CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 101 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 22 mars 2018

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le jeudi 22 mars 2018

● (1100)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Commençons.

Nous en sommes à la 101e séance du Comité permanent de la sécurité publique et nationale. Nous accueillons ce matin l'honorable Harjit Sajjan, ministre de la Défense nationale.

Bienvenue à notre comité, monsieur le ministre. Vous semblez vous retrouver parmi de nombreux vieux amis. Sur ce, je vous invite à faire votre déclaration liminaire.

L'hon. Harjit S. Sajjan (ministre de la Défense nationale): Merci, monsieur le président.

En réalité, j'ai eu un peu de déjà-vu étant donné que je comparaissais ce matin devant le Comité de la défense et que je revois la plupart des mêmes visages ici. Je suis heureux de tous vous revoir.

J'aimerais commencer par vous remercier tous du travail extraordinaire que vous avez accompli dans le cadre de votre étude du projet de loi C-59. Ces discussions et les experts avec lesquels vous avez parlé ont contribué à l'élaboration de cet important projet de loi. Je vous remercie donc de tous vos efforts.

Je suis accompagné de Greta Bossenmaier, chef du Centre de la sécurité des communications, de Shelly Bruce, chef associée du CST, ainsi que de hauts fonctionnaires du CST, de la Défense nationale et des Forces armées canadiennes. Nous avons le plaisir de comparaître devant vous alors que vous poursuivez votre examen de la Loi de 2017 sur la sécurité nationale.

Cette loi démontre que notre gouvernement reconnaît que la poursuite de la sécurité nationale comporte deux objectifs indissociables, la protection des Canadiens et la défense de nos droits et libertés. Cet engagement est manifeste dans la troisième partie du projet de loi C-59, qui établirait une loi autonome pour le Centre de la sécurité des télécommunications.

En novembre dernier, j'ai eu l'occasion de parler à la Chambre des communes de la fière histoire du CST au service des Canadiens. Depuis plus de 70 ans, le CST est l'agence de renseignement électromagnétique étranger du Canada et la principale autorité fédérale en matière de sécurité des technologies de l'information au gouvernement du Canada. Au cours de sa longue histoire, le CST s'est adapté avec succès à des changements remarquables, notamment les progrès technologiques rapides et l'évolution du paysage mondial des menaces. Toutefois, ce qu'il faut maintenant, ce sont des autorités modernisées pour faire en sorte que le CST puisse continuer à s'adapter dans cet environnement en constante évolution, tant aujourd'hui que pour les 70 prochaines années.

Dans mes remarques ce matin, j'aimerais souligner l'importance de cette mesure législative pour faire en sorte que nos organismes de sécurité et de renseignement puissent suivre les menaces à la sécurité, tout en améliorant la reddition de comptes et la transparence.

Tout d'abord, la Loi sur le CST moderniserait le mandat du CST en matière de renseignement étranger en lui permettant d'utiliser de nouvelles techniques pour acquérir des renseignements grâce à l'infrastructure mondiale de l'information. Le programme de renseignement électromagnétique étranger du CST est essentiel pour informer le gouvernement en matière de questions de sécurité nationale, de défense nationale et d'affaires internationales. Les changements proposés permettront au CST de continuer à recueillir ces renseignements vitaux.

Ensuite, en tant que centre d'excellence du Canada en matière de cyberopérations, le CST se doit d'être à l'avant-garde des changements technologiques. La loi renforcerait donc le mandat du CST en matière de cybersécurité et de protection de l'information. Elle améliorerait notamment la capacité du CST de défendre les importants réseaux canadiens non gouvernementaux et d'échanger des renseignements sur les menaces et de formuler des conseils en matière d'atténuation. Ces deux mesures prises ensemble permettraient à la Loi sur le CST de renforcer les cyberdéfenses du Canada en protégeant mieux les informations les plus sensibles des Canadiens et d'empêcher que d'importants réseaux cybernétiques ne soient compromis.

Enfin, et c'est là un point particulièrement d'intérêt pour la Défense nationale, le mandat du CST en matière technique et opérationnelle préciserait que ce dernier est bien autorisé à fournir de l'aide aux Forces armées canadiennes et au ministère de la Défense nationale. Le CST pourrait ainsi mieux soutenir les missions militaires menées par le Canada à l'étranger de même que les braves hommes et femmes des Forces armées canadiennes qui servent dans les théâtres d'opération.

Bien entendu, le CST fournit déjà des renseignements importants aux Forces armées canadiennes conformément à son mandat en matière de renseignement étranger. La loi permettrait au CST de faire plus pour les aider, entre autres, de mener des cyberopérations actives en soutien des missions militaires autorisées par le gouvernement. Le projet de loi C-59 permettrait au CST et aux Forces armées canadiennes de mieux coopérer afin de garantir la meilleure utilisation des outils et des capacités qui soit et d'atteindre nos objectifs de mission.

Le ministère de la Défense nationale et les Forces armées canadiennes sont impatients de collaborer plus étroitement avec le CST afin de mieux pouvoir tirer parti de ses capacités et de son expertise, tel qu'il est mentionné dans la nouvelle politique de défense du Canada, « Protection, Sécurité, Engagement ».

Je tiens également à parler d'un élément crucial de la Loi sur le CST proposée: les cyberopérations à l'étranger. Je sais que lors de sa comparution devant le Comité le mois dernier, Shelly Bruce, chef associée du CST, vous a parlé des cyberopérations actives et de ce à quoi celles-ci ressembleraient dans la pratique. Mais je tiens à réitérer de nouveau aujourd'hui l'importance de ces opérations et en quoi elles sont nécessaires pour protéger la sécurité des Canadiens.

Le mandat du CST en matière de cyberopérations à l'étranger fournirait au Canada les moyens cybernétiques pour réagir aux menaces étrangères graves ou aux crises internationales dans le cadre d'une approche stratégique plus vaste.

Par exemple, le CST pourrait utiliser les cyberopérations actives pour empêcher le téléphone cellulaire d'un terroriste de détonner une bombe embarquée dans un véhicule, ou encore le CST pourrait nuire à la capacité de terroristes de communiquer entre eux en faisant obstacle à leur infrastructure de communications.

Les cyberopérations actives et défensives du CST cibleraient soigneusement, dans le respect de la loi, les activités de particuliers d'États, d'organisations ou de groupes terroristes étrangers ayant des répercussions sur les affaires internationales, la défense ou la sécurité du Canada. Les cyberopérations à l'étranger seraient assujetties à des interdictions légales strictes qui interdiraient de diriger des opérations contre des Canadiens, n'importe qui au Canada ou l'infrastructure globale de l'information au Canada et nécessiteraient un processus d'approbation rigoureux.

Cela m'amène à mon dernier point. Le présent projet de loi améliorerait considérablement la surveillance et l'examen de la communauté de la sécurité nationale et du renseignement au Canada, qui comprend le CST, le ministère de la Défense nationale et les Forces armées canadiennes.

Les dispositions relatives à la surveillance et à l'examen contenues dans la Loi sur la sécurité nationale démontrent l'engagement de notre gouvernement à améliorer la légalité et la transparence. Je suis impatient de travailler avec les nouveaux organismes proposés, notamment l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et le commissaire au renseignement.

En mettant à jour, en clarifiant et en énonçant clairement dans la loi ce que le CST est autorisé à faire, le projet de loi permettrait aux Canadiens de mieux comprendre ce que fait le CST pour protéger le Canada et les intérêts canadiens. En ajoutant de nouvelles mesures en matière de surveillance et de responsabilisation, la Loi sur la sécurité nationale devrait vous assurer, comme à tous les Canadiens, que des mesures sont en place pour garantir que le CST continue de respecter la loi et de protéger la vie privée des Canadiens.

Je tiens à dire aux membres du Comité que je suis très fier du projet de loi C-59. Il s'agit d'une mesure législative importante qui respecte la promesse de notre gouvernement de protéger les Canadiens et leurs droits et libertés.

Merci.

● (1105)

Le président: Merci, monsieur le ministre.

Avant de passer aux questions, je tiens à dire aux membres du Comité que j'ai adopté une interprétation assez généreuse de la pertinence lors de comparutions précédentes de ministres, en particulier au sujet du budget des dépenses et des budgets supplémentaires des dépenses. Je rappelle à tous les membres du Comité que nous sommes ici pour discuter du projet de loi C-59. J'espère donc que les membres du Comité lieront leurs questions d'une façon ou d'une autre au projet de loi C-59.

Sur ce, monsieur Picard, vous avez sept minutes.

[*Français*]

M. Michel Picard (Montarville, Lib.): Merci.

[*Traduction*]

Comme je pose mes questions en français, j'invite ceux et celles qui en ont besoin à prendre les écouteurs.

[*Français*]

Monsieur le ministre, c'est un plaisir de vous revoir ainsi que toute votre équipe. Bienvenue au Comité.

Je reviens d'une réunion de deux heures du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, où des représentants de l'Estonie nous ont parlé de cybergouvernance.

De toute évidence, au-delà de ce qu'on fait sur terre, en mer ou dans les airs, l'information devient le nouveau champ de bataille. Les mégadonnées deviennent une nouvelle cible et un nouveau terrain de jeu pour les conflits entre les pays.

Comment ces nouveaux pouvoirs accordés par le projet de loi C-59 vont-ils servir au CST?

[*Traduction*]

L'hon. Harjit S. Sajjan: Avec le projet de loi C-59, une des choses que nous avons commencé à aborder lorsque nous avons consulté les Canadiens, c'est de nous assurer de demeurer à la fine pointe de notre technologie. Toutefois, si nous sommes à la fine pointe de la technologie, nous devons nous assurer d'avoir la bonne loi pour pouvoir nous adapter aux méthodes utilisées. Le projet de loi C-59 permettra en fin de compte au CST de pouvoir protéger les Canadiens contre les menaces étrangères.

Il s'agit de quelque chose qui est très propre au projet de loi, parce que cela n'a jamais été fait auparavant. Il crée également une loi distincte sur le CST qui donne une orientation précise quant à ce que le CST peut faire, tout en mettant en place un mécanisme très rigoureux pour protéger la vie privée des Canadiens.

D'un point de vue policier, je pense que les Canadiens veulent aussi être protégés contre le vol d'identité eu égard à la façon dont ils font leurs opérations bancaires. Le CST a la capacité et les connaissances nécessaires pour aider les Canadiens en leur prodiguant les bons conseils. Il a déjà commencé à le faire dans le cadre de ses campagnes dans les médias sociaux.

Tel est l'objet du projet de loi; il s'agit de protéger les Canadiens et les intérêts canadiens.

● (1110)

[*Français*]

M. Michel Picard: Dans les discussions antérieures de ce comité, on nous a fait des commentaires sur la dimension offensive de certains pouvoirs ou de certaines capacités du CST. On n'est pas sans savoir que des groupes terroristes ou associés aux terroristes, par exemple Daech, bénéficient de réseaux informels de sympathisants, de structures et de communications en ligne. Cette nouvelle armada ou ce nouvel équipement à la disposition de ces groupes terroristes représente une menace additionnelle.

De quelle manière doit-on définir l'approche offensive du CST? De quelle manière cette approche offensive va-t-elle répondre à la nouvelle menace qui s'installe?

[*Traduction*]

L'hon. Harjit S. Sajjan: Un aspect en particulier qui est extrêmement important, puisque le ministre de la Défense nationale est également responsable de nos Forces armées canadiennes, c'est que le CST aura maintenant la capacité de fournir le bon soutien aux Forces armées canadiennes. De toute évidence, il a fourni le bon renseignement, mais maintenant, avec le projet de loi C-59, il peut fournir la bonne expertise. Il pourra tirer parti de ses connaissances et de ses technologies pour se tenir au courant de certains réseaux terroristes et de ce qu'ils essaient de faire, surtout pour assurer la sécurité de nos soldats. Comme je l'ai mentionné, cela comprend tout, depuis la détonation d'un engin explosif improvisé jusqu'à la perturbation du réseau pour l'empêcher d'atteindre ce point.

Nous devons aussi garder à l'esprit que même avec les meilleures technologies, nous avons dû attendre qu'une cyberattaque nous vise avant de pouvoir faire quoi que ce soit. Nous devons nous assurer d'avoir un mécanisme de défense proactif afin de pouvoir mettre fin à une menace avant qu'elle ne se produise. Ce sont là des éléments très importants pour nous assurer de protéger nos infrastructures de façon très proactive.

[*Français*]

M. Michel Picard: Vous parlez de l'appui du CST aux diverses opérations, qui ne sont pas que militaires. Cet appui est nécessaire en raison du désavantage lié à l'incapacité de répondre suffisamment rapidement à une attaque, c'est-à-dire le fait d'être obligé d'attendre que l'attaque ait lieu avant de pouvoir réagir. Cette nouvelle capacité va soutenir diverses opérations.

Cet appui deviendra-t-il un nouvel instrument pour mener des opérations militaires partout dans le monde? Poser la question, c'est un peu y répondre.

[*Traduction*]

L'hon. Harjit S. Sajjan: Surtout lorsqu'il s'agit de nos Forces armées canadiennes, cela donne en fin de compte au CST la capacité d'aider les Forces armées canadiennes de façon plus juste. Cela nous met également en rapport avec nos partenaires du Groupe des cinq. Soit que cet aspect a été négligé par le passé dans les lois antérieures... En réalité, j'ai trouvé assez étonnant que le CST n'ait pas la capacité législative d'aider les Forces armées canadiennes de cette façon. Grâce au projet de loi, les Forces armées canadiennes pourront tirer parti de l'expertise technique du CST.

[*Français*]

M. Michel Picard: Vous comparez nos capacités avec celles de nos partenaires du Groupe des cinq. Ces nouveaux pouvoirs nous permettront d'être au même niveau que nos partenaires à l'étranger, voire en avance, si notre technologie le permet. Par défaut, j'en déduis que nous avions un retard à combler, et ce projet de loi nous permet de le faire.

[*Traduction*]

L'hon. Harjit S. Sajjan: Greta, voulez-vous répondre?

Mme Greta Bossenmaier (chef, Centre de la sécurité des télécommunications): Merci, monsieur le ministre.

Merci, monsieur le président, et merci aux autres membres du Comité d'être ici ce matin.

Je pense que l'on peut dire sans se tromper que le Canada, ses alliés et les pays en général font face à un environnement de cybermenace très dynamique. La technologie a changé. Si vous vous rappelez l'époque où notre loi a été adoptée, il y a environ 17 ans, c'était avant que nous parlions de choses comme l'informatique en nuage et l'intelligence artificielle, l'environnement de cybermenace dynamique. Différents types d'acteurs ont été impliqués dans les types de menaces auxquelles nous sommes confrontés. Je pense qu'il est juste de dire que des pays de partout dans le monde, nos alliés et le Canada font tous face à cette nouvelle menace dynamique.

Comme le ministre l'a dit, il s'agit vraiment de mettre en place une loi qui nous permettra d'avoir le pouvoir d'agir et de protéger le Canada et les Canadiens dans ce nouvel espace.

À la question qui a été posée en particulier...

● (1115)

Le président: Malheureusement, nous allons devoir nous en tenir à cela et peut-être répondre dans le cadre d'une autre question. Le temps est écoulé.

[*Français*]

Monsieur Paul-Hus, vous avez la parole pour sept minutes.

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

Monsieur le ministre, je vous souhaite la bienvenue au Comité permanent de la sécurité publique et nationale.

Le projet de loi C-59 précise que vous devez collaborer avec la ministre des Affaires étrangères. Nous savons déjà que, en tant que ministre de la Défense nationale, vous entretenez des relations étroites avec la ministre des Affaires étrangères. De façon probablement hebdomadaire, vous devez discuter de plusieurs dossiers et du déploiement des Forces armées canadiennes dans le monde. Je me demande pourquoi il est nécessaire que le projet de loi vous oblige à communiquer avec la ministre, puisque cette collaboration fait déjà partie, je pense, de votre travail de tous les jours.

Il y a un problème que vous pourrez sûrement m'aider à comprendre, compte tenu de votre étroite collaboration avec la ministre des Affaires étrangères. C'est au sujet d'un bris de sécurité. Je ne sais pas comment cette expression sera traduite, mais, en tant qu'ancien militaire, vous devez savoir de quoi je parle. Cet événement est survenu en Inde: il s'agit de l'invitation envoyée à M. Jaspal Atwal. Nous entendons deux histoires contradictoires. Selon le premier ministre, M. Atwal a été invité par des représentants voyous du gouvernement indien. De son côté, votre collègue la ministre des Affaires étrangères a confirmé que l'invitation venait de représentants du gouvernement canadien. Nous avons donc deux versions, soit celle du premier ministre, à qui vous êtes redevable de votre poste, et celle de la ministre des Affaires étrangères, avec qui vous travaillez tous les jours.

Quelle version croyez-vous?

M. Michel Picard: Monsieur le président, j'invoque le Règlement.

Le président: Vous avez la parole, monsieur Picard.

M. Michel Picard: Je ne vois pas la pertinence de la question; elle ne porte pas sur la communication ou sur la fonction du CST.

[*Traduction*]

Le président: J'ai pensé que M. Paul-Hus était très astucieux dans la façon d'incorporer le projet de loi C-59 à cette question, mais je m'interroge sur la pertinence de sa question pour ce qui est de la relation de travail entre le ministre de la Défense nationale et le ministre des Affaires étrangères.

L'hon. Harjit S. Sajjan: Monsieur le président, je vais laisser la deuxième partie de la question pour la période des questions.

Vous soulevez un excellent point au sujet de l'importance de la participation du ministre des Affaires étrangères. Je pense qu'il est tout à fait prudent de le faire. Cela nous permet de nous assurer que lorsqu'il s'agit de menaces et de mesures éventuelles que nous, le gouvernement, pouvons prendre, il n'y a pas seulement un ministre qui intervient. Nous devons nous assurer d'examiner de façon prudente les menaces sous différents angles, en particulier le point de vue du ministre des Affaires étrangères.

Oui, nous entretenons des relations très harmonieuses, mais nous voulons nous assurer en même temps que nos relations sont extrêmement bonnes... Nous ne savons pas comment sont les relations. Nous ne pouvons pas compter là-dessus. Les Canadiens veulent s'assurer qu'il y a un bon processus en place et que, lorsque les gouvernements prennent des décisions de cette nature, ils ont le bon encadrement et que ces décisions ont bien été examinées lorsque nous prenons des mesures à l'étranger.

[*Français*]

M. Pierre Paul-Hus: Je comprends, monsieur le ministre, vous parlez régulièrement à la ministre des Affaires étrangères. La nécessité d'inscrire cette collaboration dans un projet de loi, c'est une chose. Toutefois, j'aimerais revenir sur l'événement survenu en Inde.

Vous étiez présent lors de ce voyage. Comment avez-vous perçu la situation? Savez-vous qui dit vrai? Es-ce le premier ministre ou la ministre des Affaires étrangères? Comme vous étiez présent, vous avez sûrement été témoin des événements et vous devez être en mesure de répondre à ma question.

[*Traduction*]

Le président: Vous pouvez commenter la relation, mais ce n'est peut-être pas...

L'hon. Harjit S. Sajjan: Pour ce qui est de la première partie de votre question — je vais y répondre une fois de plus —, il est absolument important de l'inscrire dans la loi pour que, comme dans ce cas-ci, lorsqu'un gouvernement intervient à l'étranger — en particulier lorsqu'il s'agit de ce tout nouveau domaine du cyberespace, dans lequel les technologies vont continuellement changer —, nous pouvons être certains d'avoir le bon encadrement à cet égard. Les Canadiens s'attendent à ce que nous le fassions.

En ma qualité de ministre de la Défense nationale, je ne participe pas à des opérations, même avec les militaires. C'est une décision qui est prise par le gouvernement. Le Cabinet me donne le pouvoir d'aller de l'avant, ce qui me permet, dans ce cas-ci, lorsqu'il s'agit du cyberespace... C'est faire preuve de grande prudence de s'assurer que nous travaillons avec le ministre des Affaires étrangères et que cela figure dans la loi. Les Canadiens s'attendent à ce que nous assurions, tout en les protégeant, une surveillance et une transparence adéquates dans l'avenir.

[*Français*]

M. Pierre Paul-Hus: Monsieur le président, comme le ministre ne peut pas répondre à ma question même s'il était présent en Inde et qu'il travaille en étroite collaboration avec la ministre des Affaires étrangères, j'aimerais déposer la motion suivante, que j'ai envoyée au Comité plus tôt cette semaine:

> Que, conformément à l'article 108(2) du Règlement, le Comité invite Daniel Jean, conseiller à la sécurité nationale du premier ministre, à lui offrir la même séance d'information qu'il a donnée aux journalistes le vendredi 23 février 2018 et que cette séance soit faite en public au plus tard le vendredi 30 mars 2018.

Je dépose cette motion parce que les conservateurs et les néo-démocrates membres du Comité se posent de sérieuses questions sur l'affaire Atwal qui s'est déroulée en Inde.

Le 23 février, le conseiller principal à la sécurité nationale du premier ministre a déclaré à des journalistes que les responsables de l'invitation envoyée à M. Atwal étaient des représentants de l'Inde. Cela a créé un incident diplomatique avec l'Inde. Le 27 février, le premier ministre a confirmé à la Chambre des communes ce que M. Jean avait dit. Ensuite, la ministre des Affaires étrangères a mentionné que l'invitation venait de représentants du Canada. Le député de Surrey-Center, M. Sarai, a confirmé que l'invitation venait de lui. M. Atwal a également confirmé que l'invitation venait de représentants du Canada, et non de l'Inde. Nous avons donc deux versions des faits actuellement.

Les parlementaires ont le droit de savoir ce qui s'est passé en Inde. Le breffage a été donné publiquement à des journalistes. Nous devrions être en mesure de recevoir ce breffage également. C'est pourquoi je pense que le Comité devrait accepter cette motion.

De plus, les membres libéraux du Comité peuvent voter de manière indépendante, en toute liberté de conscience. Lors de sa dernière comparution, le ministre de la Sécurité publique et de la Protection civile a confirmé qu'il ne relevait pas de ses responsabilités de donner des directives au Comité et que ses membres étaient autonomes. Si les membres libéraux votent contre la motion, nous pourrons considérer que c'est le bureau du premier ministre qui prend les décisions.

Nous avons besoin de faire la lumière là-dessus. Je crois que les députés du Parti libéral aimeraient également faire la lumière sur cet incident diplomatique grave pour le Canada.

● (1120)

[*Traduction*]

Le président: Merci, monsieur Paul-Hus.

Nous avons reçu la motion en temps opportun. Elle est recevable. Elle ressemble à votre motion précédente, que le Comité a rejetée, mais elle est suffisamment différente pour être recevable. Même si c'est le même sujet dont on discute à la Chambre en ce moment et que vous n'attendez pas l'issue du débat à la Chambre, elle est quand même recevable et rien n'empêche que l'on en débatte.

Sur ce, monsieur Picard, allez-y.

[*Français*]

M. Michel Picard: Je pense que toutes les questions diplomatiques méritent d'être prises très au sérieux. Par ailleurs, il s'agit également de l'objet du débat qui se tient aujourd'hui à la Chambre. Je pense qu'il faut attendre de savoir ce qui sera dit à la Chambre et laisser celle-ci aller au fond de la question, comme prévu.

Dans ces circonstances, je demande que le débat soit ajourné.

[*Traduction*]

M. Blaine Calkins (Red Deer—Lacombe, PCC): Pouvons-nous tenir un vote par appel nominal, s'il vous plaît, monsieur le président?

Le président: Je vois cela comme une motion dilatoire qui n'est pas sujette à débat; par conséquent, nous demandons le vote.

Je présume que vous voulez que le vote soit enregistré.

M. Blaine Calkins: Oui.

Le président: Sur ce, je vais demander au greffier de mettre la motion aux voix.

M. Michel Picard: Est-ce pour ajourner le débat, monsieur le président?

Un député: Il s'agit d'ajourner le débat sur la motion.

(La motion est adoptée par 5 voix contre 4.)

Le président: La motion est adoptée.

Sur ce, nous passons à M. Dubé.

Vous avez sept minutes.

M. Matthew Dubé (Beloeil—Chambly, NPD): Merci, monsieur le président.

Monsieur le ministre, je vous remercie d'être ici aujourd'hui et je remercie également toutes les personnes présentes.

Ma question — et vous l'avez mentionné dans vos commentaires — porte sur le partage des capacités entre le CST et les forces armées, en particulier en ce qui concerne les cyberopérations actives. On s'est inquiété de l'évolution du paysage auquel on a fait allusion et ce que cela signifie exactement pour une organisation civile quand vous parlez, plus particulièrement, d'États étrangers qui pourraient être impliqués dans certaines des activités à l'encontre desquelles les cyberopérations actives sont utilisées. On a l'impression qu'il y a là une pente glissante sur le plan du droit international, quant à ce qui est une action militaire et ce qui ne l'est pas.

Je me demande si vous pourriez nous en parler et peut-être nous expliquer comment ces capacités se conjuguent et comment nous nous assurons que le CST n'est pas une organisation civile engagée dans ce que d'autres États pourraient considérer comme des attaques militaires, d'autant plus que la notion de souveraineté est très nébuleuse à l'ère numérique en ce qui concerne le droit international.

L'hon. Harjit S. Sajjan: Je vais laisser Greta vous parler de l'aspect technique. Toutefois, je crois que je dois être clair à ce sujet. Au Canada, nous misons sur un répertoire d'une excellence phénoménale qui se trouve au CST. En ce qui concerne l'expertise que nous avons ici, nous, le gouvernement, et les gouvernements antérieurs, l'avons gardé là pour cette raison, nous assurer de rester à la fine pointe.

Grâce à la nouvelle loi, les Forces armées canadiennes pourront nous permettre de tirer parti de cette technologie. Toute intervention militaire, comme toute autre opération militaire, sera menée en vertu des bonnes procédures de ciblage, des bonnes règles d'engagement et conformément au droit international et, ce qui est encore plus important, à nos lois.

● (1125)

M. Matthew Dubé: Avant d'aborder l'aspect technique, j'aimerais préciser que le projet de loi exige que vous autorisiez, en consultation avec le ministre des Affaires étrangères, toute cyberopération active. Supposons qu'un État étranger qui participe à l'activité demande cette cyberopération active. Pouvez-vous nous expliquer comment vous décidez si les Forces armées devraient intervenir avec leur cybercapacité ou si c'est le CST, comme organisation civile?

L'hon. Harjit S. Sajjan: Faisons une distinction quant à savoir s'il s'agit d'une opération militaire qui fournit... Par exemple, nous sommes en Irak en ce moment. Nous devons examiner les menaces qui existent. Si une menace était en train de se doter d'une capacité de création d'un nouveau type d'engin explosif improvisé, le CST aurait la capacité de l'aider à vaincre ce type de technologie, et c'est ce qu'il ferait. Mais lorsqu'il est question de cyberopérations actives, il pourrait s'agir strictement parlant, par exemple, du fait que le gouvernement doit prendre des mesures pour protéger les Canadiens. C'est un élément distinct que le CST examinerait. Nous devons séparer les deux. Cela se fera dans le cadre d'un processus approprié, tel que le décrit le projet de loi, qui examinera la proportionnalité, s'assurant que toutes les lois sont respectées, et une décision sera prise.

Greta, voulez-vous ajouter autre chose?

Mme Greta Bossenmaier: Bien sûr. Merci, monsieur le ministre.

Il y a environ 17 ans, lorsque la Loi sur la défense nationale a été modifiée pour reconnaître le rôle du CST, ce dernier faisait alors partie du ministère de la Défense nationale. Nous avons toujours eu un mandat d'aide, soit la partie c) de notre mandat, qui nous permet, à la demande d'un autre organisme comme un organisme fédéral d'application de la loi, de demander si le CST pourrait appuyer le travail de cet organisme dans le cadre de son mandat légal. Encore une fois, étant donné que nous faisions partie du ministère de la Défense nationale, l'aide à la Défense nationale ou aux FAC n'était pas énoncée explicitement, puisque nous faisions partie de ce ministère.

Il y a environ six ans, pour faire un peu d'histoire, nous nous sommes séparés du ministère de la Défense nationale et nous sommes devenus un organisme indépendant, le Centre de la sécurité des télécommunications, qui relève quand même toujours du ministère de la Défense nationale. Par conséquent, le projet de loi ajoute les Forces armées canadiennes et la Défense nationale comme organisations qui pourraient faire appel à notre capacité, demander notre appui, comme l'a expliqué le ministre, dans le cadre de l'une de leurs missions légales. Nous participerions à une opération de soutien des Forces armées canadiennes.

Nous avons également ce matin des représentants des Forces armées canadiennes. Ils voudront peut-être aussi parler de leurs opérations.

M. Matthew Dubé: Je comprends cela. Comme mon temps est limité, nous pourrions peut-être revenir à ce sujet dans un instant. Puisque le ministre est avec nous, j'en profiterais pour lui poser quelques autres questions.

Nous avons parlé du mandat et de la relation avec le ministère de la Défense nationale. Cela m'amène à la question que j'ai posée aux fonctionnaires de Sécurité publique. Nous avons consacré beaucoup de temps à cet aspect du projet de loi. Je pense que votre présence ici aujourd'hui est la preuve de la nécessité d'approfondir cet aspect. Notre comité n'a pas nécessairement la même mémoire institutionnelle que le Comité de la défense nationale. Pouvez-vous nous expliquer pourquoi on a décidé de prendre un projet de loi qui, essentiellement, avançait en fonction d'éléments qui figuraient dans le projet de loi précédent, le projet de loi C-51, lors de la dernière législature, et d'ajouter ce train de mesures portant sur des changements importants au CST plutôt que d'en faire une loi autonome?

L'hon. Harjit S. Sajjan: Je pense qu'il est très important que nous démontrions aux Canadiens, lorsque nous examinons une mesure législative de ce genre, que nous l'examinons dans son ensemble. Nous le devons aux Canadiens. Nous ne pouvons pas examiner la question séparément. Nous devons être en mesure de démontrer aux Canadiens que nous veillons à leur sécurité contre les menaces étrangères et nous devons nous assurer qu'ils sont bien informés et que nous avons les bons conseils à leur prodiguer pour qu'ils puissent être beaucoup plus au courant de la cybermenace, tout en veillant à ce que la transparence et la protection de la vie privée soient adéquates.

● (1130)

M. Matthew Dubé: Je comprends cela, monsieur le ministre, même si je n'en suis pas convaincu.

L'autre point que je veux aborder rapidement, dans la minute qu'il me reste, concerne l'information accessible au public. La sous-chef a mentionné la dernière fois que l'information obtenue illégalement ne ferait pas partie de cette définition. Quand on regarde la situation actuelle en ce qui concerne Facebook, par exemple, on ne sait pas très bien si cette information a été obtenue illégalement. Selon la définition actuelle, telle qu'elle est énoncée dans la loi, le type de renseignements que nous examinons dans ce scandale pourrait-il essentiellement être visé par la définition de renseignements accessibles au public qui...

L'hon. Harjit S. Sajjan: Je peux vous assurer que le CST... et que tout est respecté conformément à la loi, puis que nous nous assurons d'avoir les bons processus en place. C'est ici...

M. Matthew Dubé: Je parle des renseignements qui sont disponibles, qui sont accessibles, qui ne sont pas nécessairement obtenus de façon illégale et qui sont donc techniquement obtenus légalement, même si c'est au mieux nébuleux. Que se passe-t-il dans ces situations?

L'hon. Harjit S. Sajjan: Je veux tout simplement m'assurer d'avoir bien compris votre question. Vous parlez de...

M. Matthew Dubé: Je parle, par exemple, de Facebook.

Le président: Excusez-moi, monsieur Dubé.

Je m'excuse, monsieur le ministre.

L'hon. Harjit S. Sajjan: Ce n'est pas grave.

Le président: Cette question est importante et je doute d'obtenir le consentement unanime du Comité pour prolonger votre temps de parole, mais si nous pouvions d'une façon quelconque revenir à cette question, ce serait bien.

Madame Dabrusin, vous avez la parole.

Mme Julie Dabrusin (Toronto—Danforth, Lib.): Merci, monsieur le ministre, d'être venu nous parler aujourd'hui du projet de loi C-59. La cybersécurité est une question qui préoccupe beaucoup de gens et il est donc très important de parler de ce que nous ferons avec le CST et de la façon dont cela améliorera la cybersécurité.

Il y a des éléments dans le projet de loi qui portent sur le mode de fonctionnement du CST avec une infrastructure essentielle. Il ne s'agit pas d'une infrastructure fédérale. Pouvez-vous nous expliquer comment le CST pourra utiliser le nouveau cadre prévu dans le projet de loi C-59 pour venir en aide à des infrastructures non fédérales?

L'hon. Harjit S. Sajjan: Je vais préparer le terrain, puis laisser Greta entrer dans les aspects techniques. C'est extrêmement important. Il s'agit de protéger les Canadiens au fur et à mesure qu'ils s'adaptent aux avancées technologiques, comme les nouveaux téléphones et les médias sociaux, et de veiller à ce qu'ils soient bien informés quant à ce qu'ils doivent faire pour protéger leurs propres renseignements personnels à leur façon

Plus important encore, il s'agit également de protéger les institutions que les Canadiens utilisent. C'est extrêmement important. Les Canadiens s'attendent à ce que nous nous assurions que tout, depuis les services bancaires jusqu'à nos grilles électorales, fonctionne correctement et ne puisse pas être perturbé. Voilà pourquoi il est important que nous collaborions avec des organismes non gouvernementaux pour pouvoir fournir les bons conseils et nous assurer ainsi qu'ils sont protégés, puisqu'il s'agit en fin de compte de veiller à ce que les Canadiens soient protégés.

Greta.

Mme Greta Bossenmaier: Merci, monsieur le ministre.

Je semble toujours revenir à l'histoire, mais je pense qu'un peu d'histoire est important. Depuis plus de 70 ans, comme le ministre l'a souligné dans ses remarques liminaires, nous nous occupons de protéger les renseignements les plus délicats des Canadiens.

Aujourd'hui, 70 ans plus tard, nous bloquons en moyenne tous les jours plus d'un milliard de tentatives malveillantes de compromettre les systèmes gouvernementaux. Nous exploitons des cyberdéfenses sophistiquées au nom du gouvernement du Canada sur les systèmes du gouvernement du Canada. C'est notre réalité aujourd'hui.

Nous prodiguons également des conseils, une orientation et des services au public et aux propriétaires d'infrastructures essentielles quant à la meilleure façon de se défendre, tout depuis nos 10 mesures les plus importantes que l'on devrait prendre pour se protéger dans le cyberespace jusqu'aux conseils techniques plus détaillés.

Si le propriétaire d'une infrastructure essentielle demandait au CST de lui fournir des services supplémentaires pour l'aider à se protéger, par exemple en cas d'attaque, le projet de loi nous permettrait de le faire. Le ministre devrait désigner les propriétaires de l'infrastructure essentielle comme un système important pour le gouvernement du Canada. Le propriétaire du système essentiel devrait nous faire parvenir une demande par écrit. Nous le ferions à sa demande et si le ministre l'avait désigné comme étant d'une importance cruciale. Cela nous permettrait d'utiliser certains de nos outils sophistiqués pour le protéger. Par exemple, s'il était attaqué par un cyberacteur malveillant qui tente de voler ses renseignements ou d'infiltrer ses systèmes, cette loi nous permettrait d'essayer de fournir certaines des techniques et méthodes sophistiquées que nous employons chaque jour pour protéger les renseignements des Canadiens au nom du gouvernement du Canada et pour le compte de propriétaires d'infrastructures essentielles, par exemple.

Mme Julie Dabrusin: Merci.

Je lisais un rapport du Citizen Lab qui faisait plusieurs suggestions au sujet du CST et du projet de loi C-59. J'y ai fait allusion à quelques reprises. L'une d'elles consistait à permettre aux institutions fédérales de se retirer des conseils et de la surveillance en matière de cybersécurité si elles le veulent.

S'il y avait un tel retrait, quelles seraient les répercussions sur votre capacité de fournir une cyberdéfense?

● (1135)

L'hon. Harjit S. Sajjan: Je pense que c'est prudent, surtout à notre époque. Ce que je retiens de mes voyages et des discussions que j'ai eues, c'est que les organismes veulent une meilleure protection, mais ce qui est encore plus important, que les Canadiens s'attendent à ce que, lorsqu'ils feront des affaires avec une entité, ils disposeront des outils et de l'expertise nécessaires pour aller de l'avant.

Je pense que nous empruntons cette voie, mais je pense que le choix leur appartient, chaque institution devra faire son propre choix.

Greta.

Mme Greta Bossenmaier: Vous avez tout à fait raison, monsieur le ministre. C'est à la demande du propriétaire d'une infrastructure essentielle. Encore une fois, je pense que nous diffusons beaucoup de renseignements très importants, des conseils et une orientation qui peuvent être utilisés par les citoyens et les propriétaires d'infrastructures essentielles, par exemple, pour mieux protéger leurs systèmes et leurs renseignements, mais c'est une décision qui leur appartient. Nous sommes vivement intéressés à utiliser cela, mais pour ce qui est de la nouvelle loi, ce serait certainement à la demande du propriétaire d'une infrastructure essentielle.

L'hon. Harjit S. Sajjan: Puis-je ajouter quelque chose? Ce qui est très important, c'est que le CST a toujours en arrière-plan protégé les Canadiens de cette façon, mais ce n'est que tout récemment que les vice-chefs ont fait preuve d'une grande ouverture, ont diffusé des messages sur leurs médias sociaux et ont veillé à ce que les Canadiens comprennent ce qu'ils doivent faire. Je pense que c'est ce qui est très important. Nous changeons également les choses pour montrer aux Canadiens que le CST est un organisme phénoménal qui possède la bonne expertise et qui est reconnu par nos partenaires du Groupe des cinq comme étant l'un des meilleurs au monde. Ce qui est encore plus important, c'est que des Canadiens protègent les Canadiens, afin qu'ils aient une grande confiance dans ce qu'ils font. Les conseils donnés ont en fait un impact, surtout la liste des 10 principaux conseils.

Mme Julie Dabrusin: De fait, le budget de 2018 prévoyait 115 millions de dollars pour un centre canadien de cybersécurité. Quel est le lien avec ce que nous examinons en ce moment quand nous parlons du projet de loi C-59 et du CST?

L'hon. Harjit S. Sajjan: Il s'agit de se tenir au courant, avec nous comme gouvernement nous assurons que tous nos organismes ont un endroit où ils peuvent aller pour obtenir la bonne expertise, et de créer un cybercentre d'excellence, où vous avez l'expertise du CST pour nous aider à comprendre tout cela. Il s'agira non seulement d'offrir un guichet unique que les organismes et les Canadiens pourront consulter pour savoir comment faire face aux menaces...

Greta, voulez-vous ajouter autre chose?

Mme Greta Bossenmaier: Le budget de 2018 a effectivement proposé un centre canadien d'excellence pour le cyberespace. Il serait logé au CST. Il réunirait les composantes opérationnelles du gouvernement du Canada qui travaillent aux opérations de cybersécurité. En ce qui concerne le point soulevé par le ministre, il s'agirait d'un guichet unique d'expertise — pour employer cette terminologie — que le gouvernement du Canada, les Canadiens et l'infrastructure canadienne pourraient consulter pour obtenir des conseils, une orientation et des services dignes de confiance.

Le président: Merci, madame Dabrusin.

Monsieur Motz, vous avez cinq minutes.

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

Merci, monsieur le ministre, et merci à votre équipe d'être ici aujourd'hui.

Monsieur le ministre, compte tenu de votre rôle dans le projet de loi C-59 et à titre de ministre de la Défense, avez-vous eu des rencontres avec vos homologues au sujet de la sécurité nationale ou du projet de loi C-59 lors de votre tournée en Inde?

L'hon. Harjit S. Sajjan: Si vous voulez savoir ce qu'il en est de mon voyage en Inde, j'ai été déçu de ne pas pouvoir visiter mon village natal.

M. Glen Motz: Donc, vous ne répondrez pas à la question. Permettez-moi de la poser différemment.

Le projet de loi C-59 exige que vous, comme ministre de la Défense, consultiez les Affaires étrangères sur tout ce qui concerne le SCRS ou le CST.

L'hon. Harjit S. Sajjan: Pourriez-vous répéter?

M. Glen Motz: Le projet de loi C-59 exige que vous, comme ministre de la Défense, ayez des interactions et des contacts avec les Affaires étrangères au sujet des questions touchant le SCRS et le CST. Étant donné que le CPM a demandé au conseiller à la sécurité nationale d'informer la presse, je me demande si vous avez été consulté à ce sujet. Si ce n'est pas le cas, devrions-nous inscrire dans le projet de loi que le conseiller à la sécurité nationale ne devrait pas informer la presse avant de vous avoir d'abord consulté?

Le président: Monsieur le ministre, compte tenu des discussions que j'ai eues précédemment avec tous les membres du Comité au sujet du projet de loi C-59, et malgré la clarté avec laquelle M. Motz a formulé sa question, je vous encourage, monsieur le ministre, à répondre à la première partie de la question, mais pour ce qui est des voyages...

● (1140)

L'hon. Harjit S. Sajjan: Il est de plus en plus difficile de déterminer quelles sont les différentes parties de la question. Si vous pouviez reformuler la partie au sujet du projet de loi C-59, je serais heureux d'essayer d'y répondre pour vous.

M. Glen Motz: Encore une fois, je vais poser la même question parce que, très respectueusement, monsieur le président, elle porte sur le projet de loi C-59.

Elle est liée à votre rôle de ministre de la Défense et à votre rôle dans le projet de loi C-59. Elle concerne les Affaires étrangères. Étant donné que nous avons vu le conseiller à la sécurité nationale présenter une séance d'information à la presse avant de vous informer — et je crois comprendre que vous n'avez pas été consulté avant qu'il n'informe la presse —, je me demande s'il ne faudrait pas apporter des modifications au projet de loi — parce qu'il ne nous donne aucune indication quant à qui le conseiller à la sécurité nationale devrait parler ou qui il devrait consulter avant d'informer la presse — pour nous assurer que cela ne se reproduise pas à l'avenir.

L'hon. Harjit S. Sajjan: Comme ministre de la Défense nationale, je suis responsable de la Défense nationale, des Forces armées canadiennes et du CST.

M. Glen Motz: C'est tout. Vous n'avez donc pas été consulté alors quand cette...

L'hon. Harjit S. Sajjan: Je vous donne ma réponse pour ce qui est de mes responsabilités.

M. Glen Motz: C'est intéressant.

Le terrorisme fait certainement partie du projet de loi C-59. Une partie de votre responsabilité à titre de ministre de la Défense et l'objectif du projet de loi C-59, c'est de protéger les Canadiens.

Vous étiez en Inde avec M. Atwal. Cela ne vous a-t-il pas alarmé au sujet des questions de sécurité nationale?

L'hon. Harjit S. Sajjan: Lorsqu'il s'agit de menaces quotidiennes partout dans le monde, je cherche à m'assurer, comme ministre de la Défense nationale, que je dispose des ressources adéquates au bon endroit pour m'assurer que nous sommes en mesure d'interpréter les diverses menaces. C'est ce que nous continuerons de faire. Voilà l'objet du projet de loi C-59.

À ce sujet...

M. Glen Motz: Compte tenu de ce commentaire, monsieur le ministre...

L'hon. Harjit S. Sajjan: Voilà à quel point c'est important.

M. Glen Motz: Désolé, mon temps est limité.

Compte tenu du commentaire que vous venez de faire, est-il juste de dire que... Étant donné que vous êtes responsable des questions de sécurité nationale, avez-vous lancé une enquête sur ce qui s'est passé en Inde dans l'affaire Atwal?

Le président: Pour l'instant, monsieur le ministre et monsieur Motz, le libellé de votre question n'a presque rien à voir avec le projet de loi C-59. Je tiens simplement à souligner que nous n'avons pas encore adopté ce projet de loi. Alors, ce n'est pas...

M. Glen Motz: Très bien.

Le président: Compte tenu de cette immense orientation de la part de votre président, je vous demanderais de continuer et de poser une autre question.

M. Glen Motz: À votre avis, monsieur le ministre, qui est le principal responsable de la sécurité nationale au pays? Est-ce vous, comme ministre de la Défense? Est-ce le ministre Goodale? Est-ce le premier ministre?

L'hon. Harjit S. Sajjan: Quand il est question de sécurité nationale, c'est l'une des raisons pour lesquelles un gouvernement a des choses qui sont aussi... Par exemple, le ministre de la Sécurité publique est responsable de la sécurité au Canada. Voilà pourquoi, comme ministre de la Défense nationale, j'examine les menaces étrangères. Cela fait en sorte qu'il y a une séparation, mais en même temps, sur demande, nous pouvons fournir le bon niveau de soutien.

Par exemple, dans le cas des feux de forêt, nous pouvons intervenir à l'échelle nationale en cas de menace, au besoin. S'il y a terrorisme, je dois m'assurer que nos forces spéciales, nos capacités, sont là au besoin, sur demande, à l'intérieur du Canada.

C'est quelque chose que j'examine très sérieusement tous les jours et c'est une responsabilité que je partage avec le ministre Goodale et la ministre des Affaires étrangères. Nous travaillons constamment ensemble. Chose encore plus importante, nos hauts fonctionnaires collaborent constamment pour s'assurer que nous protégeons les Canadiens, tâche que nous prenons extrêmement au sérieux.

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

M. Glen Motz: Dans votre témoignage, vous dites que vous, la ministre des Affaires étrangères et le ministre de la Sécurité publique êtes les seuls qui... Vous avez tous les trois la responsabilité ultime de la sécurité nationale et non le premier ministre ou qui que ce soit d'autre.

L'hon. Harjit S. Sajjan: En matière de sécurité, la responsabilité du gouvernement est d'assurer la sécurité des Canadiens et c'est précisément ce que nous faisons.

Le président: Merci, monsieur Motz.

Merci, monsieur le ministre.

Monsieur Fragiskatos, vous avez cinq minutes.

M. Peter Fragiskatos (London-Centre-Nord, Lib.): Merci, monsieur le président.

Merci au ministre et aux fonctionnaires d'être ici aujourd'hui.

Mes questions porteront sur le projet de loi C-59 et la cybersécurité.

Tout d'abord, monsieur le ministre, vous avez dit dans vos commentaires liminaires que les cyberopérations « seraient assujetties à des interdictions légales strictes qui interdiraient de diriger ces opérations contre des Canadiens, toute personne au Canada ou l'infrastructure globale de l'information au Canada, et nécessiteraient un solide processus d'approbation ». À mon avis, cela est tout à fait conforme aux principes démocratiques, mais pourriez-vous nous parler de l'importance de cette question, de s'assurer que lorsque nous avons une loi, lorsque nous parlons du CST et de ses pouvoirs, que ces pouvoirs sont conformes aux principes démocratiques?

● (1145)

L'hon. Harjit S. Sajjan: Absolument, et en fait, c'est extrêmement fondamental. J'essayais de répondre à cette question dans la réponse que j'ai donnée au sujet de ma responsabilité à l'égard du CST et de l'accent mis par l'armée sur les menaces étrangères, et c'est là où en est le CST.

Cependant, avec ce que le CST a actuellement et avec le projet de loi C-59, nous aurons une capacité supplémentaire de soutenir d'autres organismes avec une autorisation judiciaire. Je pense que ce qui est extrêmement important, c'est de s'assurer, en tant que gouvernement, de tirer parti de toutes les ressources appropriées au sein de notre gouvernement et dans le cadre des lois. Cependant, en même temps — et je tiens à le souligner énormément, parce que les Canadiens s'y attendent —, nous devons mettre en place un processus qui respecte la vie privée et la transparence. C'est quelque chose qui ne s'est jamais produit auparavant. Plus important encore, nous sommes le dernier pays du Groupe des cinq à avoir enfin atteint ce niveau de transparence.

Greta, voulez-vous ajouter quelque chose?

M. Peter Fragiskatos: Bien sûr, allez-y.

Mme Greta Bossenmaier: Si je comprends bien votre question, surtout en ce qui concerne les cyberopérations étrangères, actives et défensives, je dirais que c'est très clair dans la loi. J'attire votre attention sur deux éléments. Il y a d'abord les processus d'approbation stricts qu'il faudrait mettre en place. Les cyberopérations actives exigeraient l'approbation du ministre de la Défense nationale et du ministre des Affaires étrangères, étant donné qu'il s'agit d'opérations qui se dérouleraient à l'extérieur du Canada et non au Canada. Il y aurait donc des répercussions ou des considérations du ministère des Affaires étrangères. C'est du côté des approbations.

De plus, en ce qui concerne les limites, elles sont très claires quant à ce qu'une cyberopération active ou défensive pourrait entraîner. Par exemple, il serait interdit au CST de diriger ses cyberopérations actives auprès des Canadiens, d'une personne au Canada ou de l'infrastructure mondiale de l'information. Il faudrait s'assurer qu'elles ne causent pas la mort ou des lésions corporelles, qu'elles ne fassent pas délibérément obstacle à la justice ou à la démocratie. Il y aurait des approbations importantes, sérieuses et de haut niveau en plus de limites très claires quant à ce que ces activités pourraient être.

M. Peter Fragiskatos: Merci beaucoup, monsieur le ministre.

J'aimerais vous interroger au sujet de votre évaluation de la menace actuelle. Habituellement, les menaces à la sécurité nationale ont été comprises par les États présentant une menace primaire, les États voyous en particulier, mais des acteurs non étatiques sont maintenant entrés en jeu, particulièrement les mouvements terroristes. Nous parlons maintenant de la cybersécurité. Tous ces problèmes existent dans le contexte de la menace. Où se situe la cybersécurité en ce qui concerne les risques pour notre sécurité nationale?

L'hon. Harjit S. Sajjan: Dans le contexte global, nous devons examiner les menaces actuelles, les menaces qui pourraient émerger et ce que nous pouvons prévoir comme menaces futures. C'est la responsabilité du gouvernement de s'assurer que nous avons les ressources nécessaires pour faire face aux menaces aujourd'hui et demain.

Nous traitons avec des acteurs non étatiques depuis un certain temps, ainsi qu'avec des acteurs étatiques.

La cybernétique est une préoccupation importante, mais je tiens aussi à dire que, parce que nous nous en sommes extrêmement bien tirés au Canada, le CST a la capacité et l'expertise de donner aux Canadiens l'assurance que la cybernétique est extrêmement sécuritaire. Cependant, comme vous le savez, avec la technologie, nous devons rester à la fine pointe.

Pour être honnête avec vous, ce qui m'inquiète le plus dans le cas de pays comme la Russie, c'est de savoir comment ils peuvent prendre la cybernétique et ce que nous appelons la guerre hybride, comme ce qui se passe en Ukraine et essayer de manipuler et d'influencer les populations. C'est une préoccupation et pas seulement du point de vue du gouvernement. Nous devons nous assurer d'éduquer nos citoyens et nos médias. Nous l'avons remarqué et nous nous efforçons activement de discuter avec les nations concernées qui ont une expérience éprouvée dans ce domaine et c'est la raison pour laquelle nous faisons les bons investissements dans le domaine approprié. Nous examinons les menaces vraiment coriaces, mais en même temps, nous devons examiner les menaces émergentes.

M. Peter Fragiskatos: Merci, monsieur le ministre.

Le président: Merci, monsieur Fragiskatos.

Monsieur Calkins, vous avez cinq minutes. Allez-y, s'il vous plaît.

● (1150)

M. Blaine Calkins: Merci, monsieur le président.

Monsieur le ministre, merci d'être ici aujourd'hui. Nous l'apprécions vraiment.

Il s'agit simplement d'une petite précision à apporter. À un moment donné, dans le cadre de votre rôle de ministre de la Défense, avez-vous déjà demandé à des fonctionnaires de votre domaine de compétence ou d'ailleurs au sein du gouvernement du Canada de ne témoigner devant aucun des comités permanents de la Chambre des communes?

Le président: Pourriez-vous faire le lien avec le projet de loi C-59?

M. Blaine Calkins: Le ministre de la Défense nationale doit consulter le ministre des Affaires étrangères en vertu de la partie 3 du projet de loi C-59 et il jouera maintenant un rôle de premier plan si la loi est adoptée, et il aura besoin des conseils du ministre des Affaires étrangères pour prendre des décisions. Compte tenu de ce lien, je me demande s'il a été conseillé par le ministre des Affaires étrangères. A-t-il eu des conversations avec ses collègues ministériels? A-t-il discuté avec ses collègues qui sont membres de l'organe législatif et non de l'exécutif sur la question à savoir qui devrait ou ne devrait pas comparaître devant un comité permanent de la Chambre des communes?

Le président: Compte tenu de la question de la sécurité nationale, je vais vous laisser répondre en l'absence...

L'hon. Harjit S. Sajjan: Je suis désolé. D'après mon expérience dans les services de police, j'écoute comment les gens parlent et posent des questions.

Je vois où vous voulez en venir et je peux vous assurer que, lorsqu'il s'agit du ministre des Affaires étrangères et de moi-même, nous entretenons d'excellentes relations en ce qui concerne les menaces. C'est sur quoi porte le projet de loi C-59, c'est-à-dire assurer la sécurité des Canadiens tout en leur donnant l'assurance que leur vie privée sera protégée. Plus important encore, le CST a enfin la capacité de tirer parti de son expertise. Cela n'existait pas auparavant, surtout en ce qui concerne le projet de loi C-51.

M. Blaine Calkins: Mais ma question était de savoir si vous aviez déjà conseillé à quelqu'un de ne pas parler aux fonctionnaires du ministère. C'est une question non menaçante. J'aurais supposé que votre réponse aurait été non, que vous ne l'aviez jamais fait, mais je n'ai pas eu cette réponse, ce qui est malheureux.

Compte tenu de vos responsabilités à l'égard du Centre de la sécurité des télécommunications, à votre connaissance, quelle menace, le cas échéant, les soi-disant éléments perturbateurs du gouvernement indien représentent-ils pour la réputation du gouvernement du Canada?

L'hon. Harjit S. Sajjan: En ce qui concerne les menaces, comme je l'ai dit, nous examinons quotidiennement les menaces provenant du monde entier. Nous exerçons une surveillance régulière et nous nous assurons d'atténuer tout ce qui se passe. Je travaille en étroite collaboration avec le ministre Goodale à ce sujet et, ce qui est encore plus important, c'est que nos fonctionnaires travaillent également en étroite collaboration pour assurer la sécurité des Canadiens.

M. Blaine Calkins: Vous m'avez donné une réponse très générale à une question très précise, alors je la poserai de nouveau. Compte tenu de vos responsabilités à l'égard du Centre de la sécurité des télécommunications, quelles menaces, le cas échéant, les soi-disant éléments perturbateurs du gouvernement indien présentent-ils précisément à la réputation du gouvernement du Canada?

L'hon. Harjit S. Sajjan: Une des choses que le projet de loi C-59 fera, c'est de s'assurer que nous donnons au CST les bons outils, la capacité législative de tirer parti de sa capacité technique pour protéger les Canadiens contre toutes les menaces actuelles et émergentes.

M. Blaine Calkins: Si nous parlons des capacités, y a-t-il quelque part dans la Loi sur la Défense nationale, comparativement à ce que nous faisons ici avec le projet de loi C-59, qui stipule que le ministre de la Défense doit demander l'autorisation à tout autre ministre, en particulier, le ministre des Affaires étrangères, pour mener des opérations?

C'est un peu un oui ou un non. Y a-t-il quelque part dans la Loi sur la défense une disposition qui dit que vous avez besoin de l'autorisation du ministre des Affaires étrangères pour mener des opérations?

L'hon. Harjit S. Sajjan: En tant que gouvernement, et moi, en tant que ministre de la Défense nationale, en ce qui concerne ce que nous faisons à l'étranger, par exemple...

M. Blaine Calkins: Je pose une question législative très précise, monsieur le ministre.

L'hon. Harjit S. Sajjan: J'essaie de comprendre...

M. Blaine Calkins: À votre connaissance, y a-t-il un endroit dans la Loi sur la défense où la loi exige que vous consultiez ou que vous ayez besoin de l'autorisation d'un autre de vos collègues pour exercer des fonctions légales dans le cadre de la Loi sur la défense?

L'hon. Harjit S. Sajjan: Je ne peux pas mener des opérations à l'étranger sans l'approbation du Cabinet. Une fois que j'en ai le pouvoir, cela me donne la capacité de mener...

M. Blaine Calkins: Dans la loi.

L'hon. Harjit S. Sajjan: ... les opérations.

M. Blaine Calkins: Ce n'est que le mode de fonctionnement de l'entreprise. Lorsque nous examinons le projet de loi C-59, la partie 3 stipule que vous devez consulter le ministre des Affaires étrangères.

Ma question est la suivante: le rôle du ministre de la Défense a-t-il été réduit à celui de ministre de second rang du ministre des Affaires étrangères? Si oui, pourquoi vouloir créer ce précédent?

L'hon. Harjit S. Sajjan: Je peux vous assurer que lorsqu'il s'agit des mesures prises par notre gouvernement, on nous donne les pouvoirs appropriés. Cela donne aux Forces armées canadiennes et au CST le pouvoir d'agir.

L'autre aspect de ce que le gouvernement a fait, c'est de s'assurer que nous avons pleinement financé les Forces armées canadiennes pour qu'elles puissent répondre à ces besoins.

Plus important encore, le projet de loi C-59 donne au CST la possibilité de protéger activement les Canadiens, ce qui n'était pas le cas auparavant. Votre gouvernement précédent, à l'époque du projet de loi C-51a négligé de le faire.

● (1155)

Le président: Merci, monsieur Calkins.

Madame Damoff.

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

Monsieur le ministre, c'est un plaisir de vous accueillir au Comité de la sécurité publique, alors bienvenue et bon retour aux fonctionnaires qui sont ici.

Le projet de loi C-59 vous permet de mener des opérations de cybersécurité actives contre des entités étrangères hostiles. Nous avons discuté de l'infrastructure mondiale lorsque vos fonctionnaires ont comparu la dernière fois. Je m'inquiète de la façon dont les données sur les Canadiens pourraient être balayées dans ce contexte, par exemple, si je suis en vacances à Londres, en Angleterre, et que vous menez une opération et que je me retrouve dans cette situation.

Il s'agit d'entités strictement étrangères. Quelles mesures de protection avons-nous en place pour nous assurer que vous continuez de traiter avec des entités strictement étrangères, par opposition à des citoyens canadiens?

L'hon. Harjit S. Sajjan: C'est une très bonne question. Lorsque je suis devenu ministre, j'ai suivi le processus actuel. Il est extrêmement solide.

Nous avons une responsabilité. Si des renseignements sont recueillis accidentellement, il y a un processus très strict qui est suivi. Plus important encore, le processus actuel du commissaire du CST pour s'assurer que l'information...

Je veux m'assurer que ce soit bien expliqué, alors je vais donner la parole à Greta.

Mme Greta Bossenmaier: Merci, monsieur le ministre.

En ce qui concerne les cyberopérations actives et défensives, ce qui était, je crois, la nature de votre question, le projet de loi dit que le CST ne sera pas en mesure de diriger des cyberopérations actives ou défensives contre des Canadiens, contre quiconque au Canada, ou contre l'infrastructure mondiale de l'information au Canada. Cela fait partie du cadre juridique dans lequel nous fonctionnerions.

De plus, comme je l'ai déjà mentionné, ces opérations exigeraient des approbations de haut niveau et, comme le ministre l'a mentionné, un examen par le nouveau Comité de surveillance de la sécurité nationale et du renseignement, ainsi que par le Comité des parlementaires qui a été mis en place.

En vertu de la loi, les activités que nous entreprendrions ne pourraient viser ni les Canadiens, ni les infrastructures canadiennes, ni quiconque au Canada.

Mme Pam Damoff: Je suppose que c'est là où je suis déconnectée, car comment savez-vous qu'il s'agit de Canadiens? Dans le cybermonde, comment savez-vous qui est canadien par rapport à qui est étranger?

Je ne suis pas une experte du cybermonde, mais il ne s'agit pas d'une personne physique; vous faites affaire avec une entité dans le cybermonde. Comment savez-vous si c'est un Canadien ou non?

Mme Greta Bossenmaier: Shelly, voulez-vous en parler un peu, du point de vue de la collecte?

Mme Shelly Bruce (chef associée, Centre de la sécurité des télécommunications): Si vous considérez une cyberopération active ou une cyberopération défensive comme un plan qui a été élaboré, cela ne se fait pas spontanément. Beaucoup de recherches et d'analyses doivent être faites pour arriver au point où vous avez une idée de ce que vous pourriez faire en ligne dans une action défensive ou perturbatrice.

Les renseignements qui mèneront à ce plan, qui orienteront ce plan, seront ceux qui seront rassemblés dans le cadre de notre mandat en matière de renseignement étranger et en comprenant les intervenants et l'infrastructure en cause. Il pourrait s'agir de notre mandat de cyberdéfense et de comprendre comment Internet fonctionne et quels serveurs sont configurés de quelle façon et comment ils interagissent.

Il faudrait qu'il s'agisse d'un plan très bien informé et réfléchi dans lequel on examinerait les répercussions en aval. Le commissaire au renseignement travaille au début de ces processus et aide à faire en sorte que les autorisations ministérielles qui nous permettent de recueillir ces renseignements soient solides, raisonnables et proportionnelles, en plus de toutes les mesures qui s'y rattachent. Nous avons également des mesures de protection de la vie privée dans ce domaine.

Mme Pam Damoff: Il ne me reste qu'environ une minute et j'aimerais poser une autre brève question.

Monsieur le ministre, le dernier budget prévoyait un investissement assez important dans la stratégie nationale de cybersécurité. Le fait d'avoir une loi est un aspect, mais je me demande si vous pouvez nous parler de la façon dont ces investissements vous aideront dans votre travail.

L'hon. Harjit S. Sajjan: Ils sont absolument essentiels. Les bons investissements nous permettront non seulement de fonctionner à la capacité appropriée et d'avoir le centre d'excellence en cyberdéfense, mais surtout, de demeurer à la fine pointe de la technologie. Cet aspect est très important.

Il y a un point que j'ai tenté de souligner au début. Il s'agit de notre personnel. On peut avoir la meilleure technologie, mais elle est en fait mise au point par des personnes. Je tiens à souligner que les gens du CST...

Vous avez encore gagné ce prix, n'est-ce pas?

Mme Greta Bossenmaier: En effet.

L'hon. Harjit S. Sajjan: C'est encore une fois l'un des meilleurs employeurs au Canada.

Cette habileté à recruter les meilleurs est absolument incroyable. C'est l'une des raisons pour lesquelles nous avons pu rester à la fine pointe, mais cela exige de la recherche et du développement et le bon réseau pour le faire. Cet investissement nous permettra de rester à la fine pointe de la technologie.

● (1200)

Le président: Merci, madame Damoff.

En fait, je pourrais considérer que M. Dubé a trois minutes supplémentaires s'il souhaite poser sa dernière question.

L'hon. Harjit S. Sajjan: Nous regardons l'horloge, mais c'est l'horloge officielle, n'est-ce pas?

Le président: Oui, eh bien, il y a l'horloge officielle, puis il y a l'horloge que je vois.

Monsieur Dubé, vous pouvez terminer votre question.

M. Matthew Dubé: C'est la première fois que j'aime tant l'heure avancée.

Voix: Oh, oh!

M. Matthew Dubé: Très rapidement, j'ai une seule question. J'aimerais revenir aux détails de la situation de Cambridge Analytica avec Facebook.

De toute évidence, il n'y a pas de situation où l'information a été obtenue illégalement. C'est nébuleux, peut-être douteux et immoral, mais il n'est pas tout à fait clair que c'est illégal. Des renseignements comme ceux-ci qui sont obtenus et utilisés par des partis politiques dans divers pays du monde pourraient sans doute être visés par la définition de l'information accessible au public. Comment voyez-vous cela, monsieur le ministre ainsi que le CST?

L'hon. Harjit S. Sajjan: Pour le CST, la crédibilité de l'excellent travail qu'il accomplit et la crédibilité de tout gouvernement de fonctionner dans un ordre fondé sur des règles reposent sur le respect de la loi. C'est exactement de cette façon que le CST fonctionne.

Plus important encore, nous mettons en place des mesures encore plus rigoureuses pour nous assurer que les activités du CST et de tous nos organismes de sécurité sont menées à bien et nous avons mis en place un mécanisme pour tout, du commissaire au renseignement autorisant l'approbation ministérielle jusqu'à l'agence de surveillance des activités en matière de sécurité nationale et du renseignement, et que nous avons maintenant des parlementaires de tous les partis.

Je vous réponds que le CST respectera toujours la loi.

M. Matthew Dubé: Je comprends cela, monsieur le ministre. Si nous parlons de fonctionnement légal, et que cette information est obtenue légalement — même si on peut soutenir que les lois devraient être modifiées dans ce contexte —, cela ne signifie-t-il pas que le CST pourrait obtenir cette information en vertu de l'information accessible au public?

L'hon. Harjit S. Sajjan: Comme je l'ai dit, non seulement du point de vue juridique, les activités du CST visent à protéger les Canadiens et les intérêts canadiens, et nous continuerons de le faire.

M. Matthew Dubé: J'apprécie l'indulgence du président. Je vais m'arrêter ici.

Le président: Merci, monsieur Dubé.

Monsieur le ministre, au nom du Comité, je vous remercie de votre présence. Sur ce, nous allons suspendre la séance pour vous laisser partir.

Pour les autres, veuillez rester et nous allons poursuivre, parce que le temps est précieux.

Encore une fois, merci.

● (1200)

(Pause)

● (1200)

Le président: Je vais demander aux membres de reprendre leur place.

Je vais présumer, madame Bossenmaier, qu'il n'y a pas d'autres déclarations à faire et que nous pouvons simplement passer aux questions.

Mme Greta Bossenmaier: C'est exact, monsieur le président.

Le président: Sur ce, monsieur Fragiskatos, vous avez sept minutes. Allez-y, s'il vous plaît.

M. Peter Fragiskatos: Merci beaucoup, monsieur le président.

Ma première question découle de l'entretien que je viens d'avoir avec le ministre au sujet de la place des conversations sur la cybersécurité avec nos alliés. C'est certainement ce qui se passe au niveau ministériel, mais pour ce qui est de la collaboration et des conversations entre les fonctionnaires, c'est certainement ce qui se passe, j'imagine. Quelle est notre priorité à cet égard? Il y a tellement de menaces à la sécurité nationale.

● (1205)

Mme Greta Bossenmaier: Absolument, la cybersécurité est de plus en plus un sujet de conversation avec nos alliés, avec nos partenaires. Je ne crois pas qu'une réunion avec nos collègues et nos alliés se termine sans que nous abordions le sujet de la cybersécurité. Encore une fois, la sécurité des TI fait partie de notre mission depuis 70 ans, compte tenu des nouvelles exigences, de la fréquence et des nouveaux défis. Il est certain que la nature de la discussion et l'importance de cette question dans les divers dossiers que nous traitons au sein du CST se sont accentuées.

Pour répondre à votre question, il y a certainement un haut niveau de priorité, beaucoup de discussions et de partage des meilleures pratiques. Je pense que l'une des choses que nous comprenons tous, c'est que dans ce domaine, personne n'a toutes les réponses. Plus nous pouvons partager les pratiques exemplaires, examiner les leçons apprises et apporter diverses possibilités à la table, plus celles-ci enrichissent vraiment la discussion.

La cybersécurité s'inscrit dans d'autres types de menaces et je pense que c'est une question que le Comité et d'autres comités ont abordée, et je sais que certains de mes collègues d'autres organisations ont aussi eu à répondre à cette question. Nous mettons l'accent sur les priorités du gouvernement en matière de renseignement. La cybersécurité est certainement l'une des principales questions que nous abordons, mais elle fait partie d'un ensemble plus vaste de priorités en matière de renseignement, en fonction de ce que le gouvernement considère comme les priorités du jour.

M. Peter Fragiskatos: Pourriez-vous nous parler d'une pratique exemplaire? Évidemment, ce sont des mesures de sécurité délicates, mais avez-vous tiré quelque chose des conversations que vous pourriez signaler pour dire que c'est le résultat de la collaboration avec nos alliés et que c'est pourquoi il est vraiment important d'avoir des conversations sur ces questions?

Mme Greta Bossenmaier: Permettez-moi de vous parler du nouveau centre canadien pour la cybersécurité qui a été mentionné dans le budget de 2018 et dont on a discuté à plusieurs reprises aujourd'hui.

Un certain nombre de nos alliés qui ont adopté ce genre de modèle lorsqu'ils ont constaté qu'ils devaient intégrer leurs propres organismes cryptologiques — nos organisations soeurs — pour consolider les capacités de leurs cyberopérations au sein de leurs organismes cryptologiques, ont constaté quelques éléments. Premièrement, je pense qu'ils voient la nécessité d'avoir une source unifiée et fiable d'informations, de conseils et d'orientations, un endroit où leurs citoyens et leurs entreprises peuvent se tourner.

Deuxièmement, j'aimerais revenir un peu sur ce que le ministre a dit tout à l'heure au sujet de l'expertise. Je suis très heureuse de constater que les hommes et les femmes qui travaillent au CST comptent vraiment parmi les meilleurs et les plus brillants esprits de notre pays, qu'il s'agisse de mathématiciens, d'ingénieurs, d'informaticiens ou de linguistes qui consacrent leur temps et leur attention à travailler au CST et à mettre à contribution leurs capacités et leurs compétences. Encore une fois, l'une des pratiques exemplaires que nous avons vues de la part des alliés est de consolider leurs opérations de cybersécurité au sein des organisations soeurs du CST et de vraiment mettre à profit les compétences et les capacités dont ils ont besoin pour mieux protéger leurs propres citoyens.

M. Peter Fragiskatos: Merci beaucoup.

Nous avons entendu le ministre parler des menaces à notre sécurité, du point de vue de la cybersécurité, qui émanent d'acteurs étatiques, d'États voyous en particulier et de mouvements non étatiques comme des organisations terroristes. Pourriez-vous nous dire si les cyberattaques prennent une forme différente, selon qu'elles sont lancées par un acteur étatique ou par une organisation terroriste? Je pense qu'on pourrait avoir l'impression que les organisations terroristes ne sont pas capables de mener des attaques très sophistiquées. La situation est en train de changer. Le fait est qu'ils peuvent monter des attaques complexes. Ce n'était pas le cas auparavant, mais nous le constatons maintenant. Pourriez-vous nous en parler?

Mme Greta Bossenmaier: Bien sûr.

Je vais demander à Scott Jones, notre sous-chef de la sécurité des TI, d'intervenir également. Sans vouloir lui couper l'herbe sous le pied, avant que je lui cède la parole, je dirai simplement que l'une des choses dont Scott parle souvent, c'est que nous voyons maintenant une grande variété d'acteurs de cybermenaces. Oui, nous nous inquiétons depuis longtemps des États-nations et des acteurs non étatiques, comme vous l'avez mentionné. Nous nous inquiétons des pirates informatiques, des cybercriminels. Dans le cadre de sa pratique, en défendant les systèmes du gouvernement du Canada et en fournissant des conseils et des directives aux Canadiens et aux infrastructures essentielles du Canada, Scott dit souvent que nous devons nous protéger et nous défendre contre toute cette gamme d'acteurs de menaces. Ils sont diversifiés, mais notre responsabilité est de protéger les renseignements des Canadiens et les renseignements les plus confidentiels des Canadiens contre cette variété d'acteurs de la menace.

Sur ce, je vais céder la parole à Scott afin de vous parler un peu de la menace qu'il observe.

● (1210)

M. Scott Jones (chef adjoint, Sécurité des technologies de l'information, Centre de la sécurité des télécommunications): Pour poursuivre dans la même veine, je pense que l'un des points clés à considérer est le fait que les cybertechniques sont à la portée de n'importe qui, et c'est davantage le résultat du niveau de résilience auquel nous sommes tous confrontés. Il y a des mesures simples que nous essayons de promouvoir et que nous pouvons tous prendre pour nous rendre plus résilients face à n'importe quel acteur, parce que, pour revenir à ce que vous disiez, peu importe qui ils sont, la cybertechnique est à leur portée. Voici dix mesures, dont quelques-unes très simples, que nous pouvons tous prendre pour accroître notre résilience.

Le deuxième élément, c'est la façon dont nous pouvons acheter des choses qui sont meilleures et plus sécuritaires dès le départ. C'est une partie du travail que nous faisons à l'échelle internationale. Pour répondre à votre question précédente sur le travail à l'étranger, il y a des mesures comme rechercher des produits pour avoir de meilleures caractéristiques de sécurité, des éléments qui sont sécuritaires par défaut, dont nous n'avons pas à nous inquiéter. Par exemple, nous participons à un programme de critères communs avec 27 pays différents.

Comment pouvons-nous communiquer l'information rapidement pour permettre aux gens d'agir en notre nom? Nous ne pouvons pas nécessairement compter que sur nous-mêmes. Certaines de ces techniques sont très perfectionnées, mais nous pouvons envisager l'infrastructure essentielle pour relever la barre.

M. Peter Fragiskatos: Vous avez dit quelque chose et je vais m'arrêter là, parce que le président a dit que je n'avais plus de temps, mais merci beaucoup pour le...

Le président: Je vous remercie de votre attention opportune au président.

Monsieur Motz, allez-y.

M. Glen Motz: Merci, monsieur le président, et je peux assurer au président que je vais peut-être me concentrer davantage sur mes questions pour cette portion.

Le président: Nous apprécions toujours la concentration. Je m'attends à ce que vous posiez des questions approfondies.

M. Glen Motz: À la partie 3 concernant l'article 76

> Les activités menées par le CST dans le cadre de son mandat dans les domaines du renseignement étranger, de la cybersécurité et l'assurance de l'information, des cyberopérations défensives ou actives de son mandat ne doivent pas viser un Canadien ou une personne se trouvant au Canada.

Comme nous le savons, Internet contient beaucoup de cryptage, de modificateurs IP, de réseaux privés virtuels et ainsi de suite.

Comment allez-vous vous assurer que vous ne ciblez pas un Canadien? Comment faites-vous cela? Voici une question complémentaire, si vous me le permettez, pour que vous puissiez répondre aux deux. Si vous tombez sur la propagande dans le cas d'un terroriste connu de l'EIIS et que la personne diffuse de la propagande de masse à des citoyens canadiens d'un pays étranger, devriez-vous alors vous abstenir d'utiliser des cyberopérations et laisser cette information être communiquée aux Canadiens? Comment interprétez-vous le projet de loi pour gérer cette nuance?

Mme Greta Bossenmaier: Je vais commencer par la première réponse et je demanderai probablement à Shelly Bruce, la chef associée, de répondre à cette question. Ensuite, je pense que je devrai revenir à votre deuxième question pour m'assurer d'avoir bien compris.

Pour ce qui est de votre première question, vous avez tout à fait raison de dire que le projet de loi tel qu'il est proposé — et en fait, notre loi actuelle également — nous interdit en droit de diriger nos activités à un Canadien ou à n'importe qui au Canada. Nous nous concentrons sur les cibles étrangères dans les pays étrangers, d'où l'aspect renseignement étranger de notre mandat. Nous mettons l'accent sur le renseignement étranger depuis plus de 70 ans.

C'est un peu la discussion que Shelly a déjà amorcée sur la façon dont nous nous assurons de concentrer nos efforts sur des éléments de l'infrastructure de l'information qui se trouvent à l'extérieur du Canada. Les analystes du renseignement étranger doivent s'assurer que les Canadiens ne participent pas au processus.

Sur ce, Shelly, je vous laisse la parole pour vous donner un peu plus d'informations sur la façon de nous assurer de cela.

Mme Shelly Bruce: Bien sûr. Vous avez parlé du mandat relatif au renseignement étranger et de l'aspect des cyberopérations actives des autorités proposées. Je pourrais peut-être commencer par parler du renseignement étranger.

Avant que des activités ne soient entreprises, il y a un processus très solide en place concernant les politiques, la formation et les tests. Chaque analyste effectue un test en ligne et n'a accès à aucun système tant qu'il n'a pas les connaissances approfondies de toutes les restrictions et les exigences pour s'assurer qu'il dirige ses activités contre des entités étrangères à l'extérieur du Canada d'une manière cohérente ou directement liée à une priorité en matière de renseignement du gouvernement. Il y a trois tests...

M. Glen Motz: Je suis désolé, mais permettez-moi de passer à la deuxième partie de ma question.

Vous êtes au courant de la propagande terroriste lancée contre des Canadiens, mais c'est par un Canadien en sol étranger. Comment interprétez-vous la loi comme étant en mesure de répondre à cela? Faut-il le laisser partir ou pouvez-vous répondre?

● (1215)

Mme Shelly Bruce: Il nous est interdit de cibler les Canadiens n'importe où, alors s'il y a une corrélation directe et que cette activité émane des communications d'un Canadien, c'est interdit.

Merci.

M. Glen Motz: Je vous en remercie.

Étant donné que nous vivons maintenant dans un nouvel environnement, nous avons des Canadiens, qu'ils soient des terroristes nés au pays ou qu'ils soient partis pour revenir, qui représentent une menace et continueront de représenter une menace pour la sécurité nationale. D'après votre expérience collective, y a-t-il quelque chose que nous devons faire pour changer la situation afin que, si un Canadien présente une menace imminente pour les Canadiens, vous puissiez faire quelque chose?

Mme Greta Bossenmaier: Je vais commencer par répondre à votre question, puis, encore une fois, je demanderai à Shelly de compléter ma description.

Cela nous ramène au mandat. Le mandat du Centre de la sécurité des télécommunications est le renseignement électromagnétique étranger qui n'est pas destiné à un Canadien ou à qui que ce soit au Canada, ce qui est un objectif étranger. Je me contenterai de dire qu'il y a d'autres éléments au sein de l'appareil de sécurité nationale qui mettent l'accent sur les menaces pour le Canada qui peuvent émaner d'un Canadien. Certains de nos partenaires dans ce domaine...

Shelly, voulez-vous nous parler un peu de la façon dont nous travaillons avec nos partenaires à cet égard?

Mme Shelly Bruce: L'activité terroriste est un sport d'équipe au Canada. La GRC, le SCRS, le CST et d'autres organismes ont chacun un rôle à jouer et nous travaillons ensemble pour comprendre ce que chacun d'entre nous apporte par son mandat, ses pouvoirs, ses compétences et ses capacités. Dans ce cas-ci, il se peut que les services aient pour mandat d'examiner un Canadien à l'extérieur du Canada qui a participé à ces activités.

La loi actuelle nous permet d'aider la GRC et le SCRS. En général, c'est pour les organismes de sécurité nationale et d'application de la loi, mais en pratique, c'est surtout pour le SCRS et la GRC. Dans ce cas, s'ils en avaient le pouvoir, ils pourraient nous demander de l'aide dans cet espace et nous pourrions utiliser nos capacités pour les aider, pourvu que cela se fasse dans les paramètres de l'autorité légale en vertu de laquelle ils opèrent.

M. Glen Motz: L'an dernier, nous avons appris que le Conseil national de recherches du Canada a été victime de l'exploitation du réseau informatique chinois. Les dommages ont été de l'ordre de centaines de millions de dollars. Sous votre direction, conformément à la partie 3 de l'article 76, que ferez-vous, en tant que chef du CST, pour contrer ces attaques et protéger l'intégrité de l'argent des contribuables?

Mme Greta Bossenmaier: Un élément clé de notre mandat porte sur la cybersécurité et c'était un élément essentiel de notre mandat bien avant ce nouveau projet de loi. Une des pierres angulaires de ce que nous faisons, c'est d'essayer de protéger le mieux possible les systèmes du gouvernement du Canada et davantage avec cette mesure législative, les infrastructures essentielles pour le gouvernement du Canada.

J'ai mentionné tout à l'heure que, grâce à la technologie et notre équipe, le CST déploie actuellement des moyens de défense très perfectionnés en matière de cybersécurité sur les réseaux du gouvernement du Canada. Cela nous aide tous les jours. J'ai déjà dit que nous bloquons jusqu'à un milliard d'actions malveillantes par jour. L'ampleur de ces cyberactions malveillantes est extrêmement élevée et nous travaillons donc tous les jours pour bloquer ces actions.

Lorsque quelque chose se produit — et nous disons toujours que personne n'est à l'abri de ce genre de situation, car c'est un environnement très difficile —, nous avons aussi une responsabilité très importante. Nous travaillons avec le ministère concerné, par exemple, et avec d'autres intervenants du gouvernement afin de déterminer comment nous pouvons remédier à la situation le plus rapidement possible afin de nous assurer que l'information est protégée et que les services sont rétablis.

Le président: Malheureusement, monsieur Motz, nous allons devoir nous arrêter là. Je m'excuse.

Monsieur Dubé, vous avez sept minutes. Allez-y, s'il vous plaît.

[*Français*]

M. Matthew Dubé: Merci, monsieur le président.

Je veux revenir sur la question que j'ai posée au ministre, mais à laquelle je n'ai pas réussi à obtenir de réponse, selon moi.

Dans un contexte où l'information peut être obtenue de façon légale par une entreprise, par exemple Cambridge Analytica, même si on peut dire que c'est immoral et que cela devrait être illégal, est-ce que cela correspond à la définition d'information disponible publiquement?

● (1220)

[*Traduction*]

Mme Greta Bossenmaier: Je remarque que toute la question de l'information accessible au public a été examinée autour de cette table. Je vais essayer d'ajouter quelques éléments.

Pour nous, le mandat est essentiel. Le mandat est important et il en est ainsi dans l'ensemble du projet de loi que vous avez sous les yeux, et cela comprend l'information accessible au public. Nous ne pouvons utiliser l'information accessible au public que si elle est liée à notre mandat, notre mandat relatif aux renseignements étrangers ou notre mandat en matière de cybersécurité. La loi actuelle ou proposée ne nous donne pas le mandat de concentrer nos activités sur les Canadiens, d'avoir une capacité d'enquête, de créer des dossiers sur les Canadiens. Ce n'est pas dans le cadre de notre législation actuelle ou proposée.

Je commencerais par le fait que le mandat est important.

Deuxièmement, comme on l'a déjà dit, je crois, l'information accessible au public — et c'est défini dans notre loi — ne comprendrait pas l'information qui a été piratée ou volée. Cette information serait accessible au public.

Aussi...

M. Matthew Dubé: Si vous me le permettez, avant que vous poursuiviez...

Mme Greta Bossenmaier: Oui.

M. Matthew Dubé: La partie du projet de loi qui porte sur l'information accessible au public exempte précisément l'interdiction de cibler les Canadiens. Donc, vous ne recueillez peut-être pas les données de façon active, mais vous êtes autorisé à les recueillir dans le cadre de la recherche effectuée en vertu des articles 24 et 25, si je ne m'abuse.

Vous avez parlé de renseignements piratés ou volés, mais en vertu de la loi actuelle, on pourrait soutenir que les renseignements dont nous discutons dans cet exemple particulier — je suis sûr qu'il y en a d'autres que nous ne connaissons pas — n'ont pas été obtenus illégalement. Donc, le travail qu'effectuait Cambridge Analytica — et probablement d'autres entreprises de ce genre — pour les partis politiques, par exemple, était d'obtenir de l'information sur les gens par l'entremise de Facebook, et cela, tout à fait légalement.

Cela ne relève-t-il pas de l'information accessible au public, si une entreprise comme celle-là est en mesure de l'obtenir? Il n'y a pas de répercussions juridiques parce que ce n'est pas illégal. Est-ce que le CST ne pourrait pas faire la même chose en vertu de ces dispositions, même si, incidemment, tel qu'il est énoncé dans la loi, dans le projet de loi C-59?

Mme Greta Bossenmaier: Monsieur le président, je dois revenir sur le fait que, même en ce qui concerne l'information accessible au public, cela revient à notre mandat. Nous n'aurions accès à l'information accessible au public que si elle était liée à notre mandat et nous n'avons pas de mandat axé sur les Canadiens ou quiconque au Canada. Pour le cas particulier dont vous parlez, je crois savoir que le commissaire à la protection de la vie privée se penche sur la question et j'imagine que les détails à ce sujet sont toujours en cours d'élaboration, alors je ne peux parler que de notre législation. Encore une fois, cela nous ramène à notre mandat. Ce serait très précis: pourquoi en aurions-nous besoin? De plus, le projet de loi propose de deux autres éléments.

Premièrement, il stipule qu'il faudrait mettre en place des mesures de protection de la vie privée, même pour les renseignements publics. Deuxièmement, comme tous les autres aspects du projet de loi, il devrait faire l'objet d'un examen par le Comité national de surveillance des activités de renseignement de sécurité. Le CST n'a pas le pouvoir d'examiner toute information accessible au public. Il est très ciblé et très axé sur le respect de notre mandat et, encore une fois, sur la mise en place de mesures de protection de la vie privée et, enfin, sur l'examen de toutes nos activités par un organisme de surveillance indépendant.

J'espère que cela répond à votre question.

M. Matthew Dubé: Très bien.

Vous avez parlé de l'enquête de la commissaire à la protection de la vie privée, mais je crois comprendre que votre organisation et le SCRS ont également été chargés d'examiner cette situation. Dans ce contexte particulier, lorsque vous faites les recherches prescrites dans la loi où ces exemptions existent, nonobstant l'article 25, qui parle de la protection de la vie privée, les recherches ne seraient-elles pas faites, par exemple, sur Facebook, dans le cadre de cette infrastructure d'information? J'ignore si cela relèverait de la définition de l'infrastructure de l'information, mais si on vous demande d'examiner la situation également, ne pourriez-vous pas inévitablement trouver des renseignements sur les Canadiens et être autorisé à les obtenir même si, incidemment, c'est ce que prévoit le projet de loi C-59. Et dans ces circonstances, même si ce serait dans le cadre du mandat — je le comprends —, même si je vois que vous prenez des mesures pour protéger la vie privée, l'information pourrait néanmoins être recueillie au cours de ce type d'enquête.

N'est-ce pas exact?

● (1225)

Mme Greta Bossenmaier: Vous avez couvert beaucoup de terrain. Je commencerai peut-être par le fait que la ministre des Institutions démocratiques a demandé au CST d'examiner la question des institutions démocratiques.

J'y repense et je me tourne vers Scott. Il y a environ un an, vers juin 2017, la ministre des Institutions démocratiques, Mme Gould, a demandé au CST d'examiner les cybermenaces qui pèsent sur les institutions démocratiques des Canadiens. Pour la première fois de notre histoire, nous avons produit un rapport qui est à la disposition du comité, au cas où vous ne l'auriez pas vu, et qui porte sur les grandes cybermenaces qui pèsent sur les institutions démocratiques.

Nous avons examiné de près trois aspects différents. Nous avons considéré le processus électoral en tant que tel et fonctionnement du mécanisme électoral. Nous nous sommes également penchés sur les cybermenaces pour les hommes et femmes politiques et les partis politiques, ainsi que sur les cybermenaces pour les médias. Nous avons fait une évaluation à ce moment-là, il y a environ un an.

La ministre des Institutions démocratiques nous demande maintenant de revoir notre évaluation de la menace à la lumière des changements survenus au cours de la dernière année. Même lorsque nous avons publié le rapport initial, nous avons dit qu'il s'agirait probablement d'un rapport sans cesse à renouvelé à la lumière nouveaux renseignements, notamment sur les menaces.

C'est le genre de travail que nous nous attendons à faire au cours des prochaines semaines, pour revoir notre évaluation de la menace à la lumière des renseignements et des activités qui ont eu lieu au cours de la dernière année. Il s'agit de la mettre à jour.

Le président: Malheureusement, nous allons devoir nous arrêter là.

Monsieur Picard, vous avez sept minutes.

Allez-y, s'il vous plaît.

M. Michel Picard: Merci.

Je vais poser mes questions en français, si vous me le permettez.

[*Français*]

Je vais revenir sur quelques points dont nous avons discuté au sujet du ciblage possible de citoyens canadiens.

Il est clair que le CST n'enquête pas sur des Canadiens à l'étranger. Aussi, lorsqu'il y a une information qui pourrait impliquer un Canadien à l'étranger, on n'en tient pas compte, on détruit l'information obtenue.

Le CST est un partenaire de plusieurs ministères au Canada, mais aussi un partenaire international. Il échange donc de l'information. Comment le CST doit-il gérer l'information qui vient de partenaires étrangers qui, eux, ne sont pas soumis à des restrictions en ce qui a trait aux enquêtes sur des Canadiens?

[*Traduction*]

Mme Greta Bossenmaier: Encore une fois, nous nous en tenons à notre mandat, qui est de ne pas mettre l'accent sur les Canadiens ou quiconque réside au Canada. Il s'agit de reconnaître qu'il pourrait y avoir une collecte accessoire de renseignements dans le cadre de nos activités. Si je comprends bien la question, il s'agit également de savoir comment nous collaborons avec nos partenaires étrangers.

Je suis accompagnée aujourd'hui par notre chef de la protection de la vie privée et chef adjoint aux politiques et aux communications. Comme la protection des renseignements personnels fait partie de son titre, je vais demander à Dom de vous parler un peu de la façon dont nous travaillons avec nos partenaires et traitons les renseignements personnels.

[*Français*]

M. Dominic Rochon (chef adjoint, Politiques et communications, Centre de la sécurité des télécommunications): Merci de la question.

[*Traduction*]

Je vais m'exprimer en anglais moi aussi et essayer de répondre en abordant la question sous l'angle du renseignement électromagnétique étranger.

Lorsque nous recueillons de l'information, vous avez tout à fait raison de dire que, compte tenu de la nature du fonctionnement des communications, nous pouvons trouver de l'information concernant un Canadien. Permettez-moi un exemple concret. Nous nous intéressons à un méchant X connu dans le pays Y. Ce type correspond à une priorité du gouvernement en matière de renseignement. Il va sans dire que c'est un méchant qui veut commettre des actes condamnables qui portent atteinte à la sécurité nationale. Nous recueillons des renseignements sur ce type.

À notre insu, ce type pourrait vous téléphoner. Lorsque nous recueillons des renseignements à ce sujet, nous devons comprendre que l'appel devient une communication privée. Le Code criminel dit très clairement qu'il est illégal de recueillir des renseignements sur une communication privée.

Nous avons des autorisations ministérielles qui couvrent nos diverses activités de collecte d'information et qui nous permettent de conserver cette information, si elle est effectivement d'intérêt pour la sécurité nationale ou le renseignement. Comme vous l'avez fait remarquer, nous devons supprimer immédiatement cette information si ce n'est pas le cas. Si vous recevez un appel téléphonique et qu'il est question de quelque chose qui n'a rien à voir avec la sécurité nationale, nous allons supprimer ces renseignements. Nous prenons note du fait et nous supprimons les renseignements immédiatement, et le commissaire les examine chaque année pour s'assurer que nous les supprimons.

Si les renseignements présentent un intérêt pour la sécurité nationale, nous les conservons, mais même en le conservant, nous rédigeons un rapport qui parle de la conversation que vous avez peut-être eue, peut-être au sujet d'un attentat contre quelque chose qui intéresse le Canada. Nous protégerions quand même votre identité dans ce rapport, en utilisant un terme générique pour cacher votre identité.

Puis vient le moment de la communication de renseignements. Où va notre rapport? Évidemment, il y a des organismes nationaux au sein de l'appareil de la sécurité nationale au Canada, le SCRS et la GRC, notamment, que le rapport intéresse. Il est possible que la loi les autorise à connaître l'identité du Canadien en cause. Des mécanismes sont en place pour leur communiquer cette information.

De même, lorsque nous rédigeons des rapports, une partie de l'information est évidemment communiquée à des partenaires étrangers, et il y a d'autres éléments qui régissent cet échange d'information. Mais encore une fois, s'ils veulent que ces renseignements soient communiqués, ils doivent nous expliquer pourquoi il est impératif qu'ils les obtiennent.

Bien sûr, nous sommes liés par d'autres dispositions. Nous avons une directive ministérielle, par exemple, que le ministre a récemment été émise de nouveau, concernant l'échange de renseignements qui peuvent faire apparaître des risques de mauvais traitements. Nous faisons une analyse de ce que nos partenaires veulent obtenir et de l'utilisation qu'ils en feront, et nous analysons les risques pour éviter que la communication de ces renseignements n'entraîne des mauvais traitements. Il y a un calcul qui se fait avant que l'information ne soit communiquée.

● (1230)

[*Français*]

M. Michel Picard: L'aspect de la question que je voulais aborder ne concerne pas tant l'information qui va vers l'étranger, mais plutôt le partenaire étranger qui vous informe qu'après son enquête et son analyse, il a identifié quatre personnes, dont une est de nationalité canadienne. Ce partenaire étranger n'a pas la restriction de ne pas enquêter sur des Canadiens et vous transmet de l'information. Puisque c'est une personne d'intérêt pour ce partenaire étranger, cela change-t-il le statut de cette personne et, de ce fait, le processus que vous venez de nous expliquer? Gardez-vous cette information et validez-vous que cette personne représente une menace ou, au contraire, êtes-vous tenus de ne pas accepter cette information?

M. Dominic Rochon: Sans trop entrer dans les détails, je dirais que l'exemple que vous donnez relèverait du mandat du SCRS. Si ce partenaire a de l'information qui porte sur un Canadien, c'est là que nous travaillons en partenariat avec le SCRS.

[*Traduction*]

Nous nous tournerions vers le SCRS : « Voici des renseignements qui peuvent porter sur un Canadien. C'est votre responsabilité, pas la nôtre », à propos du suivi qui concerne un Canadien en particulier.

[*Français*]

M. Michel Picard: Le mandat du CST de protéger les Canadiens des différentes menaces de l'extérieur va au-delà du contexte militaire.

Est-ce que le CST pourrait aider à contrer des menaces qui relèveraient davantage du mandat du CANAFE, par exemple, s'il s'agissait de financement d'activités terroristes ou criminelles? Disons que des communications qui entrent portent à croire qu'il se prépare un événement terroriste financé. Cela sollicite le CANAFE. Cependant, cela pourrait concerner aussi Industrie Canada ou d'autres ministères. Autrement dit, la flexibilité de l'appui du CST s'étend à l'ensemble des agences du gouvernement.

[*Traduction*]

Mme Greta Bossenmaier: Je vais dire un mot de certains éléments du mandat du CST. Du point de vue de la collecte de renseignements à l'étranger, nous avons la responsabilité de recueillir des renseignements qui se rattachent à toutes les priorités du gouvernement en la matière. Pour répondre à votre question, ces priorités vont certainement au-delà du seul soutien au fonctionnement des Forces canadiennes. Il y a aussi les menaces qui pèsent sur l'ensemble du Canada, et le gouvernement en place établit les priorités en matière de renseignement.

L'information que nous recueillons vise vraiment à protéger les Canadiens contre un large éventail de menaces et de risques.

Le président: Malheureusement, nous devons en rester là. Désolé.

Je suis mal à l'aise. Je ne cesse de vous interrompre, madame Bossenmaier.

Nous passons maintenant à M. Paul-Hus, que je n'ai jamais interrompu.

[*Français*]

M. Pierre Paul-Hus: Merci, monsieur le président.

Je souhaite la bienvenue à tout le monde.

À la partie 3 du projet de loi, l'article 4 proposé à la nouvelle Loi sur le Centre de la sécurité des télécommunications précise que le gouverneur en conseil peut, par décret, désigner tout ministre fédéral comme responsable du CST. Selon le résumé dont nous disposons, cela donne à penser que n'importe quel ministre du Cabinet pourrait être désigné responsable du CST.

Selon votre expertise, quel ministre serait le plus habilité à remplir ces fonctions? Croyez-vous que ce serait celui des Affaires étrangères, celui de la Défense nationale, celui de la Sécurité publique et de la Protection civile, ou un autre?

● (1235)

[*Traduction*]

Mme Greta Bossenmaier: Monsieur le président, en tant que chef du CST, je peux vous dire que, selon le libellé de la loi, nous relevons du ministre de la Défense nationale. Il est le ministre responsable du Centre de la sécurité des télécommunications.

[*Français*]

M. Pierre Paul-Hus: Selon vous, le ministre de la Défense nationale doit demeurer le ministre responsable de votre organisme, même si le projet de loi C-59 implique une forme d'intégration qui donne à penser que le ministre de la Sécurité publique et de la Protection civile pourrait jouer un rôle plus important.

Selon ce que je comprends, vous croyez que le ministre de la Défense nationale est celui qui devrait assumer la responsabilité du CST. Est-ce exact?

[*Traduction*]

Mme Greta Bossenmaier: Aux termes du projet de loi C-59 et de la Loi sur le CST en particulier, le CST relève du ministre de la Défense nationale.

[*Français*]

M. Pierre Paul-Hus: J'aimerais maintenant parler d'information.

La quantité d'information que vous recueillez est immense. Je ne peux même pas imaginer le nombre de renseignements qui entrent dans les réseaux canadiens. Cela dit, il y a deux volets: les réseaux gouvernementaux et les réseaux civils, c'est-à-dire privés.

Êtes-vous en mesure de recueillir de l'information qui circule dans les réseaux privés? Vous ne vous occupez pas uniquement de l'aspect gouvernemental, mais également de l'aspect privé.

[*Traduction*]

Mme Greta Bossenmaier: Je veux m'assurer de bien comprendre la question, monsieur le président. Je crois comprendre qu'elle porte sur notre mandat en matière de cyberdéfense, dans le cadre duquel nous devons protéger les systèmes du gouvernement du Canada et fournir des conseils et des orientations sur les systèmes importants pour lui. Comme je l'ai dit tout à l'heure, le projet de loi permettrait au CST, à la demande du propriétaire d'un réseau à l'extérieur du gouvernement du Canada et pour un système que le ministre a désigné comme important, de travailler avec le propriétaire du système pour aider à assurer une protection contre les cyberattaques. Nous ne mettons pas l'accent sur l'information canadienne — cela ne fait pas partie de notre mandat —, mais on pourrait nous demander d'aider à protéger un système d'importance contre une cyberattaque, ce qui peut comprendre des éléments non rattachés au gouvernement du Canada.

[*Français*]

M. Pierre Paul-Hus: Par exemple, si le SCRS a besoin d'une information, est-ce votre centre qui doit la chercher dans les réseaux privés, par exemple dans des courriels, pour le compte du SCRS?

[*Traduction*]

Mme Greta Bossenmaier: Désolé, je ne suis pas certain de comprendre la question.

[*Français*]

M. Pierre Paul-Hus: Supposons que je communique avec une personne et que le SCRS soupçonne cette communication de mettre en danger la sécurité du Canada. Il devra toutefois en obtenir la preuve. En vertu de votre mandat, disposez-vous de systèmes vous permettant d'aller chercher cette preuve? Est-ce la façon dont les choses fonctionnent, chez vous?

[*Traduction*]

Mme Greta Bossenmaier: Dom, voulez-vous répondre, à partir de vos échanges de tout à l'heure?

M. Dominic Rochon: Dans cet exemple particulier, le SCRS s'intéresserait à vous en tant que Canadien. La loi lui en donne le mandat. Il pourrait tirer parti de notre mandat d'aide. Il est toujours question de la partie *a*) le renseignement électromagnétique étranger, de la partie *b*) la cybersécurité, et de la partie *c*), le mandat d'assistance. Aujourd'hui, comme dans le cas de cette nouvelle loi, si le SCRS s'intéresse à vous, il doit avoir un mandat légal pour s'en prendre à vous, ce qui signifie qu'il doit obtenir un mandat. S'il nous montre qu'il a un mandat, il n'a pas accès à nos systèmes pour autant. Il nous demande d'agir à sa place. Nous utiliserions alors nos capacités pour les aider à recueillir de l'information. Tous les renseignements recueillis sont mais à part et ils lui sont remis. Ils lui appartiennent. En fait, nous agissons au nom du SCRS.

[*Français*]

M. Pierre Paul-Hus: Si quelqu'un à l'extérieur du pays, par exemple d'un autre gouvernement, communiquait avec un Canadien, il serait donc possible d'aller chercher cette information. Il faudrait alors un mandat d'un juge, bien entendu.

M. Dominic Rochon: Oui.

M. Pierre Paul-Hus: C'est parfait.

Je...

[*Traduction*]

Le président: Malheureusement...

[*Français*]

M. Pierre Paul-Hus: C'est déjà terminé?

Le président: *Désolé*.

[*Traduction*]

Madame Dabrusin, vous avez cinq minutes. Je vous en prie.

Mme Julie Dabrusin: Merci.

Je voudrais aborder quelques aspects. Nous sommes entrés dans certains détails. Je voudrais que vous précisiez certaines choses. Vous avez dit que les systèmes canadiens sont la cible d'un milliard de cyberattaques par jour, et ensuite, dans vos échanges avec M. Dubé, vous avez parlé de l'évaluation des menaces et de l'évolution du contexte dans lequel vous évaluer les menaces.

Pouvez-vous m'aider à comprendre? Dans le projet de loi C-59, quels sont les nouveaux outils qui vous aident à repousser ces attaques dont le nombre est astronomique, et même si important que je n'arrive pas à prononcer les mots? Pourriez-vous m'éclairer?

● (1240)

Mme Greta Bossenmaier: Bien sûr, et je vais demander à Scott Jones, notre chef adjoint à la sécurité des TI, d'intervenir.

Pour répondre à la question, monsieur le président, je vais parler de trois différents éléments du projet de loi.

Tout d'abord, pour prévenir les cyberattaques, nous devons avoir non seulement de bonnes capacités et un personnel exceptionnel qui se consacre à cette mission, mais aussi de bons renseignements pour essayer de comprendre la nature des menaces avant même qu'elles ne touchent le Canada. Le projet de loi renforce notre capacité de continuer à recueillir des renseignements électromagnétiques étrangers, y compris ceux qui se rapportent aux cybermenaces. Voilà un premier élément.

La deuxième chose à souligner, c'est que les dispositions sur la cybersécurité du projet de loi dit tendent à faciliter la communication des renseignements sur les menaces au secteur privé, et il y est également question de l'aider, à sa demande, défendre ses systèmes. C'est une autre façon dont le projet de loi renforcerait notre capacité de contribuer à la cyberdéfense des Canadiens.

Le troisième élément est la défense des cybercapacités. S'il y avait une cyberattaque, au lieu de nous tenir debout avec un bouclier avec lequel nous essaierions de nous protéger contre ces milliards de tentatives malveillantes par jour et d'attendre qu'elles se produisent, nous pourrions essayer de les prévenir. Si nous savons qu'un serveur à l'étranger tente d'infiltrer un système canadien et de voler de l'information aux Canadiens, nous pourrions, grâce à cette mesure législative, essayer de mettre fin à cette attaque avant qu'elle n'atteigne nos systèmes.

Après avoir présenté ce survol, je vais peut-être demander à Scott Jones, notre chef adjoint à la sécurité des TI...

Mme Julie Dabrusin: Si je peux intervenir, vous voulez dire entre autres choses que nous espérons faire diminuer ce milliard de cyberattaques. Pourriez-vous expliquer comment? Ce milliard d'attaque, en quoi cela consiste-t-il? Pouvez-vous me donner des précisions?

Mme Greta Bossenmaier: Bien entendu.

Scott.

M. Scott Jones: En fait, quand nous parlons d'un milliard d'actions malveillantes, nous parlons de toute la gamme, depuis les gens qui fouillent dans nos systèmes pour y déceler des vulnérabilités jusqu'à ceux qui essaient d'en compromettre la sécurité ou d'installer des logiciels malveillants, appelés maliciels, ou qui exploitent toute vulnérabilité existante. Il s'agit d'une vaste gamme d'activités, mais ce que nous essayons de faire, c'est de contrer toute cette gamme d'activités, peu importe d'où elles proviennent. Nous voulons contrer toute activité malveillante à l'égard du gouvernement du Canada, et le nombre est ahurissant. C'est vraiment là où nous allons agir sur différents plans. Premièrement, il faut améliorer les systèmes. Comment faire pour rendre les systèmes plus faciles à défendre? Il s'agit de travailler avec le secteur commercial, de communiquer davantage d'information, de mettre en commun certains de nos outils et de nos techniques, et de faire avancer les choses.

Nous avons offert certains de nos outils. Nous avons mis notre système Assemblyline à la disposition de tous ceux qui pourraient en tirer parti. C'est ainsi que nous défendons, par exemple, le gouvernement et examinons chaque jour des millions de dossiers malveillants.

Le deuxième élément consiste à assurer un niveau de défense qui comble l'écart entre ce qu'il y a de mieux dans le commerce et ce qu'il y a de plus avancé en matière de cyberattaque. Le projet de loi C-59 nous permettrait d'utiliser ces renseignements sur des systèmes essentiels d'importance désignés par leministre.

Le troisième élément, c'est l'échange de renseignements en général, qu'il s'agisse de proposer des conseils et des orientations ou de communiquer ce que nous voyons, ce qui se passe, et de préciser notre capacité de communiquer de l'information.

C'est ainsi que nous regroupons tous ces efforts pour commencer à lutter contre ce milliard d'attaques.

Mme Julie Dabrusin: Merci.

Le président: Merci.

Merci de ces réponses astronomiques et étonnantes à des questions très pénétrantes.

Monsieur Calkins, vous avez cinq minutes. Je vous en prie.

M. Blaine Calkins: Merci, monsieur le président.

J'ai quelques questions à poser. Je m'inquiète vraiment de la sécurité générale. Avant d'être député, j'étais professeur de TI dans un collège. C'était il y a longtemps, c'est-à-dire au moins 12 ans, ce qui signifie que mes compétences en TI sont maintenant à peu près inexistantes. Quoi qu'il en soit, j'ai quelques questions à poser. Je comprends la difficulté et l'énormité de la tâche, et je tiens à le souligner. Pouvez-vous me dire combien de personnes travaillent au CST pour la prévention ou l'élimination proactive des menaces? Quelle est la taille de l'équipe qui travaille là-dessus? Pouvez-vous nous donner ce chiffre?

● (1245)

Mme Greta Bossenmaier: Je pourrais peut-être parler de la composition de l'organisation dans son ensemble. Il est parfois difficile d'analyser le rôle de chacun. Par exemple, quelqu'un peut travailler à la cybersécurité dans notre groupe, examiner les cyberpolitiques, alors que quelqu'un d'autre élabore un moyen de défense et qu'une autre personne recueille des renseignements électromagnétiques étrangers qui pourraient identifier une menace étrangère. Il est difficile de catégoriser les gens...

M. Blaine Calkins: Je voudrais tout de même des chiffres...

Mme Greta Bossenmaier: Le CST compte actuellement un effectif d'environ 2 300 personnes. Nous avons les meilleurs mathématiciens et informaticiens du Canada, les plus brillants, et nous embauchons du personnel, au cas où vous vous intéresseriez encore au domaine de la TI.

M. Blaine Calkins: J'aimerais croire que je travaillerai dans ce domaine aussi longtemps que je le voudrai.

Mme Greta Bossenmaier: Au cas où quelqu'un d'autre...

Nous sommes environ 2 300 personnes dans l'ensemble. L'organisation de M. Jones s'intéresse particulièrement à la sécurité des TI de l'organisation.

Scott, je crois que vous avez fourni des chiffres sur votre organisation par le passé.

M. Scott Jones: À l'heure actuelle, elle compte environ 500 personnes et cet effectif augmente légèrement.

M. Blaine Calkins: Voici ma question, et il ne s'agit pas du tout de critiquer les gens fantastiques que nous avons. Je suis sûr que nous avons les meilleurs et les plus brillants, et je l'apprécie, mais nous savons que la Chine peut compter sur une armée d'environ 200 000 personnes. Nous le savons d'après les reportages que nous avons entendus. Ce sont donc 200 000 personnes qui en affrontent 500. En quoi le projet de loi C-59 améliore-t-il la situation de ces 500 personnes qui doivent se défendre contre ce que 200 000 personnes pourraient faire.

Nous avons vu ce qui se passe actuellement aux États-Unis, avec les sanctions prises contre la Chine sous prétexte de sécurité, d'espionnage, etc. Ce n'est un secret pour personne que le gouvernement chinois est à l'oeuvre depuis des années. En fait, le gouvernement actuel a beaucoup collaboré avec la Chine. Nous avons récemment vendu des actifs à des intérêts chinois, et nous le faisons depuis des années. Il ne s'agit en rien d'une observation partisane. Comment le projet de loi C-59 aide-t-il notre équipe de 500 personnes à affronter une foule de 200 000 personnes? La tâche est redoutable.

Mme Greta Bossenmaier: Merci, monsieur le président.

C'est une tâche redoutable, en réalité. C'est pourquoi nous prenons cette question très au sérieux. Encore une fois, nous sommes dans le domaine depuis 70 ans, et je suis sûr que nous avons la meilleure technologie, le meilleur personnel possible avoir pour travailler à cette tâche, et pour y travailler en partenariat. On dit souvent que c'est un impératif d'équipe. Aucun organisme ne peut avoir toute l'information ni toutes les réponses. Alors nous travaillons en étroite collaboration avec le milieu universitaire. Nous travaillons en étroite collaboration avec d'autres partenaires. Nous travaillons en étroite collaboration avec nos alliés pour acquérir les connaissances et les capacités nécessaires pour nous défendre dans cet environnement très difficile.

En plus de ce qui a déjà été discuté au sujet du budget de 2018... Ce budget propose une augmentation des ressources et un regroupement des capacités cyberopérationnelles du gouvernement du Canada au sein du CST, ce qui aurait un certain effet multiplicateur et il y aurait une source unique de conseils et d'orientations fiables, mais le projet de loi à l'étude nous permettrait également d'exercer des pouvoirs supplémentaires dans l'espace de la cyberprotection. Il s'agit, je le répète, de veiller à ce que nous puissions recueillir des renseignements à l'étranger dans un monde très difficile, percevoir les menaces avant qu'elles ne nous atteignent, échanger plus largement les renseignements sur les menaces et déployer nos cyberoutils — certains des outils perfectionnés dont M. Jones a parlé — sur l'infrastructure privée si la demande est faite et si ce secteur est désigné.

En ce qui concerne la défense des cyberopérations, au lieu de monter une défense seulement à la périphérie de nos réseaux, si nous voyons quelque chose qui se trouve à l'extérieur — dans un pays étranger, sur un serveur, par exemple — et qui vise à détruire l'infrastructure canadienne ou à voler l'information des Canadiens, le projet de loi C-59 autoriserait le CST à essayer de protéger le Canada avant que cette menace n'atteigne nos systèmes.

Le président: Merci, monsieur Calkins.

Monsieur Spengemann, vous avez cinq minutes. Je vous en prie.

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

Ma première question s'adresse au commodore Feltham. Nous avons beaucoup parlé des acteurs non étatiques et des menaces du secteur privé, en tant qu'initiateurs et bénéficiaires d'activités. Qu'en est-il des cyberattaques entre militaires? Quelles sont les tendances actuelles? La Russie constitue un problème. Quels sont les autres problèmes? Quelles tendances pouvons-nous déceler et quelles observations pouvons-nous faire pour l'instant? Y aura-t-il une augmentation de la cyberactivité militaire? Dans l'affirmative, quelle est la composition de cette activité, d'après ce que vous voyez jusqu'à maintenant?

Cmdre Richard Feltham (directeur général, Cyberespace, ministère de la Défense nationale): Merci, monsieur le président.

Je ne peux pas vous donner de chiffres précis sur les acteurs étatiques et non étatiques qui essaient de pénétrer les réseaux dans notre structure et à l'extérieur de celle-ci au quotidien, mais je peux vous dire que les acteurs étatiques et non étatiques essaient de pénétrer les réseaux, et ce nombre augmente de semaine en semaine, presque de jour en jour.

Je ne peux pas vous donner de ventilation précise. Je n'ai pas ces chiffres sous les yeux, mais les acteurs étatiques et non étatiques sont impliqués dans ce domaine, et leur nombre est à la hausse.

● (1250)

M. Sven Spengemann: Est-il juste de dire que des militaires potentiellement hostiles ou ouvertement hostiles investissent dans la cybercapacité et la cybercapacité offensive?

Cmdre Richard Feltham: Nous constatons une augmentation du nombre de personnes qui essaient d'avoir accès à nos réseaux, ce qui laisse entrevoir une augmentation des investissements. Je ne sais pas, mais nous voyons un grand nombre d'entités différentes essayer d'entrer dans nos réseaux.

Vous avez quelque chose à dire, monsieur Burt.

M. Stephen Burt (chef adjoint du renseignement de la Défense, Commandement du renseignement des Forces canadiennes, ministère de la Défense nationale): Du point de vue du renseignement de défense, la réponse simple à votre question est oui. Il s'agit d'une menace de plus en plus grande pour les acteurs des États-nations au sein de leurs forces armées, et c'est une menace transversale. Nous nous y intéressons de la même façon que nous nous intéressons à la croissance, par exemple, des flottes de sous-marins, parce qu'ils sont de plus en plus utilisés par l'ensemble des grands et des petits États.

M. Sven Spengemann: Pouvez-vous décrire vraiment la priorité que le MDN accorde à ce problème de militaires hostiles?

Cmdre Richard Feltham: Monsieur le président, je peux dire que la cybernétique est maintenant certifiée comme un domaine d'opérations en soi — comme terre, air, mer et espace.

Nous avons vu dans la récente politique de défense un mandat élargi pour intégrer la dimension de la cybernétique. Nous défendons les réseaux militaires depuis très, très longtemps, alors je ne voudrais pas laisser entendre que nous ne l'avons pas fait par le passé.

Le fait même que nous nous lancions dans une cyberopération active montre à quel point nous prenons au sérieux cette menace et l'investissement connexe dans ce domaine. Pour répondre brièvement à votre question, je dirais que nous examinons cette question très attentivement. Nous renforçons nos forces et notre capacité de travailler dans ce domaine tous les jours, monsieur.

M. Sven Spengemann: Merci beaucoup.

Ma deuxième question s'adresse à Mme Bossenmaier et à M. Jones.

Vous avez parlé plus tôt de l'environnement dynamique des cybermenaces et donné des précisions sur ce que cela signifie pour les Canadiens. Estimez-vous que le projet de loi C-59 est un instrument suffisamment souple et adaptable pour qu'on puisse regarder au-delà de l'horizon et dans l'avenir.

Madame Bossenmaier, je crois que vous avez parlé de l'IA, et je pense que le quantique est un autre inconnu. Nous ne savons pas vraiment comment ces deux dimensions vont se concrétiser.

L'instrument que nous envisageons et que nous nous apprêtons à mettre dans nos livres est-il suffisamment souple pour faire face aux défis qui risquent de se présenter?

Mme Greta Bossenmaier: C'est une question très importante, monsieur le président, parce que, c'est un environnement très dynamique.

Qu'il s'agisse de l'intelligence quantique ou artificielle, de l'Internet des objets ou de l'informatique en nuage, ou de toute autre technologie nouvelle, nous croyons que ce projet de loi nous permettra de réagir et d'être proactifs dans l'examen de ces menaces pour l'avenir.

Le projet de loi est en quelque sorte indépendant de la technologie en ce sens qu'il parle des diverses menaces qui pourraient survenir et nous donne le pouvoir de lutter contre les menaces non définies de l'avenir.

Scott, vous avez peut-être quelque chose à ajouter.

M. Scott Jones: Je pense que les éléments essentiels sont que le rythme des changements technologiques s'accélère à l'heure actuelle, si bien que ce que nous vivons... Par exemple, en ce qui concerne le quantique, nous travaillons sur plusieurs fronts. Tout d'abord, nous avons le devoir de protéger les renseignements les plus délicats du gouvernement du Canada, et nous nous préparons donc pour cet avenir également.

De plus, en tant qu'organisme national chargé de la cryptologie au Canada, nous sommes les experts en cryptographie, et nous travaillons donc avec des partenaires du secteur privé, du Conseil national de recherches, etc. Nous le faisons depuis 70 ans.

Un grand nombre de ces changements technologiques s'inscrivent dans notre mandat qui consiste à proposer des conseils et des orientations pour préparer l'avenir, et aussi dans le mandat de communication de l'information dans notre travail en tant que partenaires. Internet est interconnecté. Nous avons besoin d'une nouvelle façon d'aborder la question, et il s'agit surtout d'établir des partenariats et de collaborer avec des entreprises, des universités, d'autres ordres de gouvernement et à l'échelle internationale.

M. Sven Spengemann: Merci.

Mon temps de parole doit être écoulé, monsieur le président.

Le président: Merci.

Monsieur Dubé, c'est une bonne journée pour vous aujourd'hui. Vous aurez les trois dernières minutes.

M. Matthew Dubé: Merci. Je vous en suis reconnaissant, monsieur le président.

Je voudrais revenir des questions du même ordre que celles que j'ai déjà posées.

Est-ce que les interactions sur Facebook ou l'information diffusée sur les médias sociaux, bien franchement, sont englobées dans la définition de l'infrastructure mondiale de l'information contenue dans le projet de loi?

Mme Greta Bossenmaier: Je pense que nous avons déjà abordé cette question. Je ne vous répéterai pas la même réponse, qui ne semble pas répondre complètement à la question, mais je demanderai à Dom de vous parler un peu de l'information accessible au public et de sa place par rapport à notre mandat.

M. Matthew Dubé: Comme je n'ai pas beaucoup de temps, pourrais-je obtenir une réponse par oui ou par non.

M. Dominic Rochon: Oui, l'information sur l'IMI, l'infrastructure mondiale de l'information, englobe toutes sortes de choses. Toutefois, notre mandat est très précis: nous ne pouvons pas recueillir de renseignements sur des Canadiens par le biais de renseignements provenant de l'étranger.

● (1255)

M. Matthew Dubé: D'accord, c'est...

M. Dominic Rochon: C'est toujours propre à notre mandat, qui relève de la Loi sur la protection des renseignements personnels. Cette loi...

M. Matthew Dubé: Je comprends cela. Je n'ai pas beaucoup de temps. Excusez-moi.

L'article 23 de la Loi sur le CST proposée, à la partie 3 du projet de loi C-59, dispose que les activités ne peuvent être menées contre des Canadiens. Le paragraphe 24(1) dit: « Malgré les paragraphes 23 (1) et (2) » — et c'est là l'interdiction — « le Centre peut mener les activités ci-après dans la réalisation de son mandat ». Il est ensuite question de la protection de l'information sur ces réseaux.

Les médias sociaux font partie de ces réseaux, et cette information est à risque. Un ministre vous a chargé de veiller à ce que ces renseignements soient en sécurité, et, dans ce cadre, vous êtes exempté des interdictions de collecte de renseignements sur les Canadiens.

Comment pouvons-nous avoir l'assurance que l'information des Canadiens ne sera pas recueillie incidemment, étant donné que la possibilité de la collecte de cette information de façon incidente est expressément prévue dans le projet de loi?

M. Dominic Rochon: Malheureusement, la question est un peu trompeuse.

Devons-nous avoir accès aux communications privées pour protéger les réseaux? Est-ce bien ce que vous insinuez?

M. Matthew Dubé: Non, voici de quoi il s'agit. Si une entreprise engagée par un parti politique ou une maison de sondage est en mesure d'obtenir légalement ses renseignements, ceux-ci sont englobés dans la définition d'information accessible au public. Donc, si cette information peut être recueillie dans le cadre des recherches que vous faites sur la sécurité de ces réseaux — et vous avez été chargé d'examiner ce genre de situation, comme l'a dit cette semaine le ministre par intérim Brison —, n'en viendrions-nous pas à ce que l'information des Canadiens puisse être visée?

M. Dominic Rochon: Abordons la question de cette façon: l'Office de surveillance des activités en matière de sécurité nationale et de renseignement va nous soumettre à des examens pour s'assurer que nous respectons la loi. Il va examiner toutes nos activités.

S'il arrive que nous recueillions des renseignements de cette nature, cet office va nous demander pourquoi nous les avons recueillis. Si nous répondons seulement que nous sommes autorisés à le faire parce qu'il s'agit d'information accessible au public, cela ne va pas suffire. L'Office dira: « Non, la Loi sur la protection des renseignements personnels vous oblige à recueillir des renseignements seulement si ceux-ci se rapportent aux parties *a*), *b*) ou *c*). » L'exemption permet simplement à dire: « Nous avons besoin de cette information parce que nous voulons cibler tel étranger, et nous ne savions pas s'il était canadien ou non. » Il faut une raison. L'information accessible au public ne sert en fait qu'à clarifier les choses pour ces organismes d'examen afin qu'ils ne nous empêchent pas complètement de faire ce que tout le monde fait normalement, c'est-à-dire d'utiliser Internet pour obtenir de l'information afin d'éclairer leurs décisions.

Le président: Malheureusement, nous allons devoir nous arrêter là.

Avant de remercier nos témoins, je tiens à dire que la semaine prochaine, dans une semaine à compter d'aujourd'hui, la réunion a été annulée parce que, jeudi, nous adopterons l'horaire du vendredi. Il n'y aura donc pas de réunion cette heure-ci la semaine prochaine. Mardi, M. Paul-Hus présidera la séance, et je compte sur le greffier pour s'assurer qu'il la préside brillamment, comme je compte qu'il le fera. Je serai absent et je vous souhaite à tous de joyeuses Pâques.

Merci beaucoup de votre contribution à nos délibérations

Mme Greta Bossenmaier: Merci, monsieur le président.

Le président: Voilà qui met fin à aux témoignage sur le projet de loi C-59. Nous passerons à l'étude article par article après le congé de Pâques.

Merci.

La séance est levée.