CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

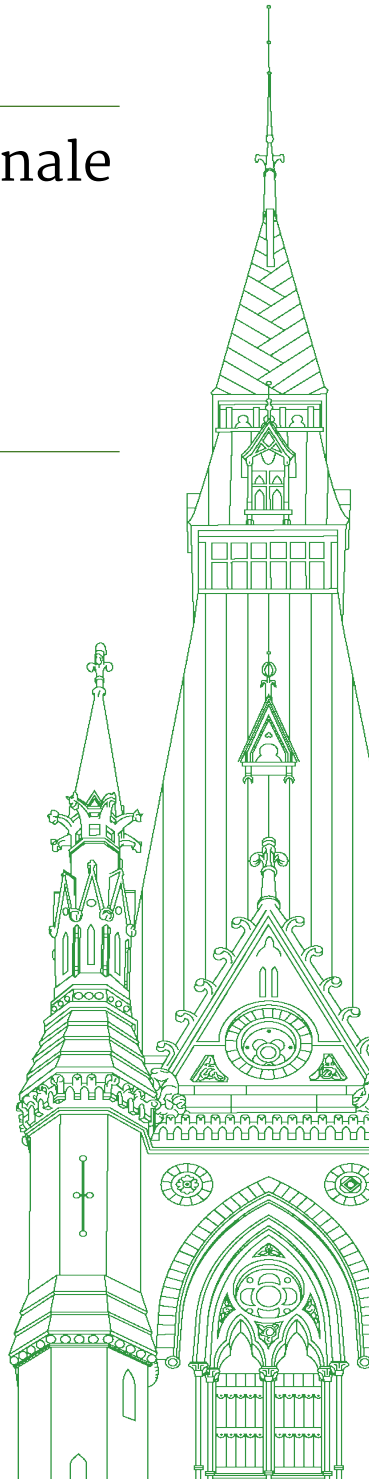
Comité permanent de la défense nationale

TÉMOIGNAGES

NUMÉRO 055

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le vendredi 31 mars 2023



Président : L'honorable John McKay

Comité permanent de la défense nationale

Le vendredi 31 mars 2023

● (0845)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): La séance est ouverte. Je constate que nous avons le quorum et qu'il est 8 h 45. Nous allons commencer sans plus tarder avec nos trois premiers témoins, avec qui nous allons poursuivre notre étude sur la cybersécurité et la cyberguerre.

Les représentants de BlackBerry, M. John de Boer, et de la Coalition pour la surveillance internationale des libertés civiles, M. Tim McSorley, comparaîtront en personne. Le président du conseil d'administration de l'organisme Slovenian Certified Ethical Hackers, M. Tadej Nared, témoignera par vidéoconférence.

Bienvenue à vous tous.

Je vais d'abord donner la parole à M. Nared, et les deux autres témoins suivront. Vous aurez chacun cinq minutes. Comme je l'ai déjà indiqué aux témoins présents dans la salle, nous attendons des invités vers 10 h 15. Je ne sais pas si nous aurons une heure ou plus. Nous allons commencer et nous verrons bien.

Monsieur Nared, vous disposez de cinq minutes. Nous vous écoutons.

M. Tadej Nared (président du conseil d'administration, Slovenian Certified Ethical Hackers Foundation, à titre personnel): Monsieur le président, distingués membres du Comité, merci.

Bonjour à tous. Permettez-moi de dire que je suis honoré de prendre la parole devant vous.

J'en suis à mon deuxième mandat de président du conseil d'administration de Slovenian Certified Ethical Hackers, une fonction que j'exerce de manière occasionnelle. Je collabore également avec des parlementaires et des comités de pays membres de l'Organisation du Traité de l'Atlantique Nord, l'OTAN, dans divers dossiers allant de la sécurité des élections électroniques aux infrastructures essentielles. J'agis de plus à titre de responsable virtuel de la sécurité de l'information pour le compte d'une société suisse de technologie financière, de même comme responsable de l'information d'une société de cyberdéfense détenue par des femmes ukrainiennes et établie aux États-Unis. Je fais de mon mieux pour aider ces femmes remarquables et totalement engagées à renforcer l'arsenal de cybermoyens et autres qui sont leur disposition pour défendre leur pays. Monsieur le président, si vous me le permettez, je vais maintenant prendre quelques minutes pour vous présenter mes remarques liminaires.

Je souligne pour commencer que normalement, je me serais préparé assidûment en vue d'une audition comme celle d'aujourd'hui, et que j'aurais réfléchi longuement à chacun des sujets dont je veux vous entretenir. Cependant, depuis que j'ai rencontré ces femmes d'un courage et d'une détermination sans nom, qui ont mis sur pied, dans une très large mesure, une des cyberarmées parmi les plus impressionnantes dans le monde, sans soutien ou sans financement extérieurs et sous les tirs de roquettes, ma conception de ce qui est important a complètement changé. J'adhère sans réserve à cette nouvelle réalité.

C'est une chose de parler de cyberguerre dans le confort de son foyer ou de son bureau tout en jouant à des jeux en ligne comme Locked Shields, de l'OTAN. C'en est une autre, comme nous l'avons vécu, quand un membre de l'équipe rapprochée ne peut pas se brancher à Internet parce qu'une roquette a atterri dans son appartement et a sectionné les câbles. Par chance, elle n'a pas explosé.

De la même manière, c'est une chose de pouvoir compter sur une bonne nuit de sommeil, et c'en est une autre de dormir deux ou trois heures par jour parce que les sirènes d'attaques aériennes vous réveillent constamment, mais malgré tout de continuer de faire un travail intellectuel exigeant jour après jour pendant plus d'une année parce que le temps est précieux et que vos compatriotes meurent.

C'est une réalité dont il faut absolument parler. Je connais plusieurs scénarios de cyberguerre, mais aucun qui prend en compte cette réalité d'avoir à travailler dans des conditions extrêmement stressantes, dans lesquelles le repos est possible seulement s'il y a une panne d'électricité ou si l'accès à Internet est coupé.

Récemment, nous avons présenté un exposé lors d'une conférence fermée sur les nouvelles technologies qui s'est tenue à Washington D.C. Les participants venaient surtout de forces armées et de services de renseignement du Groupe des cinq. Ils nous ont demandé comment nous arrivions à accomplir tout ce que nous leur avons présenté, et j'ai répondu simplement que les femmes ne dorment pas. C'est ce qui leur permet d'abattre autant de travail. Pour être très honnête, ce sont elles qui m'aident, et non le contraire.

J'ajouterai que je suis déçu que la réunion ne se déroule pas à huis clos, comme on dit, je crois. J'aurais aimé vous parler de certains résultats obtenus grâce aux opérations dans le cyberespace qui ont forcé l'admiration des représentants des forces armées et des services de renseignement présents. J'ai aussi en main de l'information essentielle sur la sécurité de tous les pays membres de l'OTAN. Cette information a été acquise par des cybermoyens et je suis à peu près certain que les agences occidentales n'y ont pas toutes accès. Je pense donc qu'il serait intéressant si, après la réunion, nous pouvions nous entendre sur une voie de communication sécurisée avec le Comité. Mes collègues et moi avons toute confiance au Comité pas seulement parce que le Canada agissait et aidait l'Ukraine pendant que d'autres se contentaient de parler, mais aussi parce que d'autres expériences nous ont convaincus que les membres du Comité sont dignes de confiance.

Pour ce qui a trait à la situation dans le monde réel, j'aimerais vous donner un exemple qui selon nous illustre parfaitement les efforts déployés par l'Ukraine pour mener sa cyberguerre, qui servira de point de départ à la discussion. La collecte de renseignements à participation volontaire est utilisée de manière très efficace, notamment dans les domaines du renseignement, de la surveillance et de la reconnaissance, et surtout grâce au système Delta, que les membres du Comité connaissent sûrement.

● (0850)

À cela s'ajoutent les opérations à participation volontaire. L'Ukraine s'est employée activement à mobiliser ce qu'il est convenu d'appeler une « armée des technologies de l'information », ou TI, qui regroupe plus de 100 000 spécialistes du domaine qui sont principalement chargés de mener des campagnes de guerre de l'information. De plus, une équipe de base de quelque 1 400 pirates informatiques très doués, qui ne sont pas rattachés à un organe militaire ou d'électronique intégrée, coordonnent les opérations entre les deux. Leurs compétences se sont révélées un atout remarquable.

Enfin, je voudrais attirer votre attention sur la divulgation récente des fichiers Vulkan, déjà connus des services de renseignement occidentaux. Essentiellement, cet incident ajoute du poids à mes appels des dernières années, y compris l'alerte que j'ai lancée devant le Comité à mon dernier passage concernant l'analyse des menaces par les Forces armées canadiennes…

Le président: Monsieur Nared, je suis désolé, mais je dois vous interrompre. Vos cinq minutes sont écoulées. Chose certaine, vous avez introduit dans notre discussion un aspect de la réalité qui, je crois, nous avait échappé jusqu'ici.

Je vous remercie. Vous allez avoir l'occasion d'échanger directement avec les autres membres du Comité.

M. Tadej Nared: Merci beaucoup.

Le président: Je vous en prie.

Sur ce, je donne la parole à M. de Boer, qui sera suivi de M. McSorley.

Vous avez cinq minutes, monsieur.

M. John de Boer (directeur principal, Affaires gouvernementales et politiques publiques, Canada, BlackBerry): Merci, monsieur le président.

Au nom de BlackBerry, je suis ravi de pouvoir échanger avec les membres du Comité.

Depuis plus de 35 ans, BlackBerry invente et met au point des solutions de sécurité fiables pour protéger la sûreté et la sécurité des particuliers, des gouvernements et des communautés. Nous faisons partie des chefs de file mondiaux dans les domaines des logiciels et des services de cybersécurité. Nos solutions protègent plus de 500 millions de systèmes dans le monde. Nous comptons parmi nos clients des gouvernements du G7, l'OTAN, 45 des sociétés figurant au classement Fortune 100, ainsi que 9 des 10 plus grandes banques.

Parce que tous les aspects de nos vies sont liés de près ou de loin au cyberespace, il faut agir de manière proactive pour réduire les cyberrisques auxquels le Canada est exposé. Nous pouvons y arriver en adoptant des technologies et des approches éprouvées pour la prévention des cyberattaques.

Pour cela, il faut modifier radicalement notre approche fondée sur un modèle réactif afin d'adopter une attitude proactive, et substituer une approche de la cybersécurité axée sur la prévention à l'approche actuelle de réponse aux incidents. Sur le plan opérationnel, la première chose est d'adopter des solutions de cybersécurité fondées sur l'intelligence artificielle les plus évoluées pour contrer les logiciels malveillants avant leur exécution. Ensuite, il faut bien définir les rôles liés à la cyberpréparation afin d'optimiser notre cyberdéfense collective. Enfin, il faut renforcer la collaboration entre le public et le privé pour optimiser notre cyberdéfense collective.

En matière de technologie, la plupart des solutions de cybersécurité fonctionnent selon le modèle des menaces connues liées aux logiciels malveillants, aux techniques d'attaque ou aux attaquants. Ces menaces connues sont définies à partir d'un ensemble d'échantillons de logiciels malveillants et d'indicateurs de compromission. Une fois recensées toutes les menaces connues, elles sont triées, examinées et publiées dans un répertoire hébergé dans le nuage. C'est seulement ensuite que les systèmes sont mis à jour, testés et réglés pour contrer les menaces connues.

Avec un modèle réactif, notre seule option est de ramasser les pots cassés après une cyberattaque. Il est impératif de réorienter notre approche pour tabler sur la prévention plutôt que sur la réponse aux incidents.

Chez BlackBerry, nous savons que c'est possible. À preuve, depuis 90 jours, nous avons intercepté plus de 1,5 million de cyberattaques par logiciels malveillants, dont 200 000 étaient de nouveaux échantillons, avant leur exécution. Nous y sommes parvenus en tirant profit de l'intelligence artificielle et de l'apprentissage automatique évolués pour dépister sans interruption les attaques et les contrer, y compris celles qui n'avaient jamais été vues. Si on ne met pas la priorité sur la prévention et les cybersolutions évoluées fondées sur l'intelligence artificielle, le Canada va continuer d'opérer en mode réactif.

La défense proactive exige en outre de définir clairement les rôles et de concerter nos efforts. Au sein du gouvernement fédéral, les cyberresponsabilités sont actuellement réparties entre une douzaine de ministères et d'organismes, sinon plus. Plusieurs ministères ont des responsabilités dans ce domaine, mais il est impossible de déterminer qui dirige et qui assure la cohérence et la concertation des efforts.

Si personne n'a la responsabilité claire de promouvoir et de défendre le dossier de la cybersécurité, il risque d'être relégué au énième rang parmi les autres priorités du gouvernement.

L'Australie et les États-Unis ont attaqué cet enjeu de front en nommant un cyberresponsable. Aux États-Unis, un cyberdirecteur national a été désigné par le président et approuvé par le Congrès. Le Canada devrait envisager la création d'un cabinet ou d'un poste supérieur auquel serait rattachée la responsabilité d'assurer la cohérence et l'action en matière de cybersécurité à l'échelle du gouvernement.

Enfin, le renforcement de la collaboration public-privé dans le domaine de la cybersécurité doit devenir prioritaire. Les sociétés comme BlackBerry peuvent mettre à contribution des connaissances et une expertise uniques en matière de défense contre les adversaires, et les organismes fédéraux ont les moyens et les pouvoirs nécessaires pour agir. Il faut favoriser une collaboration proactive entre le gouvernement et le secteur privé sur le plan des opérations. C'est essentiel pour combler les lacunes en matière de connaissance de la situation, assurer l'uniformité des guides d'intervention en cas d'incident et favoriser une culture axée sur la collaboration proactive à grande échelle.

BlackBerry sera à la disposition du Comité pour l'aider à renforcer la cyberrésilience du Canada. Je vous remercie de m'avoir donné l'occasion de prendre la parole aujourd'hui.

● (0855)

Le président: Merci, monsieur de Boer.

Monsieur McSorley, vous avez cinq minutes. Vous avez la parole.

M. Tim McSorley (coordinateur national, Coalition pour la surveillance internationale des libertés civiles): Merci beaucoup, monsieur le président, de me donner la chance de m'adresser au Comité.

La Coalition pour la surveillance internationale des libertés civiles est un organisme canadien qui fait un travail de veille dans les dossiers de sécurité nationale, de lutte au terrorisme et de libertés civiles au Canada. Nous avons une longue expérience dans le suivi du travail du Canada, et notamment de ce que fait le Centre de la sécurité des télécommunications, le CST, dans les domaines de la surveillance et des cyberactivités.

Nous reconnaissons qu'il est vital pour le Canada de moderniser ses lois en matière de cybersécurité afin de mieux protéger les renseignements confidentiels des Canadiens et les infrastructures d'information dont nous dépendons. Nous sommes très conscients également que le nombre et la complexité des cyberattaques augmentent, et que le Canada n'a pas le choix de prendre des mesures pour se défendre. Néanmoins, nous pensons que rien ne doit être fait au détriment de la responsabilité et de la transparence des activités du gouvernement, y compris celles du CST.

Notre travail nous a permis de voir comment des pouvoirs trop larges et une culture du secret trop poussée laissent la porte ouverte à des violations des droits des Canadiens et des personnes qui vivent au Canada. Les conséquences sont réelles, notamment lorsque les renseignements des Canadiens et des personnes qui vivent ici sont transmis à des pays du Groupe des cinq ou à des organismes étrangers. Quand ces renseignements tombent entre les mains d'une autorité étrangère, le Canada perd le contrôle sur ce qu'on en fait et laisse le champ libre à des utilisations qui peuvent mener à des atteintes aux droits, à des abus et même à la torture.

Nous ne souscrivons pas non plus à l'idée que les renseignements confidentiels de non-Canadiens peuvent être livrés en pâture pour les opérations de collecte et de conservation massives à l'étranger. Cette approche contribue à renforcer les systèmes mondiaux actuels de surveillance de masse et les violations des droits qui en découlent.

C'est ce qu'Edward Snowden nous a expliqué avec force détails. Il s'en est ensuivi des promesses de réforme au Canada, mais il est pour l'instant impossible d'établir en quoi les méthodes du CST ont changé. Ces préoccupations touchent les activités de renseignement électromagnétique du CST, mais elles s'appliquent aussi à ses activités en matière de cybersécurité et cyberguerre. Son mandat comporte effectivement deux volets distincts, le renseignement électromagnétique et la cybersécurité ainsi que l'assurance de l'information, mais leur exécution ne se fait pas en vase clos.

Dernièrement, l'Association des libertés civiles de la Colombie-Britannique a publié du matériel divulgué dans le cadre d'une poursuite intentée contre le gouvernement fédéral relativement aux activités du CST. Ces documents révèlent entre autres qu'au titre d'une entente avec l'ancien ministère des Affaires étrangères, le CST pouvait transmettre à ses homologues du Groupe des cinq les éléments d'information recueillis lors de ses activités de soutien à la cybersécurité du ministère, y compris les communications privées des Canadiens. L'entente date de 2012, mais ce sujet de préoccupation persiste malgré l'adoption de la Loi sur le Centre de la sécurité des télécommunications en 2019.

Plus précisément, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, a relevé dans son rapport annuel de 2021 que la Loi sur le CST autorise explicitement la communication de ce type d'information pour la conduite d'activités au titre de ses divers mandats, y compris celles qui touchent la cybersécurité et le renseignement étranger. Selon l'OSSNR, il y a lieu de réduire l'étendue de ces communications et de prendre des décisions au cas par cas, et le CST devrait obtenir un avis juridique sur la conformité à la Loi sur la protection des renseignements personnels. Le CST s'est dit en désaccord avec ces conclusions.

Pourquoi est-ce important? Le projet de loi C-26, actuellement à l'étude au Parlement, officialiserait le rôle du CST dans la protection de la cyberinfrastructure et l'autoriserait à recueillir de l'information sur la sécurité de l'infrastructure essentielle.

Le CST aurait donc accès à beaucoup plus de renseignements, qui pourraient englober des renseignements confidentiels concernant des Canadiens. À défaut de mesures de protection adéquates, tant dans la Loi sur le CST que dans le projet de loi C-26, les renseignements recueillis par le CST, y compris ceux qui concernent des Canadiens, pourront être utilisés de manière inattendue et être communiqués à des partenaires étrangers n'ayant aucun compte à rendre.

Pour un exposé plus détaillé à cet égard, j'invite le Comité à prendre connaissance d'une lettre ouverte que nous avons cosignée avec plusieurs autres groupes de la société civile concernant un rapport récent du Citizen Lab qui s'intitule *Cyber Security Will Not Thrive in Darkness*. Je pourrai transmettre les deux documents au Comité après la réunion.

Il faut savoir que le CST a des antécédents assez troublants pour ce qui est de masquer la nature de son travail et de transgresser son mandat. Par exemple, il a surveillé les connexions sans fil de Canadiens se trouvant dans de grands aéroports, en dépit de l'interdiction de faire de la surveillance au Canada. Il a recueilli des quantités phénoménales de communications en ligne par l'intermédiaire de 200 sites Internet du réseau de base un peu partout dans le monde. Même si cela lui est interdit, le CST recueille régulièrement les renseignements des Canadiens. Il en a reçu de partenaires étrangers, et il a violé les lois canadiennes pendant cinq ans en omettant de minifier les renseignements des Canadiens avant de les transmettre à des partenaires du Groupe des cinq.

Qui plus est, le CST ne se conforme pas complètement à ses obligations en matière d'examens et de surveillance. Notamment, il refuse de donner à l'OSSNR le plein accès aux dossiers dont il a besoin pour s'acquitter de sa fonction d'examen. Le CST demande à l'OSSNR de lui soumettre une requête et le personnel lui transmet les documents qu'il juge pertinents. Cette tactique, selon ce que l'OSSNR a souligné dans son dernier rapport annuel, nuit à son pouvoir de déterminer si l'information est liée à ses examens, et elle contribue à retarder considérablement la communication de l'information à l'OSSNR.

● (0900)

Le commissaire au renseignement s'est aussi inquiété du fait que les autorisations du CST en ce qui concerne les services de renseignement étrangers et la cybersécurité ne comprennent pas de données essentielles pour le processus d'approbation, notamment en ce qui a trait aux résultats d'activités autorisées auparavant ou d'explications d'activités particulières reposant sur des faits.

Enfin, l'OSSNR s'est également dit préoccupé par le fait que le CST ne fournisse pas de renseignements suffisants sur les conséquences de cyberopérations actives ou défensives et ne fasse pas suffisamment la distinction entre les deux types d'activités qui, pourtant, nécessitent des processus d'approbation différents.

J'ai quelques recommandations à formuler, très courtes, mais je les garde pour la période des questions.

Je vous remercie.

Le président: Si vous ne les mentionnez pas pendant la période des questions, vous pouvez, en tout cas, les communiquer au greffier.

Cela étant dit, nous passons à la série de questions de six minutes, et nous commençons par M. Kelly.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Je vous remercie.

Je commencerai par M. de Boer, mais j'inviterai les trois témoins à commenter ma question.

Je veux parler de la menace que représentent l'espionnage industriel ou les vulnérabilités dans le secteur privé en matière de cybersécurité. Un article expliquait dernièrement comment les pirates informatiques peuvent manipuler la température d'une étable et décimer des cheptels, ou que la chaîne d'approvisionnement alimentaire est particulièrement vulnérable aux cyberattaques. On dépasse là les dommages causés à une société privée. C'est la sécurité alimentaire, entre autres, qui est en jeu.

Je commencerai par vous, puis je demanderai à chaque témoin des commentaires sur les vulnérabilités du secteur privé qui se répercutent sur la sécurité nationale.

M. John de Boer: Je vous remercie, monsieur le président. C'est une excellente organisation.

Jusqu'à présent, la cybersécurité se concentre surtout sur ce que nous appelons les systèmes informatiques des entreprises. Une des plus grandes failles se révèle être dans la technologie opérationnelle. Il y a normalement des systèmes qui contrôlent, par exemple, un réseau électrique, des turbines à gaz, des systèmes de contrôle industriels dans les canalisations, etc. Beaucoup de ces systèmes sont maintenant mis en ligne. Ce que nous avons vu aux États-Unis, par exemple, avec l'attaque contre le Colonial Pipeline ou même contre le réseau d'alimentation en eau d'Oldsmar, en Floride, c'est que ces systèmes ne sont pas conçus pour être reliés à Internet, y compris l'équipement agricole, etc., mais des personnes essaient maintenant de permettre une optimisation moyennant une connexion à Internet.

Nous avons remarqué, par exemple, que le nombre d'attaques a augmenté de 2 000 % dans le secteur manufacturier au cours de l'année écoulée. Les trois secteurs les plus ciblés par les cybercriminels au cours des 12 derniers mois sont les soins de santé, la finance et la fabrication, mais c'est la fabrication qui est le plus souvent visée. Pourquoi? D'après notre évaluation, c'est à cause des vulnérabilités de la chaîne d'approvisionnement que nous voyons et du lien intrinsèque entre la sécurité économique et la sécurité nationale. De plus, comme tout est étroitement lié, comme je le mentionnais plus tôt, ce sont de plus en plus des vecteurs d'attaque.

● (0905)

M. Pat Kelly: Si vous le permettez, je demanderai aussi leur avis aux autres témoins. Peut-être que j'aurai du temps pour d'autres questions.

Allez-y.

Le président: Monsieur Nared, avez-vous des commentaires?

M. Tadej Nared: La cybercriminalité, qui est le terme que nous employons généralement pour décrire l'espionnage industriel et les activités criminelles ordinaires, constitue, en fait, la troisième économie mondiale. D'ici 2025, les dégâts causés par la cybercriminalité s'élèveront à 15 billions de dollars. Ils augmentent de 1 500 milliards de dollars par an. C'est un énorme problème. Les efforts consentis pour contrer la cybercriminalité ne sont pas à la hauteur des dégâts causés qui ne cessent d'augmenter.

À propos de ce que disait le témoin précédent, les attaques contre les infrastructures essentielles en particulier, qui sont interdites par les conventions de Genève, car elles visent des infrastructures civiles, augmentent de jour en jour. Nous devons prendre en compte les acteurs étatiques, notamment la Russie.

C'est ce que j'essayais de faire mettre en vigueur avant les fichiers Vulkan. Avant, nous ne faisions que des suppositions sur les capacités des Russes, mais maintenant, nous sommes certains et nous avons la confirmation qu'ils collectent des données dans le monde entier. Ils compromettent des réseaux, des centrales électriques, des centrales hydroélectriques et des infrastructures civiles allant d'hôpitaux à tout le reste. Ils collectent ces données, passent systématiquement au crible les vulnérabilités et versent les données dans une immense base de données pour se préparer à un scénario de type cygne noir.

Ce que je crains vraiment, c'est que les pays occidentaux, les pays de l'OTAN, ne protègent pas leurs infrastructures comme ils le devraient. C'est un énorme problème, et il faudrait s'y attaquer rapidement.

M. Tim McSorley: Je serai bref. Il est évident que le gouvernement fédéral a un rôle à jouer pour ce qui est d'aider les entreprises privées à renforcer leur cybersécurité et de protéger la sécurité nationale. Il est essentiel, selon nous, à cet égard que ce processus soit transparent et fiable pour que les entreprises privées sachent ce que le gouvernement va faire quand il apportera cette aide. Le public a besoin de cette confiance et de savoir ce que sont les services offerts. Ce doit être, selon nous, un élément central de textes législatifs tels que le projet de loi C-26.

M. Pat Kelly: D'accord. Je vous remercie.

Si je peux avoir un instant, j'ai une question très précise qui découle du témoignage de M. Nared.

Le président: Moi aussi, mais vous êtes pile à six minutes. Si je vous laisse poser votre question, c'est la porte ouverte aux problèmes pour moi parce que j'aurai laissé quelqu'un dépasser le temps imparti. Je suis désolé, monsieur Kelly.

M. Pat Kelly: Peut-être que vous pouvez quantifier ce chiffre en billions de dollars sur le temps de quelqu'un d'autre.

Le président: Le chiffre est impressionnant. Je l'ai relevé moi aussi.

Monsieur May, vous disposez de six minutes.

M. Bryan May (Cambridge, Lib.): Je vous remercie, monsieur le président.

Monsieur de Boer, en 2021, vous souligniez dans un article pour la Chambre de commerce que:

> Selon l'OCDE, le Canada fait partie des quelques pays où l'investissement dans la R-D sur les technologies « stagne ». En fait, cet investissement ne représente que 1,5 % du PIB et il diminue, alors que les concurrents du Canada investissent des milliards pour améliorer leurs capacités sur le plan de la cybersécurité.

À votre avis, monsieur, quels sont les facteurs qui contribuent à ce sous-investissement du secteur privé canadien dans la R-D?

● (0910)

M. John de Boer: C'était en 2021, mais les données restent les mêmes aujourd'hui. Nous sommes à la traîne en matière d'investissement dans la R-D. Nous nous réjouissons, par exemple, du renouvellement et de la révision des encouragements fiscaux pour la recherche scientifique et le développement expérimental annoncés tout récemment, mais les entreprises gagnent bien plus à développer la R-D à l'étranger, notamment les multinationales parce qu'il y a beaucoup plus de systèmes de soutien collaboratifs en place, que ce soit avec la recherche universitaire ou autrement.

BlackBerry s'est engagée à investir au Canada. Nous investissons environ 24 % de notre chiffre d'affaires annuel dans la R-D et travaillons en étroite collaboration avec des universités canadiennes, etc., mais toutes les entreprises ne sont pas incitées à en faire autant.

Il faut vraiment un partenariat concerté entre le gouvernement et le secteur privé, pas sur toute la ligne, mais en pariant sur certains créneaux où le Canada jouit d'un avantage comparatif. Notre article disait que la cybersécurité fait partie des domaines où le Canada jouit d'un avantage comparatif. Nous occupons le quatrième rang mondial en nombre d'entreprises de cybersécurité, mais nous accusons du retard sur Israël, le Royaume-Uni ou les États-Unis qui sont loin devant nous.

M. Bryan May: Pouvez-vous en dire un peu plus et formuler quelques recommandations quant aux mesures à prendre pour faire en sorte que la propriété intellectuelle créée au Canada, souvent avec une aide financière directe ou indirecte de l'État, reste au Canada?

M. John de Boer: Je pense que la commercialisation est un des éléments clés en l'occurrence.

Il y a beaucoup de ce que nous appelons un niveau de maturité technologique inférieur. Autrement dit, le tout début de la R-D se déroule au Canada, mais ensuite, passée cette étape initiale, la R-D traverse ce qu'on appelle la vallée de la mort, ce qui veut dire qu'il est très difficile de productiser cette R-D ici, au Canada.

Par exemple, très peu de programmes soutiennent les entreprises canadiennes pour les aider à lancer des produits initiaux afin de les essayer et de commercialiser, alors qu'aux États-Unis, par exemple — évidemment, les budgets d'approvisionnement du gouvernement américain sont beaucoup plus élevés —, le processus d'appel d'offres est beaucoup plus souple. Ils ont mis en place des systèmes pour aider les entreprises à franchir cette vallée de la mort afin qu'elles puissent commercialiser leurs produits.

Nous avons notamment proposé à la Chambre de commerce du Canada de créer un fonds de commercialisation canadien qui aiderait des entreprises canadiennes à passer à l'étape de la productisation.

La Corporation d'innovation du Canada, qui était annoncée dans le budget de 2022, est peut-être un début, mais nous manquons encore de détails à son sujet. Nous espérons que tout le volet de la commercialisation, qui aidera à faire en sorte que les produits commercialisés au Canada permettent de garder la propriété intellectuelle dans ce pays, sera un aspect essentiel de cette question.

M. Bryan May: Nous avons entendu dire à maintes reprises qu'il est à craindre que des composantes électroniques fabriquées par des sociétés affiliées à l'État dans des pays comme la Chine présentent un risque pour la cybersécurité au Canada. Faut-il s'inquiéter du risque pour la cybersécurité que représente la fabrication à l'étranger de matériel informatique?

M. John de Boer: BlackBerry, parce qu'elle a créé des appareils, veillait tout particulièrement à ce que tous les composants de ces appareils, y compris les logiciels, correspondent à ce qui était annoncé. Nous avons même développé un logiciel qui nous aidait à retracer la provenance de chaque composant.

La question préoccupe énormément aux États-Unis. Le décret présidentiel 14028, qui concerne la cybersécurité du pays, ordonne la production d'une nomenclature des logiciels, c'est-à-dire d'une liste des ingrédients de tous les logiciels contenus dans tous les appareils. Pour l'instant, si vous demandez aux gens quels sont les logiciels dans leur système ou dans leur appareil, très peu le savent.

Le problème tient aussi en partie aux graticiels. Il s'agit de logiciels gratuits disponibles sur Internet qui sont largement utilisés, mais qui présentent des failles de sécurité importantes.

Il me semble que le Canada devrait notamment envisager, ce que font d'ailleurs beaucoup d'autres pays de l'Union européenne et les États-Unis, de s'assurer qu'il y ait un engagement envers des principes de conception sécurisée. On ne peut pas ajouter la sécurité après coup.

● (0915)

M. Bryan May: Je vous remercie.

Dans les 10 dernières secondes qui me restent, monsieur, je me demande si le comité souhaite que M. Nared parle de l'information qu'il ne peut pas nous communiquer. Est-ce que je peux demander qu'il cherche avec le greffier une solution éventuelle à ce sujet?

Le président: Pourquoi pas? Nous en donnerons donc instruction. Je vous remercie.

Cela dit, madame Normandin, vous disposez de six minutes.

[*Français*]

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

Monsieur de Boer, je vais vous poser le même genre de questions que celles de mon collègue M. May.

Vous avez mentionné, parmi vos trois priorités, l'importance d'être bien équipé pour agir de façon préventive plutôt que réactive. Le Canada semble toujours agir de façon réactive.

Pour ce qui est de l'équipement, dans quels domaines faudrait-il investir en priorité, si on veut agir de façon préventive? S'agit-il de l'intelligence artificielle ou de la cryptographie post-quantique, par exemple?

M. John de Boer: Je vous remercie de votre question.

[*Traduction*]

Ce que nous pouvons faire immédiatement, c'est veiller à ce que le ministère de la Défense nationale, le gouvernement et les infrastructures essentielles soient équipés de ce que nous appelons les toutes dernières technologies. Des technologies qui reposent sur l'intelligence artificielle, l'IA. Ce n'est pas le cas aujourd'hui.

À l'heure actuelle, il y a deux gros problèmes. L'un est qu'il n'y a pas assez de cyberprofessionnels dans le monde. Il y a plus de trois millions de postes vacants à l'échelle mondiale et, au Canada, il y en a probablement autour de 200 000. Le ministère de la Défense nationale et les organismes chargés des infrastructures essentielles en souffrent aussi.

Nous devons compenser avec des machines, avec l'IA, parce qu'on dénombre plus de 400 000 nouveaux types de logiciels malveillants par jour. Il s'agit d'une technologie éprouvée. Celle de BlackBerry, par exemple, a été mise au point en 2012. Nous en sommes à notre septième génération.

Cette solution peut être mise en œuvre. Il faut veiller dans les spécifications des marchés publics, etc. à ne pas inclure de spécifications qui nous lient à des générations de technologie antérieures, à des technologies reposant sur des signatures. C'est la première chose.

Ensuite, nous devons investir continuellement dans la R-D, comme il a été dit plus tôt, pour ne pas être dépassés par nos rivaux. Nous voyons déjà des cybercriminels utiliser ChatGPT, entre autres, pour des attaques par hameçonnage. Nous devons faire en sorte que notre IA soit meilleure que la leur pour nous défendre.

C'est quelque chose que nous pouvons faire dès maintenant. Il existe des technologies de cryptographie quantique, mais nous devons travailler continuellement sur certains de ces problèmes. Ce doit être un effort constant. Je dirai d'utiliser la technologie dont nous disposons actuellement.

[*Français*]

Merci.

Mme Christine Normandin: Merci beaucoup.

Vous avez aussi parlé de la collaboration entre les secteurs public et privé. J'aimerais entendre vos commentaires à cet égard, et peut-être aussi ceux de M. Nared sur une éventuelle collaboration tripartite avec les cyberpirates.

Pourrait-on faire progresser quelque chose en ce sens? Y a-t-il des risques de travailler avec des communautés de cyberpirates?

J'inviterais M. de Boer à répondre en premier et ensuite M. Nared.

M. John de Boer: C'est une très bonne question.

[*Traduction*]

La réalité à l'heure actuelle est que le partenariat ou la collaboration entre les secteurs public et privé est pour beaucoup réactive, encore une fois. Elle intervient au lendemain d'un incident ou en présence d'un indicateur de vulnérabilité, et est, dans une large mesure, unilatérale. Nous fournissons l'information au gouvernement et elle disparaît dans un trou noir.

BlackBerry entretient de bonnes relations avec le Centre canadien pour la cybersécurité, etc., mais elles pourraient être bien plus solides.

Je proposerai, encore une fois, de passer à une approche d'abord axée sur la prévention. Planifions avant un incident. Élaborons des plans opérationnels, des plans d'urgence et des plans d'atténuation qui clarifient les rôles et responsabilités lorsque le système informatique d'une infrastructure essentielle est piraté.

Quant à travailler avec des pirates informatiques, absolument, nous travaillons avec des « white hackers », des pirates bien intentionnés, des pirates éthiques, pour tester les vulnérabilités des systèmes, qu'il s'agisse d'automobiles ou d'autres dispositifs connectés. Ce sont des éléments clés de notre communauté.

Je ne suis pas aussi certain pour ce qui est de la situation au Canada, mais dans certains contextes, leur aptitude à travailler en cohorte en collaboration avec des entreprises et le gouvernement est limitée à cause du cadre juridique habilitant qui n'est pas autorisé. Au Royaume-Uni, par exemple, on envisage actuellement de changer le cadre juridique afin de permettre une bien plus grande collaboration entre les pirates bien intentionnés, les bons pirates, et le gouvernement, etc.

C'est un sujet fantastique.

[*Français*]

Merci beaucoup.

● (0920)

Mme Christine Normandin: Merci beaucoup, monsieur de Boer.

Monsieur Nared, voulez-vous ajouter un commentaire?

[*Traduction*]

M. Tadej Nared: Je pense qu'il est essentiel de collaborer avec des pirates éthiques si nous voulons sécuriser les pays occidentaux.

J'utiliserai comme exemple le programme pilote de primes de bogues du Pentagone. Le Pentagone a ouvert ses systèmes sur la plateforme de primes de bogues où des pirates éthiques pouvaient tester les systèmes et signaler leurs vulnérabilités. Le résultat a été que les systèmes ont été compromis. Le premier signalement est arrivé, je crois, dans les sept premières minutes et, dans les six premières heures, il y a eu entre 200 et 300 signalements. Autrement dit, 300 vulnérabilités en matière de sécurité, 300 failles qu'un adversaire pouvait exploiter pour accéder aux systèmes du Pentagone.

Grâce à cette collaboration, le Pentagone a renforcé sa sécurité. Il me semble que c'est M. Ash Carter qui a félicité l'initiative et qui a conclu, en un sens, qu'on ne savait pas combien de bons pirates éthiques et combien de bons professionnels des TI aimeraient aider, mais n'en ont pas l'occasion.

Comme l'expérience en Ukraine le montre, il est essentiel d'utiliser du renseignement participatif, des efforts participatifs, dans de tels contextes, surtout dans le cyberespace, pour obtenir les résultats désirés. Autrement, je ne crois pas que ce soit même possible.

Le président: Je vous remercie, madame Normandin.

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

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

Je remercie tous les témoins de leur présence aujourd'hui.

Monsieur McSorley, j'aimerais vous poser une question. Au Comité, au début de l'étude, nous avons entendu les témoignages des services de renseignement canadiens, notamment du CST, et ils ont déclaré à maintes reprises qu'ils ne ciblent pas les Canadiens et ne recueillent pas de données sur les activités canadiennes, mais la BC Civil Liberties Association a déclaré dans sa plaidoirie lors d'une action en justice que « ce qui est vraiment choquant, c'est à quel point le CST repousse les limites de la légalité et se joue même de la réglementation et de la supervision la plus raisonnable ».

Que pensez-vous du fait que ces services de renseignement repoussent constamment les limites légales fixées par le droit canadien?

M. Tim McSorley: Je pense que cela dépend beaucoup du verbe « cibler » et de ce que vous disiez à propos du témoignage du CST devant le Comité.

Il est vrai que le CST, de par son mandat et la Loi sur le Centre de la sécurité des télécommunications, ne peut pas prendre pour cible des Canadiens, mais dans la collecte de renseignements électromagnétiques et dans l'exécution de ses tâches, y compris relatives à la cybersécurité et à la protection des cyberinfrastructures, comme je le mentionnais, il recueille toutes sortes de données qu'il trie ensuite. Il y a ce qu'on appelle de l'information non sélectionnée, c'est-à-dire qui n'est pas spécifiquement ciblée, mais qu'il arrive au CST d'accumuler dans ses collectes, et ensuite, cette information est conservée et une partie peut se rapporter à des Canadiens. C'est là que surviennent les problèmes, comme je le mentionnais tout à l'heure, dans le partage de renseignements canadiens avec le Groupe des cinq et avec d'autres pays.

Le CST ne cible pas des Canadiens — revoilà le verbe « cibler » —, mais il recueille accessoirement ces renseignements et les conserve, et ils sont encore utilisés par ailleurs. Voilà ce que nous voyons. C'est ce qui arrive quand il repousse les limites.

Il y a une autre catégorie d'information, les métadonnées. Les métadonnées ne sont pas les communications elles-mêmes. C'est toute l'information autour de la communication, comme qui a envoyé l'information, qui l'a reçue, d'où elle est partie, quel type de logiciel a été utilisé et quel genre d'équipement. Il y a depuis longtemps un débat sur la question de savoir si les métadonnées devraient être considérées comme des données personnelles ou pas. Il est évident que, mises en ensemble, des métadonnées peuvent brosser un tableau très clair de ce que des personnes font et permettre d'identifier certaines personnes, mais le CST a toujours soutenu qu'elles ne constituent pas des données personnelles. Encore une fois, il ne cible pas des Canadiens, mais recueille ce type d'information.

La dernière chose que je mentionnerai concerne les renseignements publics. Malgré toutes les autres restrictions qui lui sont imposées dans la collecte de renseignements, le CST peut recueillir des renseignements publics. Là encore, il n'est pas autorisé à recueillir des renseignements qui ont des répercussions sur la vie privée des Canadiens, mais le débat demeure sur ce qui est considéré comme des données personnelles ou ce qui justifie une attente raisonnable en matière de respect de la vie privée. Par exemple, en ce qui concerne l'information que nous publions dans les médias sociaux, nous attendons-nous à ce qu'elle soit collectée, conservée et, peut-être, partagée par les organismes chargés de la sécurité nationale?

C'est ce qui était au cœur du débat sur Clearview AI. La société faisait valoir que les images faciales des Canadiens en ligne étaient considérées comme étant du domaine public et qu'elle pouvait les collecter. Le commissaire à la protection de la vie privée a statué qu'il s'agissait d'une surveillance de masse et que c'était illégal. Quand la question a été posée à la GRC, elle a répondu qu'elle n'avait aucune obligation de vérifier, si elle travaillait avec la société Clearview AI, qu'elle respectait le droit canadien.

Nous ne savons pas ce qu'il en est du travail du CST sur la technologie de reconnaissance faciale, mais si nous voyons cette attitude de la part de la GRC et cette approche, cette définition et l'absence de clarté en ce qui concerne l'information déjà du domaine public, nous devons craindre que le CST adopte la même interprétation.

● (0925)

Mme Lindsay Mathyssen: Merci de votre réponse.

En effet, le glossaire des termes relatifs aux données non sélectionnés et aux données publiques, ainsi que leur utilisation, était mentionné dans la même action en justice, dans les documents que la BC Civil Liberties Association a produits. Est-ce que des lois comme le projet de loi C-59...? Cette action en justice est antérieure au projet de loi C-59. Elle concerne plus les problèmes visés par le vieux projet de loi C-51. Plus particulièrement, lorsque nous regardons le projet de loi C-26, est-ce que ces lois contrent efficacement les menaces dont s'inquiètent les défenseurs des libertés civiles au sujet de l'exploitation des données publiques?

Le président: Je vous remercie.

C'est une bonne question. Vous avez une trentaine de secondes pour y répondre, toutefois.

M. Tim McSorley: Je dirai simplement que non. Plusieurs des problèmes que j'ai soulevés figuraient dans le projet de loi C-59, à l'origine de la Loi sur le Centre de la sécurité des télécommunications. Nous pensons qu'il faut, entre autres, renforcer les pouvoirs de l'OSSNR et du commissaire au renseignement afin qu'ils puissent examiner ces types d'activités et parler publiquement de leurs conclusions.

Le président: Je vous remercie.

C'était une réponse concise. Il vous reste donc encore 15 secondes, madame Mathyssen.

Nous passons à la série de questions de cinq minutes et la parole est à Mme Gallant.

Mme Cheryl Gallant (Renfrew—Nipissing—Pembroke, PCC): Je vous remercie, monsieur le président.

Mes questions sont pour M. Nared. Je poserai rapidement trois questions, puis il pourra gérer son temps pour y répondre.

Nous venons de terminer une étude sur l'Arctique au Comité. Nous recommandons notamment qu'au lieu d'acheter des sous-marins, nous utilisions des drones sous les glaces de l'Arctique canadien. Nous savons que des adversaires traversent actuellement cet espace en sous-marin et qu'ils ont les données en temps réel.

Est-ce que la transmission de données à qui que ce soit depuis un drone sous-marin dans l'Arctique est plus vulnérable que la surveillance sur place en temps réel? C'est la première question: les menaces pour les drones sous les glaces arctiques.

Voici la deuxième: quelle est l'incidence de l'intelligence artificielle sur les menaces cybernétiques?

Et la troisième: comment les services de sécurité ou la défense nationale peuvent-ils faire la distinction entre une série d'attaques, ou des attaques simultanées, contre la technologie des communications ou des systèmes de contrôle industriels et dire si ces attaques sont les précurseurs d'une attaque cinétique?

M. Tadej Nared: Je vous remercie, madame Gallant, de ces questions, qui sont excellentes.

En ce qui concerne les drones, il s'agit, en fait, du summum de l'industrie de la cybersécurité. Autrement dit, il s'agit de la guerre électronique. J'ai eu dernièrement des discussions avec des personnes associées de très près au domaine, et c'est un jeu du chat et de la souris permanent. Il n'est pas facile de répondre à cette question, mais les drones sont équipés de technologies davantage fabriquées dans le secteur privé qui les rendent très résistants face à la guerre électronique. Nous avons eu l'occasion d'en voir quelques-uns survoler le territoire russe récemment, et ils continuent de voler, alors...

C'est plus une question de guerre électronique. L'essentiel est que toutes ces unités de guerre électronique sont capables de transmettre le signal, mais le problème le plus crucial est de savoir comment transformer ce signal en zéros et uns, pour dire les choses simplement. C'est un des plus grands problèmes qui se posent actuellement aux unités de guerre électronique du Groupe des cinq ou des pays de l'OTAN, mais ils cherchent des solutions.

Pour ce qui est de l'incidence de l'intelligence artificielle sur les menaces cybernétiques, je dirai que l'IA est une arme à double tranchant. Elle peut être utilisée pour des moyens défensifs et offensifs, comme l'a expliqué tout à l'heure l'autre témoin. ChatGPT, par exemple, est devenu un des plus gros producteurs de maliciels. Il a été piraté en moins de quelques jours. Comme Head Hackers, les pirates l'utilisent efficacement non seulement pour produire des courriels de hameçonnage et le contenu qui s'y rapporte, mais aussi pour produire des logiciels malveillants perfectionnés. Il est très facile de contourner les restrictions mises en place par OpenAI et, en gros, de lui faire écrire n'importe quel code auquel on peut penser, y compris pour attaquer des systèmes SCADA ou pour faire une copie du ver STUXNET. Tout dépend de la créativité de la personne qui parle avec.

Quant à voir dans des attaques préliminaires le signe avant-coureur d'attaques cinétiques, je dirai que toute attaque préliminaire conduira à une attaque cinétique, surtout lorsqu'il s'agit de la Russie et de ses capacités. Je soulignerai encore une fois que, pas plus tard qu'hier, des informations ont été publiées sur les fichiers Vulkan qui décrivent très bien les cybercapacités russes. Ces fichiers prouvent que les Russes attaquent systématiquement des infrastructures occidentales depuis des années — qu'ils attaquent nos infrastructures et nos systèmes de contrôle industriels — et qu'ils recueillent tous les renseignements qu'ils peuvent, qu'ils les réunissent dans la base de données et qu'ils attendent le bon moment pour frapper, et nous devrions commencer à le prendre très au sérieux.

● (0930)

Le président: Je vous remercie, monsieur Nared et madame Gallant.

Monsieur Sousa, vous disposez de cinq minutes. Vous avez la parole.

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

Je remercie les témoins de leurs exposés. Nous sommes préoccupés — nous tous — par les mesures de sécurité dans ce pays, ainsi que par la protection des renseignements personnels et notre souveraineté nationale.

Ma première question est pour M. de Boer. Si nous examinons la notion de propriété intellectuelle et la commercialisation de la propriété intellectuelle, et la propriété des technologies, nous voyons que le Canada semble s'en sortir plutôt bien... En fait, le Canada est un fournisseur important d'infrastructures et de TI à d'autres pays, et ils ont eux-mêmes remarqué que nous sommes à la traîne par rapport à ce qui se fait ailleurs. Je crois que le comité des sciences et de la recherche examine aussi la commercialisation de la propriété intellectuelle et les solutions pour franchir cette vallée de la mort que vous mentionniez.

Les questions sont donc les suivantes: qui tranche à propos de certains de ces contrats? Comment coordonnons-nous le secteur privé pour faciliter la collaboration avec le milieu universitaire? Quel doit être le rôle du gouvernement dans tout cela? Vous avez mentionné deux fonds qui étaient proposés.

J'ai encore du mal, toutefois, à cause de notre attitude, qui peut sembler réactive, qui est que c'est nécessairement un moyen de proposer une nouvelle technologie et une nouvelle innovation, pour ensuite les protéger en détenant la propriété intellectuelle et le brevet, de sorte que d'autres ne puissent pas les utiliser. Comment obliger quelqu'un qui en profite — et, au fond, comment obliger d'autres pays — à rendre des comptes? Est-il vraiment...? Nous avons, par exemple, le Groupe des cinq, mais il y a des comportements répréhensibles. Comment faisons-nous pour les obliger à rendre des comptes?

● (0935)

M. John de Boer: C'est une question complexe, évidemment, et beaucoup de choses sortent de mon champ d'expertise, mais lorsqu'il s'agit de se protéger, par exemple, contre l'espionnage ou les comportements malveillants qui tentent de siphonner ou de saboter la propriété intellectuelle et l'ensemble du processus de recherche et de développement, il y a, à mon avis, quelques points vulnérables qu'il faut régler immédiatement.

Premièrement, des entreprises comme BlackBerry, mais pas seulement BlackBerry, travaillent en étroite collaboration avec les universités, les instituts de recherche et les petites et moyennes entreprises du Canada pour créer de nouveaux produits, de nouvelles propriétés intellectuelles, tout au long de la chaîne d'approvisionnement. Les garanties de sécurité requises ne sont pas toujours en place. Nous devons veiller à ce que la sécurité, la protection de la propriété intellectuelle au fur et à mesure que nous la développons, soit aussi importante que le développement lui-même. En fait, elle devrait être considérée comme un bien national. En ce qui concerne les universités, je sais que le Service canadien du renseignement de sécurité commence à promouvoir des programmes de sensibilisation à la sécurité au sein des laboratoires de recherche universitaires en vue de la protection de la propriété intellectuelle. Nous devons agir de la même manière avec les PME qui travaillent sur la propriété intellectuelle, alors s'il y a une recommandation que je peux faire...

Le Bureau d'assurance du Canada a réalisé l'an dernier une enquête auprès des PME pour savoir si elles avaient investi dans la cybersécurité. L'année dernière, 47 % d'entre elles n'avaient rien investi dans la cybersécurité. Nous savons que les PME sont essentielles à la création de propriétés intellectuelles. Nous devons faire quelque chose pour les inciter à protéger leur propriété intellectuelle. Elles n'investissent pas dans ce domaine, principalement, semble-t-il, en raison du coût. C'est un choix. Je crois qu'en tant que gouvernement et en tant que société, nous devons changer d'optique et commencer à inciter à l'inclusion de la sécurité dans ce processus.

La dernière chose que je mentionnerai est qu'il y a deux ans, Innovation, Sciences et Développement économique Canada a lancé un programme fantastique, en théorie, appelé le plan canadien d'adoption du numérique. L'idée était d'accroître l'utilisation des technologies numériques par les PME. La cybersécurité n'en faisait pas partie au départ. Nous avons travaillé avec ISDE par la suite pour l'inclure dans l'évaluation, mais ce type de programme doit intégrer la cybersécurité comme un élément fondamental de ses opérations.

Le président: Merci, monsieur Sousa. Il vous reste huit secondes et vous ne les aurez pas.

Des voix: Oh, oh!

M. Charles Sousa: Merci beaucoup, monsieur le président.

Le président: Madame Normandin, vous disposez de deux minutes et demie.

[*Français*]

Mme Christine Normandin: Merci beaucoup.

J'aimerais maintenant poser des questions à M. McSorley.

Vous avez fait état de plusieurs situations, qui touchent notamment le Centre de la sécurité des télécommunications, ou CST, et qui posent des enjeux quant à la protection de la vie privée.

Comme je suis complètement inculte en la matière, j'aimerais savoir de quelle façon vous obtenez ces informations sur les activités du CST, tel le suivi de connexion WiFi dans les aéroports, dont vous avez fait mention.

Ces informations sont-elles diffusées par le CST ou s'agit-il d'informations que vous collectez autrement sur les activités du CST?

M. Tim McSorley: Merci beaucoup de cette question.

● (0940)

[*Traduction*]

Nous recueillons ce genre de renseignements de multiples façons.

Pour certains d'entre eux, avant la création du commissaire au renseignement, il y avait le commissaire du CST, qui a lancé l'examen, et ce sont les organismes d'examen et de surveillance indépendants qui ont souvent accès à ces renseignements et qui les partagent, bien qu'ils soient toujours expurgés d'une manière qui protège la sécurité nationale, lorsqu'il y a des préoccupations. Parfois, ces renseignements sont encore difficiles à interpréter en raison des expurgations, des euphémismes et du langage. Souvent, cela dépend des demandes d'accès à l'information. Les chercheurs universitaires et nos propres recherches demandent et dépouillent des documents pour tenter de trouver des renseignements.

En ce qui concerne la question du WiFi dans les aéroports, nous nous sommes appuyés à la fois sur le commissaire et sur les journalistes qui ont découvert l'information et l'ont rendue publique, et ensuite, l'une des choses qui, à mon avis, pourrait...

Le président: Monsieur, excusez-moi.

Monsieur Sousa, pouvez-vous éteindre votre microphone, s'il vous plaît?

Bien, continuez.

M. Tim McSorley: L'une des raisons pour lesquelles j'ai l'accès à l'information que j'ai aujourd'hui est le procès intenté par la BC Civil Liberties Association qui a abouti à la divulgation. L'association a ensuite dû se battre pour partager publiquement les renseignements qu'elle avait obtenus, et ce n'est que récemment qu'elle a pu les publier.

Je suppose que ce qui relie tout cela, c'est que l'information ne provient pas du CST lui-même. Elle provient d'organismes extérieurs — de chercheurs, de comités d'examen et de poursuites judiciaires — et il ne devrait pas en être ainsi.

[*Français*]

Mme Christine Normandin: Justement, j'aimerais obtenir d'autres commentaires. Vous avez parlé de l'importance de la reddition de comptes et de la transparence.

Avez-vous des recommandations à faire qui permettraient plus de reddition de compte et de transparence?

[*Traduction*]

M. Tim McSorley: Oui, certainement.

L'une des choses que nous avons constatées en ce qui concerne le commissaire au renseignement et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, c'est qu'ils ne reçoivent pas les renseignements dont ils ont besoin pour faire leur travail d'examen et, dans le cas du commissaire au renseignement, leur travail de surveillance. Nous pensons qu'il faut modifier la Loi sur le Centre de la sécurité des télécommunications pour subordonner l'autorisation de leurs diverses activités à la fourniture de renseignements adéquats et appropriés au commissaire au renseignement, et examiner l'idée de donner au commissaire au renseignement le pouvoir d'apporter des modifications contraignantes aux autorisations demandées par le CST...

Le président: Malheureusement, nous allons devoir en rester là. Il semble que chaque fois que nous abordons vos recommandations, je dois vous interrompre. Je suis sûr que nous allons les entendre dans le courant de l'heure.

Madame Mathyssen, vous avez deux minutes et 45 secondes.

Mme Lindsay Mathyssen: Avec ces 15 secondes supplémentaires, je voudrais simplement remercier M. McSorley pour toutes ces recommandations. J'espère que vous les soumettrez au greffier, si vous voulez bien, pour que cela fasse partie de notre dossier et de notre étude.

Au sein de ce comité, de nombreux témoins ont parlé des silos du renseignement et de la nécessité pour les agences de renseignement canadiennes de s'intégrer davantage pour un meilleur partage du renseignement, mais lorsqu'on parle, par exemple, du partage par l'Agence du revenu du Canada avec le SCRS ou du partage avec le CST, on s'inquiète du fait que nous avons vu la discrimination jouer un rôle dans les enquêtes sur les organisations caritatives musulmanes, par exemple.

Monsieur McSorley, pourriez-vous nous parler des dangers que pose cette intégration plus poussée et de ce que nous pouvons faire pour éviter d'aller trop loin sur le plan de la discrimination et de la victimisation de certaines organisations tout à fait légitimes?

M. Tim McSorley: Merci beaucoup pour cette question.

Tout d'abord, il est clair, comme vous l'avez dit, qu'une collaboration est nécessaire entre les agences de sécurité nationale. Une partie de cette collaboration nécessite le partage de renseignements.

Toutefois, comme vous l'avez souligné, nous avons constaté que la manière dont certains de ces renseignements sont partagés et l'impact qu'ils peuvent avoir suscitent de vives inquiétudes.

Par exemple, la BC Civil Liberties Association a constaté dans ses recherches que le CST partageait des renseignements avec l'ARC afin de soutenir ses efforts de lutte contre le financement du terrorisme. Cependant, nos recherches nous ont permis de constater que l'ARC, dans le cadre de ses efforts de lutte contre le financement du terrorisme, a adopté une approche fondée sur les préjugés à l'égard des organisations caritatives musulmanes au Canada. Elle est partie de l'idée qu'en raison des menaces terroristes émanant d'organisations liées aux musulmans, la communauté musulmane doit faire l'objet de davantage de soupçons. Cela se traduit par une surveillance accrue, une collecte et un partage d'information plus importants et des répercussions plus graves que pour les autres communautés du Canada.

Ce qui nous ramène à l'étude en question, c'est que les renseignements échangés ne sont pas connus publiquement par l'organisation contre laquelle ils sont utilisés, de sorte que celle-ci n'a pas la possibilité de les contester. Cela se reflète également, par exemple, dans le projet de loi C-26, où il y a, à notre avis, une quantité excessive de secrets et la possibilité d'utiliser des renseignements et de cacher des renseignements aux entreprises d'infrastructure essentielle qui fournissent des services de télécommunication aux Canadiens si elles tentaient, par exemple, d'interjeter appel ou de contester un arrêté pris par le ministre.

● (0945)

Le président: Malheureusement, nous allons devoir en rester là, monsieur McSorley, encore une fois.

Madame Kramp-Neuman, allez-y pour cinq minutes, s'il vous plaît.

Mme Shelby Kramp-Neuman (Hastings—Lennox and Addington, PCC): Merci et bonjour.

J'aimerais poser mes questions à M. Nared ce matin.

Un document d'information que votre organisation a fourni à un comité précédent de la Chambre indiquait que les préoccupations soulevées par d'autres observateurs étaient toujours valables. En fait, l'organisation a fait référence en particulier à un article écrit par Alexander Rudolf, qui a comparu devant ce comité au début de l'année. Dans cet article, il déclarait:

> Le Canada a besoin à la fois d'une réponse pangouvernementale en matière de cybersécurité et d'une réponse très ciblée en matière de cyberdéfense.

En outre, dans un document fourni au Comité l'année dernière, il est cité que l'auteur souhaite réitérer cela:

> Les Forces armées canadiennes ne sont pas prêtes à faire face aux cybermenaces, même modérées (comme les hacktivistes). Et compte tenu des renseignements auxquels le public a accès et des menaces émergentes, elles ne seront pas prêtes à relever les défis modernes de la cybernétique dans un avenir prévisible.

Pourriez-vous développer ce point? Partagez-vous toujours ce point de vue?

M. Tadej Nared: Merci pour votre question.

Oui, je partage toujours ce point de vue, car je pense qu'un an s'est écoulé depuis ce document. Je crois avoir écrit que le problème fondamental est que l'environnement de la menace a été précisé uniquement là où les Forces armées canadiennes sont stationnées au Canada et à l'étranger. Cela représente un échec dans la compréhension de l'environnement de la cybersécurité en général. Il n'existe plus de périmètre de défense. Non seulement les FAC et leurs membres, mais aussi les membres de leurs familles sont des cibles pour un agresseur modéré, un pirate informatique de type « black hat » ou surtout une sorte de groupe comme le groupe russe Sandworm. Ils ne s'attaqueront pas en particulier à des cibles dures et sûres, mais plutôt aux cibles faciles. Cela signifie qu'ils s'attaquent même à des membres de la famille, par exemple, en compromettant leurs réseaux domestiques et en se propageant à partir de là. Nous avons connu un cas semblable en Slovénie, où notre réponse d'urgence a été neutralisée de la même manière. C'était un échec de la pensée stratégique.

Je ne sais pas si ce programme a changé au cours de l'année écoulée. Si ce n'est pas le cas, il devrait être mis à jour et amélioré.

J'espère avoir répondu à votre question.

Mme Shelby Kramp-Neuman: Tout à fait. Cela m'amène à ma question suivante.

Vous avez également été cité en disant que le génie est sorti de la bouteille en ce qui concerne la cyberguerre et que la troisième guerre mondiale cybernétique bat déjà son plein.

De nombreux observateurs ont souligné l'existence d'un déficit important de cybercompétences dans notre secteur civil.

Pouvez-vous nous en dire plus et partager avec le Comité ce que cela signifie pour les Forces armées canadiennes, qui sont actuellement confrontées à une crise de recrutement et de rétention au sein de leur toute nouvelle division des cyberopérations?

M. Tadej Nared: Merci pour cette question.

Pour vous donner un exemple, comme l'a montré l'expérience ukrainienne, une guerre ne peut être gagnée sans le soutien de la population autochtone. Je pense que c'est un terme qui colle à la réalité. Il en va de même dans le domaine de la cybersécurité. Les pays occidentaux en particulier, les Amériques, comptent en quelque sorte sur leur océan pour se défendre, et sur des dépenses excessives pour se défendre également, mais ce n'est pas un concept sur lequel on peut compter sur le plan de la cyberguerre. À mon avis, la voie à suivre consiste à s'appuyer sur les renseignements provenant de la population, à faire appel à tous ceux qui peuvent aider et à organiser des initiatives. En circuit fermé, on ne résoudra aucun problème.

● (0950)

Mme Shelby Kramp-Neuman: Merci.

Puis-je vous laisser le reste de votre temps pour...

Allez-y.

M. Tadej Nared: Si vous le permettez, j'aimerais prendre une minute pour expliquer les cyberdommages dont j'ai parlé tout à l'heure, parce que cela se rapporte un peu à ce dont on parle.

Par exemple, le programme du F-35, dont le développement a coûté 1 700 milliards de dollars en recherche et développement, a été piraté par les Chinois et tous les plans ont été volés. Il ne s'agit là que d'un seul piratage. Si nous combinons tous les éléments, nous obtenons une image plus claire de l'origine des dommages. Cela concerne l'armée, l'armée de l'air et pratiquement tous les aspects de la société moderne.

Le président: Malheureusement, nous allons devoir en rester là. C'est un point plutôt malheureux.

Madame O'Connell, vous avez cinq minutes.

Mme Jennifer O'Connell (Pickering—Uxbridge, Lib.): Merci beaucoup.

Merci à tous nos témoins d'être ici aujourd'hui.

Monsieur de Boer, vous avez parlé de la déclaration obligatoire et d'autres choses du genre, mais j'aimerais aussi aborder certains des problèmes que nous avons entendus dans d'autres témoignages, à savoir que le secteur privé ne veut pas nécessairement dire s'il a été piraté ou si ses systèmes sont vulnérables. Je pourrais certainement imaginer que BlackBerry, par exemple, qui a une réputation en matière de sécurité, n'a jamais été victime d'une intrusion: le conseil d'administration ou la direction de l'entreprise ne voudra pas forcément faire savoir qu'il y a eu intrusion ou qu'une attaque a réussi.

Comment le gouvernement s'associe-t-il pour comprendre la situation réelle du secteur privé, en gardant à l'esprit que le secteur privé n'est pas forcément intéressé par le partage de ces renseignements?

M. John de Boer: Merci pour cette question.

Il est très important de garantir la confidentialité de l'information qu'une entreprise transmet au gouvernement. Les protections en matière de responsabilité et toutes ces choses doivent être prises en considération. À l'heure actuelle, cette confiance n'est pas encore totalement établie.

L'un des moyens d'y parvenir est, par exemple, ce que font le Royaume-Uni et les États-Unis, à savoir la mise en place d'un environnement de collaboration commun ou d'une collaboration commune en matière de cyberdéfense. Avant qu'un incident ne se produise, les voies de communication pour l'échange de renseignements et l'échange de renseignements sur les menaces se font volontairement, ce qui permet souvent au secteur privé de mieux comprendre comment les renseignements qu'il fournit sont effectivement utilisés et circulent. Il s'agit alors d'un véritable partenariat entre le secteur privé et le secteur public. À l'heure actuelle, je pense que les régulateurs et autres hésitent à s'engager, mais nous reconnaissons tous, à mon avis, qu'un partenariat public-privé plus étroit est indispensable.

Mme Jennifer O'Connell: Merci.

Cette précision est importante, car lorsque j'entends l'expression « déclaration obligatoire », je ne pense pas nécessairement qu'il s'agit d'une déclaration confidentielle. D'autres témoins nous ont dit qu'il s'agirait d'une déclaration obligatoire publique pour que les Canadiens aient une idée plus large, mais je pense que cette distinction, au moins de ce point de vue, est intéressante.

Je pense qu'il incombe également aux particuliers et aux entreprises de protéger leur sécurité. Vous avez mentionné dans votre témoignage que votre organisation a pour politique de savoir d'où vient chaque composant du produit, mais lorsque les entreprises ont des conseils d'administration et des actionnaires et que la rentabilité est importante, ce n'est peut-être pas le cas. Quelle serait votre recommandation pour que le public soit plus conscient de ce qu'il achète — c'est à lui qu'incombe cette responsabilité — et que peut faire le gouvernement pour encourager le secteur privé à ne pas toujours tenir compte uniquement des résultats financiers, mais aussi de la cybersécurité?

M. John de Boer: L'un des principaux moteurs de la sécurité, en particulier dans le secteur automobile, a été l'accent mis sur la sécurité, n'est-ce pas? Lorsque les consommateurs commencent à exiger de la sécurité, les choses changent. J'ai parlé tout à l'heure de la nomenclature d'un logiciel ou de la liste des ingrédients. Lorsque nous achetons des produits à l'épicerie, nous savons exactement... Il y a une liste d'ingrédients. Ils sont énumérés, n'est-ce pas?

Il pourrait y avoir, et il y a des débats dans plusieurs sphères sur, par exemple, une cote de cybersécurité pour les produits de l'Internet des objets, qu'il s'agisse de votre réfrigérateur ou d'un autre appareil. Cela pourrait être envisagé. On pourrait envisager de sensibiliser davantage le public à la question de savoir si un produit est plus sûr qu'un autre pour la consommation publique. Je pense que ce sont des mesures importantes, non seulement pour sensibiliser, mais aussi pour inciter les producteurs à intégrer la sécurité dès le départ, car ce n'est pas le cas aujourd'hui.

● (0955)

Mme Jennifer O'Connell: Ai-je encore du temps?

Le président: Non. Merci, madame O'Connell. Je vais vous arrêter. Vous aviez trois secondes.

Chers collègues, j'ai besoin de conseils. Nous avons dépassé notre heure.

Tout d'abord, je me tourne vers le greffier pour savoir si nous connaissons l'heure d'arrivée de nos amis.

Non? Bien.

J'ai quelques points de travaux du Comité que j'aimerais traiter à huis clos. Nous avions prévu que nos amis arriveraient à 10 h 15. Cela nous laisse 20 minutes. Il nous faudra quelques minutes pour passer à huis clos. Mon idée, étant donné l'excellence de ce panel, est de faire un tour de table de deux minutes avec chaque parti. Il y a des choses qui pourraient être intéressantes. Est-ce une idée acceptable, deux minutes?

Des députés: D'accord.

Le président: Nous allons maintenant...

Mme Cheryl Gallant: Allons-nous d'abord à huis clos?

Des voix: Non.

Le président: Ce sera les conservateurs, les libéraux, les bloquistes et les néo-démocrates, puis nous arrêterons. Les tours durent deux minutes.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Monsieur le président, avant que vous ne fassiez démarrer mon chronomètre, j'aimerais donner avis de la motion suivante.

> Que le comité entreprenne une étude d'au moins huit (8) réunions pour examiner comment l'état de préparation des Forces armées canadiennes est affecté par les processus d'approvisionnement du Canada et les capacités de notre industrie de la défense pour s'assurer que les besoins de l'armée canadienne sont satisfaits. Et que le ministère de la Défense nationale, les Forces armées canadiennes, Services publics et Approvisionnement Canada, le Bureau de la vérificatrice générale, le directeur parlementaire du budget, le Conseil du Trésor, l'industrie de la défense, les experts en approvisionnement militaire et les universitaires soient invités à témoigner devant le comité à ce sujet; et que le comité fait un rapport de ses conclusions et de ses recommandations à la Chambre.

Nous disposons de ce document dans les deux langues officielles et nous le ferons circuler.

Je vais commencer mon tour de questions éclair.

Tout d'abord, je tiens à remercier tous les témoins d'être ici.

Le gouvernement a proposé le projet de loi C-26 pour encourager l'industrie à se doter d'une défense plus solide en matière de cybersécurité. De nombreuses préoccupations ont été exprimées quant au caractère trop normatif et brutal des amendes et des pénalités pour les particuliers et les entreprises, alors que ces mêmes types d'amendes et de pénalités ne s'appliquent pas au gouvernement lui-même.

J'aimerais connaître l'avis de M. de Boer en particulier, car il représente ici une industrie canadienne. Mon téléphone BlackBerry d'autrefois me manque.

Qui est responsable de la protection des infrastructures critiques, y compris dans le secteur privé? Est-ce les Forces armées canadiennes, le ministère de la Défense nationale, le CST ou le gouvernement du Canada dans son ensemble, ou vaut-il mieux que cela vienne des entreprises individuelles? Vous pouvez également aborder la question des personnes disponibles, car le Conseil canadien des affaires affirme qu'il y a actuellement 25 000 postes non pourvus dans le domaine de la cybersécurité.

Le président: Vous avez un peu moins d'une minute.

M. John de Boer: Qui est responsable? Ce n'est pas clair. Cela faisait partie de mon témoignage. Nous devons éclaircir les rôles et les responsabilités, et cette clarté n'existe pas à l'heure actuelle. Il n'y a pas d'unité d'action.

Le projet de loi C-26 est un début important. Nous sommes en retard en ce qui concerne la déclaration obligatoire des cyberincidents dans les infrastructures critiques, et nous saluons donc cette initiative. Toutefois, elle se limite à quatre secteurs.

En réalité, de nombreuses mesures politiques sont prises en ce moment même. La stratégie sur les infrastructures critiques est en cours de renouvellement. Elle a été rédigée en 2009. Le cyberespace n'y est même pas mentionné. Il y a ensuite la stratégie nationale de cybersécurité et le projet de loi C-26. Tous ces éléments doivent être réunis.

● (1000)

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

Qui parle au nom des libéraux?

Monsieur Fisher, vous avez deux minutes.

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

Merci à tous d'être venus. Votre témoignage aujourd'hui est précieux.

J'ai déjà posé cette question. J'aimerais savoir ce que vous en pensez: comment le Canada peut-il mieux s'associer au secteur privé pour relever la barre de la cybersécurité dans tout le pays?

Hier, j'ai lu un article de la CBC sur Halifax Water. La cybersécurité de l'entreprise a été mise à l'épreuve. Des courriels ont été envoyés à 55 personnes, et 45 d'entre elles ont répondu. Elles ont cliqué sur le lien et envoyé tous leurs renseignements.

Nous parlons de déclaration obligatoire. Nous parlons de l'importance des infrastructures critiques. Lorsque nous pensons à des infrastructures comme Halifax Water et aux services publics de tout le pays en ce qui concerne la déclaration obligatoire et l'affûtage de leurs crayons de cybersécurité, j'aimerais savoir ce que vous en pensez.

Nous allons commencer par vous, monsieur de Boer, puis nous passerons peut-être à M. McSorley dans le peu de temps dont nous disposons.

M. John de Boer: Très rapidement, si des outils de cybersécurité pilotés par l'intelligence artificielle avaient été utilisés sur le Colonial Pipeline, notre modèle de 2015 aurait arrêté cela. Il faut utiliser les technologies de pointe. Elles peuvent aider à résoudre les problèmes de personnel et à protéger les infrastructures critiques.

M. Darren Fisher: Allez-y, monsieur McSorley.

M. Tim McSorley: Je vous remercie.

Je vais mentionner un autre projet de loi.

Le gouvernement examine actuellement la loi sur l'intelligence artificielle et les données. Je suis d'accord avec M. de Boer pour dire que nous devons envisager des solutions innovantes, y compris l'intelligence artificielle, mais nous devons également veiller à mettre en place des règlements. Le secteur privé et la société civile sont très inquiets. Le contenu actuel de la loi sur l'IA et les données pose des problèmes.

M. Darren Fisher: Je vous remercie.

Le président: Je vous remercie.

Madame Normandin, vous avez deux minutes.

[*Français*]

Mme Christine Normandin: Merci beaucoup.

Mes questions sont un peu en lien avec celles de M. Bezan.

Monsieur de Boer, vous avez mentionné qu'il y a un enjeu de clarté dans les rôles. Vous avez parlé du fait qu'aux États-Unis et en Australie, il y a des ministres de la cybersécurité. Un témoin dont je me souviens, M. Christian Leuprecht, mentionnait que le Danemark avait un ambassadeur en cybersécurité.

À quoi pourrait ressembler un poste unifié, ici? Avez-vous des recommandations à nous faire? Quelles caractéristiques seraient intéressantes?

[*Traduction*]

M. John de Boer: Le rôle principal d'une telle personne — qui pourrait être un secrétaire parlementaire — serait, tout d'abord, de signaler à tous les Canadiens que la cybersécurité est importante. Deuxièmement, cette personne serait chargée d'assurer la cohérence des politiques et des programmes dans l'ensemble du Canada. À l'heure actuelle, cela n'existe pas.

J'ai mentionné le cas de l'Australie, mais le Royaume-Uni dispose également d'un secrétaire parlementaire chargé de la cybersécurité. Nous avions auparavant un secrétaire parlementaire chargé du numérique. Ce n'est plus le cas.

Le rôle du secrétaire parlementaire serait d'examiner l'ensemble du gouvernement du Canada afin d'assurer la cohérence et l'unité des efforts et d'unifier notre approche de défense du pays.

[*Français*]

Mme Christine Normandin: Monsieur McSorley, souhaitez-vous ajouter quelque chose?

[*Traduction*]

M. Tim McSorley: Oui.

Je voudrais juste dire que je pense que nous avons besoin d'un bureau centralisé pour la cybersécurité. L'une des questions que nous nous posons au sujet du projet de loi C-26 est qu'il n'est pas clair si cela relèverait des organes d'examen de la sécurité nationale existants. Il serait également important de disposer d'un organisme chargé non seulement de veiller à ce que la cybersécurité soit gérée correctement, mais aussi à ce qu'elle fasse l'objet d'un examen et d'une reddition de comptes, et à ce qu'elle soit transparente.

Le président: Merci, madame Normandin.

Madame Mathyssen, vous avez les deux dernières minutes.

Mme Lindsay Mathyssen: Dans ce comité, nous avons beaucoup entendu parler de la surclassification de l'information et du fait que 90 % de ce que les Canadiens classifient n'a pas besoin de l'être.

Monsieur McSorley, en quoi cette surclassification des renseignements crée-t-elle un obstacle ou des problèmes pour les organisations de défense des droits civils lorsqu'il s'agit de demander des comptes à ces agences de renseignement? Quelle est votre solution à ce problème?

M. Tim McSorley: Merci beaucoup pour cette question.

Ce n'est pas seulement une préoccupation des groupes de défense des libertés civiles et de la société civile, mais de nombreux secteurs au Canada, qui estiment qu'il faut instaurer un climat de confiance. Il faut de l'ouverture et de la transparence pour que nous comprenions ce que font les agences canadiennes, y compris le CST, lorsqu'elles s'engagent à protéger la cybersécurité du Canada, à mener des cyberopérations actives et défensives et à faire du renseignement d'origine électromagnétique.

Le moyen de s'en assurer est d'imposer davantage de déclarations obligatoires sur les activités qu'elles mènent. Par exemple, le projet de loi C-26 ne prévoit pas de déclarations obligatoires à l'heure actuelle, de sorte qu'il serait très difficile de suivre non seulement la façon dont il est utilisé, mais aussi de déterminer s'il y a des défaillances afin d'améliorer le système. Le contrôle et l'examen ne consistent pas seulement à mettre les organisations sur la défensive et à les dénoncer, mais aussi à voir comment nous pouvons tirer des leçons de nos erreurs et améliorer les opérations.

À l'heure actuelle, il y a le commissaire au renseignement et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, et, comme je l'ai mentionné, il n'est pas évident qu'ils aient un rôle à jouer dans l'examen des opérations de cybersécurité du Canada, parce qu'elles touchent à la sécurité nationale, mais pas forcément de la manière dont ces organismes l'examinent toujours. Par conséquent, nous pensons qu'il faut soit créer un nouveau poste, soit modifier leur mandat pour bien préciser qu'elles ont ce mandat.

● (1005)

Le président: Merci, madame Mathyssen.

Monsieur Nared, j'ai vu que vous aviez la main levée. Il est désavantageux d'être virtuel quand tout le monde est physiquement présent, alors permettez-moi de vous donner une minute ou deux pour faire votre observation.

M. Tadej Nared: Merci beaucoup, monsieur le président. Je serai très rapide.

Une idée pour améliorer rapidement la cybersécurité est de responsabiliser l'ensemble du secteur des technologies de l'information, c'est-à-dire les fournisseurs de logiciels et de matériel, parce qu'à l'heure actuelle, ils jouissent d'un statut tout à fait unique par rapport aux autres secteurs d'activité.

Par exemple, si vous avez une voiture et que les freins fonctionnent mal ou quelque chose comme ça, ils seraient tenus pour responsables. Cependant, dans le secteur des technologies de l'information, de tels scénarios ne sont jamais pris en compte — ils ne le sont pas, et ils devraient l'être. Ils ne devraient pas simplement mettre sur le marché des produits qui ne sont pas prêts à être commercialisés et qui ne sont pas sûrs, et nous mettre tous en danger à cause de cela.

Je vous remercie de votre attention.

Le président: Merci, monsieur Nared.

Je tiens à remercier tous les témoins. Il me semble que nous aurions pu facilement poursuivre cette conversation jusqu'à la fin de la journée. Personnellement et au nom du Comité, je tiens à vous remercier de votre présence. C'est un sujet extraordinairement difficile à apprivoiser, en particulier pour ceux d'entre nous qui n'y sont pas confrontés quotidiennement et qui n'en comprennent pas nécessairement les nuances.

Sur ce, je vous remercie.

Nous allons suspendre la séance, passer à huis clos et poursuivre les travaux du Comité.

Monsieur McSorley, si vous n'avez pas reçu toutes vos recommandations, veuillez coordonner cela avec le greffier.

Monsieur Nared, je pense que le greffier communiquera avec vous à une date ultérieure.

Je vous remercie à nouveau.

La séance est suspendue.

[*La séance se poursuit à huis clos.*]