. Elles sont attirées de manière disproportionnée par les acteurs malveillants tolérés par l'État, ainsi que par les services de renseignement, les agences militaires, etc. Certaines de ces personnes ont quitté le pays, mais la Russie dispose de capacités considérables qu'il ne faut pas sous-estimer et que nous ferions mieux de continuer à surveiller de près.

Le président: Merci, monsieur May.

Madame Normandin, vous avez une minute.

[*Français*]

Mme Christine Normandin: Monsieur Leuprecht, vous avez piqué ma curiosité. Je me permets de vous poser une brève question concernant le poste d'ambassadeur de la cybersécurité.

Quelles sont les fonctions de cet ambassadeur et quels seraient les avantages de créer un tel poste?

M. Christian Leuprecht: Il s'agit d'établir des liens avec le secteur privé et les différentes parties prenantes de la planète, qui ne se trouvent pas forcément dans un pays à proprement parler. Le domaine de la cybersécurité se caractérise par une très grande distribution sur le plan géographique, et l'établissement de contacts directs requiert un effort.

L'objectif des ambassades et des ambassadeurs est de fournir au gouvernement des renseignements ouverts. Je dirais que le gouvernement du Canada n'a actuellement pas assez de renseignements ouverts sur les différentes parties prenantes et les acteurs privés dans ce domaine.

Un ambassadeur de la cybersécurité nous permettrait de bâtir des liens avec ces importants joueurs qui, dans plusieurs cas, sont plus puissants que beaucoup de nos partenaires de puissance moyenne.

[*Traduction*]

Le président: Merci.

Madame Mathyssen, vous avez une minute. Allez-y.

Mme Lindsay Mathyssen: Merci.

Monsieur Leuprecht, vous avez parlé des dangers posés par la Chine, de sa relation avec TikTok et de la divulgation de renseignements. J'aimerais que vous nous parliez des Américains, qui disposent de la Foreign Intelligence Surveillance Act et de l'article 702, dont ils discutent actuellement, comme nous l'avons mentionné plus tôt, pour pouvoir obtenir des renseignements auprès de Google, Microsoft, Apple et d'autres entreprises.

Pouvez-vous parler de cette question et nous dire si le Canada est exposé à des dangers? Quelles précautions devons-nous prendre à cet égard?

M. Christian Leuprecht: Il s'agit d'une activité justifiée qui fait l'objet d'une discussion et qui nécessite donc une autorisation en vertu du principe du respect de l'état de droit. Il existe également des garanties quant à l'utilisation ultérieure de ces renseignements.

Les gens ont des avis différents sur la question de savoir si ces autorisations et les lois en place sont acceptables pour eux ou non, et si les mécanismes de contrôle, d'examen, de responsabilisation et de gouvernance sont suffisants. Il s'agit là d'une différence importante par rapport au mode de fonctionnement appliqué par tout acteur autoritaire hostile, en vertu duquel aucune de ces garanties n'est mise en place.

Nous devons nous souvenir que les Américains sont au sommet de la pyramide de la sécurité internationale. Leurs objectifs sont également différents des nôtres en termes d'équilibre des forces. Comme je le dis souvent, les Américains sont nos meilleurs amis, que cela nous plaise ou non.

Le président: Merci.

Monsieur Bezan, vous avez trois minutes.

M. James Bezan: Je ne pensais pas que nous allions consacrer un tour complet à ce sujet.

Tout d'abord, je tiens à remercier le professeur Leuprecht de s'être joint à nous aujourd'hui. Je sais que son expertise dans ce domaine nous a beaucoup aidés.

Nous avons beaucoup parlé du risque que pose le régime de Pékin pour nos médias sociaux et pour le large éventail de services dont nous disposons dans les télécommunications ici au Canada, mais pouvez-vous également parler de la façon dont d'autres organisations criminelles transnationales néfastes ou d'autres pays, comme le régime du Kremlin, nous ont attaqués ou peuvent nous attaquer ici au pays? Comment pouvons-nous être rapidement compromis et comment pouvons-nous sécuriser nos propres vulnérabilités pour que cela ne se produise pas?

● (1045)

M. Christian Leuprecht: C'est une excellente question, monsieur Bezan.

Je pense que le problème fondamental auquel nous sommes confrontés est que nous nous sommes concentrés sur la défense, et tant que vous jouez en défense, par définition, vous ne serez jamais en mesure de marquer et vous ne pourrez donc pas gagner le match. Dans le meilleur des cas, vous pouvez obtenir un match nul. Lorsque vous avez affaire à des acteurs déterminés, malveillants et hostiles comme la Chine et la Russie, il y a de fortes chances qu'ils marquent des points.

C'est l'occasion pour le gouvernement du Canada d'être plus robuste et musclé en démontrant à ces adversaires que certains types de comportements ne seront pas tolérés dans le cyberespace et entraîneront des répercussions, qu'elles soient cybernétiques ou cinétiques.

M. James Bezan: Professeur Leuprecht, ce que nous disons vraiment ici, c'est que nous devons être capables de tirer sur l'archer plutôt que de dévier les flèches. Vous parlez du gouvernement du Canada, mais ils s'attaquent souvent aux infrastructures civiles, comme les institutions financières et les réseaux électriques, comme nous l'avons vu avec les cyberattaques des Russes en Ukraine et en Europe de l'Est.

La responsabilité de la capacité d'attaque incombe-t-elle uniquement au gouvernement du Canada ou devons-nous également permettre aux organisations civiles d'attaquer pour protéger leurs propres infrastructures et les Canadiens par la même occasion?

M. Christian Leuprecht: Certes, la résilience des infrastructures essentielles et des acteurs du secteur privé est essentielle. Cependant, quand — et non pas si — ils seront submergés... Il y aura des incidents dans le cadre desquels, par exemple, le système financier de l'une de nos banques pourrait être submergé par une attaque. Quels mécanismes avons-nous mis en place pour que la banque puisse appeler le Centre de la sécurité des télécommunications pour lui dire qu'elle est débordée et qu'il doit faire quelque chose pour désactiver cette attaque particulière ou peut-être saboter entièrement les capacités qui permettent ce type d'attaque, afin de préserver le système financier?

Je pense qu'à l'heure actuelle, nous ne disposons pas de mécanismes appropriés permettant aux acteurs des infrastructures essentielles et du secteur privé de s'adresser aux échelons supérieurs et de connaître les seuils exacts et les conditions dans lesquelles ils peuvent appeler le gouvernement pour que ce dernier intervienne. Je pense qu'il est essentiel pour un ministre et pour le gouvernement de mettre en place ces mécanismes pour que nous puissions obtenir l'aide dont les infrastructures essentielles et le secteur privé auront besoin dans des moments critiques.

Le président: Merci.

Merci, monsieur Bezan.

La parole est à M. Sousa, pour les trois dernières minutes.

M. Charles Sousa: Je vous remercie, monsieur le président.

Je vous remercie de votre témoignage.

Parlons donc des répercussions de certaines de ces questions. Comment pouvons-nous renforcer ces normes de comportement responsable? Si j'ai bien compris, certaines personnes craignent que nous ne renforcions pas le système ou que nous ne le remettions pas en question de manière efficace en vue de son application. Par ailleurs, nous sommes sensibles à une cyberattaque parrainée par un État, dont vous semblez suggérer qu'elle empêche certains de ces pays d'agir. Comment le Canada, en association avec le Groupe des cinq, veille-t-il à ce que des pays comme la Russie ou la Chine rendent compte de leurs actions? Comment vous en assurez-vous?

M. Christian Leuprecht: Vous le faites en partie en établissant des limites très claires et, d'autre part, en démontrant que nous sommes prêts à utiliser les capacités dont nous disposons en réponse à des comportements malveillants. Traditionnellement, les puissances moyennes, comme le Canada, agissent de concert avec leurs alliés et leurs partenaires. C'est ce qui fait la force de nos capacités, car ensemble, nous disposons toujours de capacités plus nombreuses, bien meilleures et plus avancées que [*difficultés techniques*].

M. Charles Sousa: Donnez-nous un exemple d'une de ces capacités.

M. Christian Leuprecht: Pensez, par exemple, au mécanisme de renseignement de l'OTAN qui est actuellement mis en place entre un grand nombre d'alliés et de partenaires. Nous pourrions également l'utiliser comme mécanisme de coordination des mesures cybernétiques actives et offensives, mais nous ne disposons actuellement d'aucun mécanisme efficace de ce type en dehors de la communauté du renseignement du Groupe des cinq.

M. Charles Sousa: Nous sommes en danger parce que nous ne sommes pas en mesure de l'appliquer ou parce que nous refusons de l'appliquer. Que font les États-Unis, par exemple, dans ce cas?

● (1050)

M. Christian Leuprecht: Nous risquons le sophisme de la composition, car actuellement le tout n'est pas plus grand que la somme des parties.

Le problème pour le Canada est que, pour pouvoir exploiter et tirer parti de cette capacité à coopérer avec les alliés et à travailler ensemble à l'établissement de ces normes, le Canada doit également fournir des capacités considérables. En effet, pourquoi les gens diraient-ils « Bien sûr, Canada, vous devriez participer à l'établissement des limites et nous aider à les cerner », alors que nous ne sommes pas disposés à déployer les capacités dont nous disposons en retour ou que nous n'avons pas réellement les capacités ou l'engagement nécessaires pour faire respecter ces limites?

Nous devons établir des limites au comportement cinétique inacceptable des États dans l'espace cybernétique, comme nous l'avons fait dans l'espace cinétique. Nous pouvons le faire, mais le gouvernement du Canada n'a pas manifesté la volonté politique d'engager ces discussions avec nos alliés et partenaires.

Le président: Merci, monsieur Sousa.

Je tiens à remercier le professeur Leuprecht d'être resté avec nous malgré les difficultés techniques.

Chers collègues, cette séance est terminée.

Vous avez reçu le budget pour les déplacements. J'ai besoin que quelqu'un le propose.

M. May le propose et M. Bezan l'appuie.

Fait-il l'objet d'un débat?

(La motion est adoptée).

Le président: Les partis doivent trouver une solution pour que ce budget puisse être mis en œuvre. J'espère que nous y parviendrons dans un avenir proche, car la planification du temps dépend entièrement de la coopération des partis. Vous pouvez vous adresser à vos whips respectifs.

Le dernier point que je voulais aborder est que nous aurons une politique « Protection, sécurité, engagement » 2.0. Elle vient d'être lancée. Je vous serais reconnaissant de me faire part de toute réflexion que vous pourriez avoir au cours de la semaine ou des deux semaines à venir quant au fait que le Comité s'engage ou non dans cet espace.

Sur ce, la séance est levée.