CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 097 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 13 février 2018

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mardi 13 février 2018

● (1055)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Même si nous sommes en avance de quelques minutes sur l'horaire, je déclare la séance ouverte et demanderais à M. Brown de prendre la parole en premier.

La réunion va durer deux heures. Pendant la première heure, nous allons poser des questions selon un ordre officiel. Pendant la deuxième heure, je m'attends à ce que la structure soit un peu moins rigide, alors que nous examinerons en détail le projet de loi C-59.

Je remercie les fonctionnaires du ministère de leur intérêt à l'égard des délibérations du Comité. C'est l'occasion pour les membres du Comité et les fonctionnaires de discuter de manière moins officielle.

Nous allons commencer avec M. Brown.

M. Malcolm Brown (sous-ministre, ministère de la Sécurité publique et de la Protection civile): Merci beaucoup, monsieur le président.

Je vais présenter une déclaration liminaire, puis je pense que ma collègue Shelly, du Centre de la sécurité des télécommunications, fera aussi une déclaration liminaire.

Je suis heureux d'avoir l'occasion de comparaître avec mes collègues aujourd'hui pour discuter du projet de loi C-59, Loi de 2017 sur la sécurité nationale.

Comme vous pouvez le constater, je suis accompagné de fonctionnaires du portefeuille de la Sécurité publique, dont la GRC et le SCRS, du Centre de la sécurité des télécommunications et du ministère de la Justice.

[*Français*]

Je tiens tout d'abord à remercier tous les membres du Comité d'examiner ce projet de loi.

[*Traduction*]

Comme vous le savez, le projet de loi est le point central du mandat du ministre Goodale en ce qui concerne la sécurité nationale. C'est aussi le fruit d'une consultation publique nationale sans précédent, au cours de laquelle votre comité a joué un rôle important.

Les consultations entreprises par Sécurité publique Canada et le ministère de la Justice comprenaient un questionnaire en ligne, des assemblées publiques aux quatre coins du pays, une mobilisation dans les médias sociaux et j'en passe. Au total, des dizaines de milliers de points de vue ont été entendus, recueillis, consignés et analysés.

Bien entendu, votre comité a lui-même tenu de nombreuses réunions portant sur la sécurité nationale.

[*Français*]

Le projet de loi tient compte de tous ces apports — ceux des citoyens, des parlementaires, des dirigeants communautaires, des experts de la sécurité nationale et des universitaires.

[*Traduction*]

Le projet de loi C-59 compte trois thèmes principaux.

Premièrement, il vise à accroître la reddition de comptes et la transparence. Pour ce faire, il propose de créer le poste de commissaire au renseignement et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. Ce poste et cette entité viendraient compléter les travaux du nouveau Comité des parlementaires sur la sécurité nationale et le renseignement.

Deuxièmement, le projet de loi vise à respecter les engagements au titre du mandat prévus dans l'ancien projet de loi C-51. Il s'agit notamment de révisions proposées aux activités de réduction de la menace en vertu de la Loi sur le Service canadien du renseignement de sécurité, de modifications au Code criminel, d'améliorations à la Loi sur la sûreté des déplacements aériens et de révisions à la Loi sur la communication d'information ayant trait à la sécurité du Canada.

Troisièmement, le projet de loi vise à faire en sorte que les organismes canadiens de sécurité nationale et de renseignement puissent s'adapter à l'évolution des menaces à la sécurité. Cela comprend des mesures comme la modernisation de la Loi sur le SCRS, l'édiction de la Loi sur le Centre de la sécurité des télécommunications et d'autres mises à jour législatives.

● (1100)

[*Français*]

Bref, le projet de loi C-59 est conçu pour mettre à jour et moderniser le cadre de sécurité nationale du Canada en fonction des réalités actuelles. Son objectif global est de protéger les Canadiens tout en préservant nos droits et nos libertés.

[*Traduction*]

Pour s'assurer que le projet de loi atteint cet objectif, le ministre Goodale a exprimé son intention de procéder à un examen et à une analyse en profondeur de son contenu tout au long du processus parlementaire.

Depuis l'été dernier — et les travaux se poursuivent cette année —, des fonctionnaires de Sécurité publique Canada et des responsables du milieu de la sécurité et du renseignement mobilisent des intervenants clés. À bien des égards, c'est la suite des conversations qui ont commencé par les consultations sur la sécurité nationale qui ont été menées en 2016 et que j'ai mentionnées plus tôt.

[*Français*]

Ces discussions et ces interactions n'ont pas seulement eu pour visée de répondre aux questions techniques concernant le contenu du projet de loi, mais aussi, et surtout, de recevoir une rétroaction et des commentaires sur des façons d'améliorer le projet de loi.

[*Traduction*]

Nous avons eu des rencontres et des échanges avec le Commissariat à la protection de la vie privée du Canada, le Comité de surveillance des activités de renseignement de sécurité, le Bureau du commissaire du Centre de la sécurité des télécommunications et la Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada.

[*Français*]

Nous avons aussi eu plusieurs échanges avec d'éminents universitaires du domaine de la sécurité nationale pour recevoir une rétroaction constructive visant à faciliter l'atteinte des objectifs du projet de loi. Je puis vous assurer que ces discussions ont été très utiles.

[*Traduction*]

De même, nous nous intéressons vivement aux délibérations de votre comité, notamment aux témoignages et aux mémoires détaillés que l'on peut consulter sur le site Web du Comité. Je souligne aussi que, même si cet élément est distinct du projet de loi C-59, le gouvernement a annoncé en juin qu'il adopterait un engagement de transparence en matière de sécurité nationale, qui s'appliquera à l'ensemble de l'appareil fédéral de sécurité nationale. Sécurité publique Canada remplit un rôle de leadership et de coordination eu égard à la mise en oeuvre de cet engagement. II soutient aussi la mise en place et le fonctionnement d'un groupe consultatif. Ces travaux viendront s'ajouter aux objectifs ultimes poursuivis par le projet de loi C-59.

[*Français*]

Le ministre Goodale cherche à avoir une conversation ouverte et étoffée pour s'assurer que ce projet de loi sera le meilleur possible.

[*Traduction*]

C'est dans cet esprit que mes collègues et moi comparaissons devant vous aujourd'hui. Nous serons heureux de répondre à vos questions sur le projet de loi.

Merci beaucoup, monsieur le président.

Le président: Merci.

Madame Bruce, vous avez la parole.

Mme Shelly Bruce (chef associée, Centre de la sécurité des télécommunications): Merci.

[*Français*]

Monsieur le président, distingués membres du Comité, je suis chef associée du Centre de la sécurité des télécommunications. Je vous remercie de cette invitation à participer à votre étude du projet de loi C-59, qui édicte la Loi sur le Centre de la sécurité des télécommunications, le CST.

Je suis heureuse d'être ici aujourd'hui afin de clarifier et d'expliquer certains aspects de cet important texte législatif.

[*Traduction*]

Permettez-moi d'abord de citer les propos que le ministre Sajjan a tenus lorsque la Chambre des communes a été saisie pour la dernière fois du projet de loi. Le ministre a déclaré ce qui suit:

> Il n'y a pas d'obligation plus importante que celle d'assurer la sécurité des Canadiens au pays et à l'étranger. Le projet de loi C-59 accorderait au CST les pouvoirs et les outils nécessaires pour adhérer aux normes les plus rigoureuses en matière tant de sécurité que de reddition de comptes et de transparence.

Le CST aide à assurer la sécurité des Canadiens depuis plus de 70 ans, en produisant du renseignement étranger de premier plan sur les menaces contre la sécurité nationale du Canada et ses forces armées déployées et en protégeant les informations et les systèmes d'information les plus sensibles du Canada. Pour remplir ce mandat important, les gouvernements qui se sont succédé au cours de cette période se sont attendus à ce que le CST se penche sur les priorités du jour, à ce qu'il ait constamment une longueur d'avance par rapport aux menaces mondiales en constante évolution, à ce qu'il suive l'évolution rapide de la technologie et à ce qu'il relève ces grands défis tout en protégeant la vie privée, les droits et les libertés des Canadiens. C'est à cela que serviront les nouveaux mécanismes de reddition de comptes et les nouveaux pouvoirs prévus dans la Loi sur le CST. Ces pouvoirs modernisés permettront au CST de protéger le Canada et les Canadiens contre les menaces mondiales, notamment les cybermenaces, tout en s'adaptant à la technologie en évolution rapide. De plus, grâce aux nouvelles mesures de reddition de comptes, les activités de l'organisme feront l'objet d'autorisations et d'examens, et elles seront aussi transparentes que possible.

Depuis que le Comité a entrepris l'étude du projet de loi, un certain nombre de questions importantes ont été soulevées. Je profite de l'occasion pour vous présenter les réponses à quelques-unes des questions qui reviennent le plus souvent.

Premièrement, j'aimerais aborder la disposition du projet de loi portant sur l'information accessible au public. Certains se demandent comment le CST se servira de l'information accessible au public et quel pourrait en être l'impact sur la vie privée des Canadiens. Précisons que cette disposition ne servira qu'à permettre au CST d'effectuer des recherches de base à l'appui de son mandat dans des ressources publiques auxquelles toute personne au Canada peut avoir accès. Le CST n'utilise pas et n'utilisera jamais de l'information accessible au public pour enquêter ou pour monter un dossier sur des Canadiens ou des personnes se trouvant au Canada. De telles activités ne font pas partie du mandat du CST, et l'organisme prend son mandat très au sérieux.

La Loi sur le CST proposée renforce cette notion en exigeant expressément que le CST mette en place des mesures pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à l'utilisation, à la conservation et à la divulgation d'information accessible au public.

Comment le CST se servira-t-il de l'information accessible au public? Je vais vous présenter brièvement trois exemples. Premièrement, nous pourrions utiliser de l'information accessible au public pour ajouter des renseignements généraux à un rapport de renseignement étranger ou de cybersécurité. Deuxièmement, nous pourrions nous en servir pour déterminer la nationalité d'une personne ou d'un organisme. Troisièmement, nous pourrions l'utiliser pour consulter des manuels techniques associés à des technologies ou à des infrastructures nouvelles.

Le CST n'utiliserait en aucune circonstance cette disposition pour avoir accès à de l'information obtenue illégalement. Les données piratées ou volées ne constitueraient pas de l'information accessible au public aux termes de la Loi sur le CST.

On a aussi posé des questions au Comité sur le volet proposé du mandat du CST qui porte sur les cyberopérations actives, dont des questions sur la façon dont ces cyberopérations seraient utilisées et sur leur incidence possible sur la vie privée des Canadiens. Comme il s'agit d'un nouveau pouvoir pour le CST, j'aimerais apporter quelques éclaircissements. Les cyberopérations actives autoriseraient le CST, en vertu d'un cadre juridique strict et d'autorisations provenant des plus hauts échelons du gouvernement, de prendre des mesures en ligne pour contrecarrer les menaces étrangères, pour mener des activités visant à protéger nos institutions démocratiques, pour contrer les plans de groupes terroristes et extrémistes violents ou pour freiner les cyberattaques perpétrées par des États étrangers. Par exemple, le CST pourrait mener des cyberopérations actives pour empêcher un terroriste d'utiliser son téléphone cellulaire pour faire exploser une bombe dans une voiture piégée; il pourrait empêcher des terroristes de communiquer entre eux en perturbant leur infrastructure de communications; ou il pourrait entraver secrètement les activités d'un auteur de menaces étranger qui tente de perturber le processus démocratique du Canada.

La loi proposée définit clairement les limites relatives à ces pouvoirs et interdirait au CST de diriger des cyberopérations actives contre des Canadiens ou des personnes se trouvant au Canada, ou encore contre l'infrastructure mondiale de l'information au Canada. La loi proposée exigerait également que ces activités soient raisonnables et proportionnelles. De plus, elle interdirait spécifiquement au CST de causer des lésions corporelles à une personne ou la mort de celle-ci, ou de tenter intentionnellement d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie.

J'aimerais maintenant souligner le principal changement apporté aux modalités régissant les autorisations ministérielles.

● (1105)

Le projet de loi C-59 s'appuie sur le régime actuel d'autorisations ministérielles, mais il en élargit l'application et met en place de nouvelles fonctions importantes d'examen et de surveillance. En vertu de la loi proposée, le CST devra obtenir une autorisation ministérielle avant de mener une activité qui entrave l'attente raisonnable qu'un Canadien ou une personne se trouvant au Canada peut avoir à l'égard du respect de sa vie privée, ou qui contrevient à une loi fédérale.

Toutes les activités de renseignement étranger et de cybersécurité du CST devraient être approuvées par le ministre de la Défense nationale et le commissaire au renseignement. Les cyberopérations actives et défensives ne constituent pas des activités de collecte d'information et ne peuvent pas être dirigées contre des Canadiens ou des personnes se trouvant au Canada. Elles devraient être approuvées à la fois par le ministre de la Défense nationale et par le ministre des Affaires étrangères. Toutes les activités du CST seraient également assujetties à des examens complets menés par des organes d'examen indépendants.

[*Français*]

Monsieur le président, je conclurai en remerciant le Comité de nous avoir invités, mes collègues et moi, à témoigner aujourd'hui.

Je vous remercie de prendre part à ces délibérations importantes sur la Loi sur le Centre de la sécurité des télécommunications. Nous serons heureux de répondre à vos questions.

Merci.

[*Traduction*]

Le président: Merci, madame Bruce. Bienvenue au Comité. Je crois que c'est la première fois que vous témoignez devant notre comité. J'espère que vous aurez l'occasion de revenir.

Je pense que cela conclut les exposés officiels.

Monsieur Spengemann, vous disposez de sept minutes.

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

Je remercie les témoins d'être ici aujourd'hui. Je vous remercie de vos services et de votre expertise.

J'aimerais d'abord poser une question à M. Brown.

Monsieur Brown, pour la gouverne du Comité, pourriez-vous présenter brièvement votre évaluation des menaces stratégiques auxquelles le pays fera face en 2018, en vous attardant aux deux menaces principales, soit les cyberactivités et les risques d'attentats terroristes, de violence, d'extrémisme et de radicalisation, que ce soit de source intérieure ou d'inspiration étrangère?

Quelles comparaisons faites-vous entre ces deux menaces et devrions-nous tenir compte d'autres menaces en 2018?

M. Malcolm Brown: En six minutes?

M. Sven Spengemann: Pas pour cette question, s'il vous plaît. J'en ai d'autres pour vous.

Un député: Vous auriez besoin d'une heure et demie environ pour celle-ci.

M. Malcolm Brown: Sérieusement, je vais tenter de répondre à votre question, mais mes collègues pourront me corriger ou préciser mes propos.

Je pense que vous avez cerné deux des enjeux principaux. Il va sans dire que, à l'heure actuelle, les menaces sont multidimensionnelles, que ce soit sur le plan de la lutte contre le terrorisme ou des réalités auxquelles nous devons tous faire face, en tant que particuliers ou membres d'une entité donnée, ou encore sur les plans social ou professionnel ou en tant que gouvernement, qui doit composer avec des cybermenaces.

Je dois aussi ajouter que, selon moi, nous continuons de faire face à des menaces traditionnelles. Des documents rendus publics par Sécurité publique Canada et le SCRS révèlent clairement que les menaces sont plus complexes que celles qui ont été mentionnées tout à l'heure. Il s'agit notamment des activités traditionnelles de collecte de renseignements réalisées par des pays qui sont des concurrents du Canada ou qui veulent lui causer du tort. En outre, pour ce qui est de la lutte antiterroriste, nous allons continuer de faire face à des menaces de sources à la fois étrangères et intérieures.

Je pourrais très facilement utiliser tout le temps qui vous est alloué, mais je pense qu'il s'agit d'un bon aperçu de la situation. Je vous invite à poser d'autres questions.

● (1110)

M. Sven Spengemann: En résumé, serait-il juste de dire que, dans le cadre de notre étude actuelle, nous devrions accorder autant d'importance au risque de violence — terrorisme et extrémisme — qu'au risque de cyberattaques?

M. Malcolm Brown: L'un des aspects les plus difficiles du travail réalisé par le personnel des organismes représentés ici aujourd'hui, c'est de jongler constamment avec ces différentes menaces. La réalité, c'est que les organismes passent leur temps à examiner attentivement les menaces que vous avez décrites et celles que j'ai cernées.

Dans tous les cas, il est toujours très difficile d'atteindre un juste équilibre.

M. Sven Spengemann: Je vous remercie. Votre réponse est très utile.

Dans quelle mesure croyez-vous que, dans sa forme actuelle, le projet de loi tient compte de ce qu'on pourrait appeler les « incertitudes inconnues », surtout dans le domaine cybernétique? Par exemple, pour ce qui est des cybermenaces liées à l'intelligence artificielle et à l'informatique quantique, le projet de loi est-il suffisamment souple pour que nous puissions faire face aux enjeux nouveaux, sur lesquels nous ne nous sommes peut-être pas penchés?

M. Malcolm Brown: Il est difficile de prédire l'avenir. Je dirais que, lors de la conception du projet de loi, on s'est efforcé de... Nous savons que nous ne faisons pas ces choses régulièrement. La dernière fois qu'on a procédé à une réforme ou à un examen important de toutes les caractéristiques du système, c'était il y a une génération. Je pense que les conseils que nous avons tous donnés — et qui se reflètent dans la décision prise par le gouvernement — visaient à créer un cadre suffisamment souple pour qu'on puisse réagir aux nouvelles menaces.

M. Sven Spengemann: Merci beaucoup.

Ma prochaine question s'adresse à Mme Bruce.

Je vous remercie de vos précisions au sujet des cyberopérations actives. Je pense que les Canadiens savent que certaines questions ne sont pas évidentes à leurs yeux. Ils savent qu'il s'agit d'un milieu complexe et qu'ils ne sont pas toujours conscients des mesures qui doivent être prises pour contrer une menace. Dans votre exposé, vous avez cité quelques exemples, dont le fait de désactiver un téléphone cellulaire qui pourrait être utilisé pour faire exploser une bombe. Par ailleurs, il va sans dire qu'on ne prendrait aucune mesure pour menacer ou supprimer des vies. Qu'en est-il des dommages collatéraux, par exemple si l'interruption d'une partie du réseau électrique cause des problèmes à l'infrastructure civile et met des personnes en danger, sans toutefois leur faire courir un risque de mort? Des gens pourraient se demander ce qui arriverait si, par inadvertance, on coupait le courant dans un hôpital. Pour la gouverne du Comité, pourriez-vous préciser davantage ce que pourraient être les règles d'engagement en la matière?

Mme Shelly Bruce: Comme vous l'avez dit, le milieu est extrêmement complexe. Dans le cadre de son mandat traditionnel en matière de renseignement étranger et de cybersécurité, le CST est en mesure de définir le contexte dans lequel une cyberopération active pourrait être menée. Il faut effectuer beaucoup de recherche et de travail et recueillir énormément de renseignements pour comprendre les cibles et les infrastructures étrangères, leurs liens et les répercussions possibles si une cyberopération était lancée. Il faut donc procéder à de nombreuses analyses en vue de proposer des options au gouvernement. Celui-ci doit aussi déterminer s'il souhaite ou non que le CST mène une cyberopération active contre un objectif de grande envergure. Ces activités sont donc soumises à d'importantes restrictions, y compris la nécessité qu'elles soient raisonnables et proportionnelles. Deux ministres — le ministre de la Défense nationale et le ministre des Affaires étrangères — doivent approuver l'autorisation et être conscients des répercussions éventuelles.

Mon collègue pourrait vous parler de certaines des autres restrictions et limites, dont vous pourriez tenir compte dans vos décisions.

● (1115)

Le président: Vous pourrez peut-être répondre à cette question plus tard parce que notre temps est malheureusement écoulé.

Monsieur Paul-Hus.

[*Français*]

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

Bonjour à tous. Je vous remercie de votre présence, qui nous est très utile.

Ma première question concerne le financement des groupes terroristes. Elle s'adresse à M. Brown comme à n'importe qui d'entre vous.

M. Michael Nesbitt a comparu devant le Comité. Il a manifesté son inquiétude en disant que le Canada court le risque d'être le théâtre d'activités de financement du terrorisme et d'autres activités. C'est donc une possibilité.

De son côté, par l'entremise de mon collègue M. Tony Clement, notre parti a déposé le projet de loi C-371, qui est actuellement à l'étude à la Chambre. Ce projet de loi vise à contrer ce qu'on appelle les voies secrètes. Le gouvernement a semblé ne pas vouloir l'appuyer en faisant valoir que le projet de loi C-59 ou les autres lois canadiennes donnent les outils nécessaires pour contrer le financement qui provient de voies secrètes et qui vise à favoriser le terrorisme.

Avez-vous quelque chose à dire là-dessus?

M. Malcolm Brown: Je vais commencer à répondre et mes collègues pourront compléter ma réponse.

[*Traduction*]

Le gouvernement estime que les modifications proposées dans le projet de loi C-59 au cadre gouvernemental suffisent pour corriger les problèmes associés au financement des activités terroristes. De façon générale, dans le contexte du projet de loi C-59, le gouvernement est ouvert aux suggestions. Quant au projet de loi d'initiative parlementaire que vous avez mentionné, je pense qu'il y a des considérations pratiques qui le rendent franchement problématique.

Cela dit, je crois que nous cherchons constamment à nous assurer que tous les organismes possèdent les outils nécessaires pour s'attaquer aux défis relatifs au financement des activités terroristes. Il y a diverses mesures que nous pouvons prendre en nous servant des outils en place qui, à notre avis, nous permettront de réagir en conséquence. J'inviterai maintenant mes collègues à intervenir sur la question, s'ils le souhaitent.

Gilles.

[*Français*]

Sous-commissaire Gilles Michaud (sous-commissaire, Police fédérale, Gendarmerie royale du Canada): De manière pratique, ce qu'on voit sur le terrain, en ce qui a trait au financement du terrorisme, est vraiment lié à tous nos dossiers d'enquête. Nous cherchons toujours à découvrir s'il pourrait y avoir un volet de financement du terrorisme.

Cependant, nous faisons toujours face au défi de l'utilisation des fonds. Il nous est très difficile de prouver de quelle manière l'argent a été utilisé parce qu'il l'est dans des pays où il n'y a pas de protocole d'échange d'information ni de protocole qui réponde aux normes requises pour appuyer la preuve au Canada.

Nous travaillons activement, comme M. Brown l'a indiqué. Nous croyons que, par l'entremise d'autres mécanismes, nous avons actuellement les outils nécessaires au partage d'information et des renseignements financiers, ce qui nous permet d'obtenir au moins un portrait de la situation et nous concentrer sur certaines cibles. Par contre, encore une fois, le défi demeure toujours de recueillir de l'information et d'arriver à apporter des preuves qui répondent aux normes des cours canadiennes.

M. Pierre Paul-Hus: D'accord. Je vous remercie.

Ma prochaine question porte sur le partage de l'information. L'ancien directeur du SCRS a dit au Comité que, bien qu'il ne les ait pas comptées, le nombre de fois où les mots « protection de la vie privée » sont mentionnés dans ce projet de loi est vraiment stupéfiant. Il s'est dit tout aussi favorable à la protection de la vie privée que tout le monde, mais qu'il se demandait parfois si le fait que nous mettions autant l'accent sur ce sujet ne ferait pas peur à certaines personnes en ce qui concerne la sécurité nationale.

Pouvez-vous commenter cette observation?

● (1120)

[*Traduction*]

M. Malcolm Brown: Je vais laisser ma collègue, Tricia Geddes, répondre au nom du Service canadien du renseignement de sécurité.

Mme Tricia Geddes (directrice adjointe, Politiques et partenariats stratégiques, Service canadien du renseignement de sécurité): Bien sûr. À mon avis, il est très clair que, grâce au projet de loi, nous disposerons des pouvoirs et des outils nécessaires pour mener nos enquêtes. Afin de pouvoir nous acquitter de notre mandat, il est crucial que nous obtenions la confiance des Canadiens et que nous le fassions d'une manière qui protège leur vie privée. Je pense que le projet de loi a atteint ces deux objectifs.

[*Français*]

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

Nous avons également entendu M. Fadden parler de la Chine, qui employait quelques 200 000 personnes pour mener des cyberopérations.

Pensez-vous que les pouvoirs accordés par le projet de loi C-59 ouvrent la voie à une intervention plus efficace contre la menace chinoise dans le cyberespace?

M. Malcolm Brown: Je peux commencer à répondre, et je passerai ensuite la parole à Mme Bruce.

Je dirais que oui, sans aucun doute. Je suis certain que la modernisation de

[*Traduction*]

nos ressources d'intervention en cas de menace, en vertu du cadre consolidé, aurait dû être faite depuis longtemps.

Je tiens aussi à préciser que le gouvernement mène actuellement un examen de la stratégie de cybersécurité et que ses résultats seront connus en temps et lieu. C'est là un autre élément de réponse à votre question.

Auriez-vous quelque chose à ajouter, Shelly?

[*Français*]

Mme Shelly Bruce: Je vous remercie de votre question.

Je vais répondre en anglais parce que j'en connais beaucoup mieux le vocabulaire.

[*Traduction*]

Je suis d'accord avec Malcolm en ce qui concerne notre environnement opérationnel. Nous faisons face à des cybermenaces croissantes. Les acteurs étatiques et non étatiques hostiles se servent d'Internet. Nous observons aussi une croissance et une évolution rapide des technologies au sein du cyberespace. De plus, certaines de nos cibles et nos propres concitoyens utilisent cet espace. Pour toutes ces raisons, il est fort difficile pour nous de fonctionner dans un tel environnement, mais la mesure législative nous donnera des outils et des capacités de pointe qui nous permettront de régler certains des problèmes existants. Grâce au projet de loi, le Centre de la sécurité des télécommunications pourra également utiliser ses capacités et son expertise pour se livrer à des activités en ligne visant à contrer ou à neutraliser des menaces en ligne avant qu'elles se concrétisent ou qu'elles déclenchent une crise au Canada.

Le président: Merci, monsieur Paul-Hus.

Monsieur Dubé, vous avez sept minutes. Allez-y.

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

Je m'excuse à l'avance si je semble impoli, mais mon temps de parole est assez limité.

Madame Bruce, vous avez dit que votre mandat est important. S'agit-il d'un mandat prescrit par la loi ou d'un mandat que votre organisme s'est lui-même confié?

Mme Shelly Bruce: C'est un mandat prescrit par la loi.

M. Matthew Dubé: Merci.

C'est le ministre de la Défense nationale qui est responsable des pouvoirs prévus dans le projet de loi. Quelqu'un autour de la table peut-il donc m'expliquer pourquoi ces pouvoirs ont été ajoutés à un projet de loi présenté par le ministre de la Sécurité publique? Ce dernier comparaît devant notre comité, qui est saisi du projet de loi même s'il ne possède pas la mémoire institutionnelle qu'aurait le comité de la défense nationale.

M. Malcolm Brown: Pour répondre brièvement à votre question, je ne pense pas que nous devrions décider à quel comité le projet de loi devrait être renvoyé… Nous ne sommes que de simples fonctionnaires. Nous comparaissons devant tout comité qui aimerait nous poser des questions. Il ne nous appartient pas de nous prononcer sur la pertinence de la tribune.

M. Matthew Dubé: Je comprends. Alors, pourquoi les mesures concernant le CST sont-elles spécifiquement incluses dans le projet de loi?

M. Malcolm Brown: C'est parce que le projet de loi vise à mettre à jour un cadre fédéral de sécurité nationale qui englobe les activités d'organismes comme le CST.

M. Matthew Dubé: Merci.

Madame Bruce, je reviens à vous. Dans l'article 25 de la partie 3, qui porte sur la protection de la vie privée, on peut notamment lire « et à la divulgation ». Le ministre a expliqué que le terme « divulgation » qui est maintenant utilisé dans la Loi sur la communication d'information ayant trait à la sécurité du Canada renvoie à des renseignements déjà en la possession de divers organismes ou ministères. Quand vous parlez de la divulgation d'information obtenue à l'aide de cette recherche, cela signifie-t-il que les renseignements pourraient être échangés entre divers organismes et ministères?

Mme Shelly Bruce: Allez-y.

M. Scott Millar (directeur général, Politiques stratégiques, planification et partenariats, Centre de la sécurité des télécommunications): Bonjour.

Je tiens à préciser que, en vertu de nos pouvoirs actuels, nous échangeons maintenant des renseignements avec d'autres ministères et organismes. Nous le faisons par l'entremise d'un rapport de produit final, d'un rapport de renseignement. Cela ne changera pas. Lorsque nous échangeons ces renseignements, nous nous servons de mesures de protection des renseignements personnels, qui sont soumises à un examen. Le processus que nous utilisons est passé en revue. Cela fait 20 ans que nous procédons ainsi. La mesure législative inscrira donc dans la loi une pratique qui existe déjà au Centre de la sécurité des télécommunications.

● (1125)

M. Matthew Dubé: Je pose la question à cause d'une des réponses que vous avez fournies… Vous avez dit que vous n'utilisez pas les renseignements que vous recueillez en vertu de l'article 24 pour créer des profils ou mener des enquêtes. Est-ce que cela empêche d'autres organismes de le faire si vous leur communiquez les renseignements que vous avez recueillis, et que vous ne pouvez rien faire avec cette information à cause de votre mandat?

Mme Shelly Bruce: Quand nous disons avoir besoin de mesures de protection des renseignements personnels pour la divulgation d'information, c'est parce que nous pourrions tomber sur une entité, une adresse IP, un particulier ou une entreprise que nous ne connaissons pas dans le cadre de nos activités de renseignement étranger ou de cybersécurité. Nous devons donc effectuer des recherches dans des sources ouvertes pour mettre les choses en contexte et nous assurer que nous comprenons ce à quoi nous avons affaire.

S'il s'avère que le particulier, l'entreprise ou le propriétaire de l'adresse IP est canadien, nous mettrons en place des mesures pour cacher son identité si ces renseignements sortent du CST. Notre objectif est de protéger cette information.

M. Matthew Dubé: Le projet de loi indique que vous prenez des mesures, mais ce sont essentiellement des mesures internes… Par exemple, il n'y a pas de période de conservation, comme c'est souvent le cas.

Pourriez-vous préciser au Comité les mesures que vous prenez pour protéger les renseignements personnels recueillis en vertu de l'article 24?

Mme Shelly Bruce: Comme je l'ai dit, les renseignements qui sont recueillis... En fait, ils ne sont pas recueillis, mais consultés. Ce sont des données de recherche que nous utilisons. Si elles se rapportent à la communication de renseignements étrangers ou de renseignements sur la cybersécurité, nous le mentionnerons, mais nous dissimulerions la mention. Nous supprimerions tous les renseignements canadiens et nous les remplacerions par un terme générique. Par exemple, au lieu d'inscrire le nom de l'adresse IP canadienne ou du Canadien, nous dirions « une personne canadienne » ou une « adresse IP canadienne ».

M. Scott Millar: J'aurais quelque chose à ajouter.

Comme il a déjà été dit, nous ne pouvons pas diriger nos activités contre des Canadiens. Nous les dirigeons vers des cibles étrangères. Si une cible étrangère parle d'un Canadien ou, disons, appelle une personne au Canada et que nous en prenons connaissance, nous devons détruire ces renseignements aux termes de la loi actuelle, sauf s'ils sont essentiels aux affaires internationales, à la sécurité et à la défense. Si nous décidons de conserver l'information, nous devons en prendre compte. Nous devrions expliquer la façon dont nous avons obtenu l'information, la manière dont nous l'avons détruite ou, si nous l'avons conservée, la raison pour laquelle nous avons pris cette décision. C'est quelque chose qui fait maintenant l'objet d'un examen par le commissaire du CST.

Notre système comprend des politiques et des procédures qui sont incluses dans une fiche d'information sur la protection des renseignements personnels sur notre site Web. Cette fiche indique les diverses mesures en vigueur. Le commissaire du CST évalue notre respect de ces mesures.

M. Matthew Dubé: Pardonnez-moi, mais c'est dans l'article 24 qu'on précise que malgré l'article 23, qui interdit de cibler des Canadiens ou des personnes au Canada, il est possible de recueillir de l'information accessible au public pour des raisons données, puis qu'on énumère les raisons.

L'article 25, quant à lui, mentionne ces vagues notions de mesures prises pour protéger les renseignements personnels. Pouvez-vous me signaler la partie du projet de loi qui décrit explicitement ce qui est fait pour protéger les renseignements personnels et où l'on trouve les détails que vous avez fournis sur la destruction de cette information ou la décision de ne pas la conserver? Je ne trouve pas ces renseignements sur l'information recueillie en vertu de l'article 24 dans la mesure législative.

M. Scott Millar: En ce moment, le projet de loi prévoit, sous le titre « Autorisations ministérielles », que le ministre énoncera les mesures de protection des renseignements personnels propres à cette autorisation concernant l'utilisation, la rétention et l'élimination de ces renseignements, et nous sommes tenus d'observer ces mesures. Encore une fois, certains de ces éléments sont énumérés sur notre site Web à l'heure actuelle. Je peux les nommer. Il y a des politiques, des procédures, de la formation et j'en passe.

Je crois qu'il est important de souligner que la seule façon pour nous d'assister un autre organisme de sécurité et d'application de la loi dans la réalisation de son mandat serait pour celui-ci de faire appel à nous en vertu de ses propres pouvoirs légitimes. Le cas échéant, nous l'aiderons, conformément à notre mandat d'assistance, dans les limites de ce pouvoir légitime et de cette activité.

Le Centre de la sécurité des télécommunications est tenu d'avoir des mesures de protection des renseignements personnels pour toutes ses activités, depuis la collecte de renseignements jusqu'à la cybersécurité en passant par la consultation de renseignements publics. Certaines choses pourraient rejoindre nos intérêts en matière de vie privée, alors ces mesures doivent être là.

Il y a tout un éventail de mesures de protection des renseignements personnels pour le genre de recherches générales que nous effectuons, le genre d'activités de collecte de renseignements que nous effectuons pour appuyer les priorités du gouvernement du Canada en matière de renseignement, ainsi que le genre de choses que nous faisons en réponse aux demandes de partenaires.

M. Matthew Dubé: En ce qui a trait à...

Le président: Malheureusement...

J'ai l'intention de laisser un peu plus de marge de manoeuvre dans la deuxième heure, alors je crois que nous pourrons revenir sur bon nombre de ces points.

Madame Damoff, vous avez la parole pour sept minutes, je vous prie.

● (1130)

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

J'aimerais poursuivre dans le même ordre d'idées, car je ne saisis pas encore tout à fait quand cette collecte de renseignements vise les Canadiens. J'ai une ou deux questions.

Vous avez mentionné que vous masquez l'identité, mais que vous conservez ces renseignements. Combien de temps les conservez-vous?

Mme Shelly Bruce: Le Centre de la sécurité des télécommunications a effectivement un calendrier de rétention, mais nous ne les avons pas rendus publics pour l'instant.

Mme Pam Damoff: Ces renseignements finissent-ils par être détruits?

Mme Shelly Bruce: Oui.

Mme Pam Damoff: Cette information est-elle publique?

M. Scott Millar: Nous sommes tenus de les détruire, oui. À l'heure actuelle, le critère est que, si un renseignement n'est pas essentiel pour les affaires internationales, la sécurité ou la défense, alors il doit être détruit. L'observation de ce critère fait ensuite l'objet d'un examen.

Mme Shelly Bruce: Si un renseignement est retenu, alors il est protégé.

Mme Pam Damoff: Qu'arrive-t-il si, en trollant sur Internet, vous trouvez un renseignement essentiel à la sécurité nationale canadienne et qu'il est de source canadienne?

Mme Shelly Bruce: Le Centre de la sécurité des télécommunications ne trolle pas vraiment sur Internet.

Mme Pam Damoff: Pardonnez-moi, c'était la mauvaise expression. Ce que je voulais dire, je suppose, c'est que vous n'êtes pas activement à la recherche de Canadiens...

Mme Shelly Bruce: Absolument pas.

Mme Pam Damoff: ... mais vous êtes présents sur Internet et effectuez de la surveillance. Admettons que, ce faisant, vous découvrez qu'un Canadien participe à des conversations d'intérêt pour la sécurité nationale, sans pour autant commettre un crime. Que faites-vous de cette information?

Mme Shelly Bruce: Comme l'a dit mon collègue, advenant que, dans le cadre de nos activités ciblant des entités étrangères et associées à une exigence de renseignement étranger que le gouvernement nous impose, nous découvrions de l'information sur un Canadien qui n'est pas pertinente pour le renseignement étranger en question, alors nous détruisons cette information.

Mme Pam Damoff: Qu'advient-il si cette information est pertinente pour le Canada? Qu'advient-il si vous découvrez un renseignement pouvant représenter une menace à la sécurité? Vous avez dit « à moins que ce soit une menace pour la sécurité nationale ». Qu'arrive-t-il si vous recueillez de l'information sur un Canadien possiblement impliqué dans une question de sécurité nationale pour le Canada? Vous n'en avisez personne et cette information reste là, tout simplement?

Mme Shelly Bruce: Nous avisons. Si l'information est pertinente pour les rapports en matière de renseignement étranger que nous effectuons à propos d'une menace légitime pour la sécurité du Canada, nous incluons cette information et la consignons dans un produit de renseignement, lequel est distribué aux clients au sein du gouvernement du Canada ayant la cote de sécurité « très secret » qui sont munis des instructions nécessaires pour recevoir cette information. Toutefois, l'information n'identifierait pas explicitement le Canadien. Une expression serait utilisée au lieu des détails précis. Si le client qui reçoit l'information veut comprendre l'information sous-jacente, ce qui se cache derrière cette étiquette, il peut présenter une demande au Centre de la sécurité des télécommunications conformément à la Loi sur la protection des renseignements personnels. Il doit alors en donner la justification, expliquer en quoi cette information est liée à son mandat et pourquoi il a le pouvoir légitime d'obtenir ce renseignement. Alors, le Centre de la sécurité des télécommunications pourra divulguer le renseignement. Toutes ces divulgations sont consignées et examinées annuellement par le commissaire du Centre de la sécurité des télécommunications.

Mme Pam Damoff: Comme je l'ai demandé à plus d'un témoin, ne devrait-on pas exiger l'obtention d'une autorisation ministérielle pour la divulgation de ce genre d'information concernant des Canadiens à d'autres ministères? Certains témoins croient que oui.

M. Scott Millar: Ce qui distingue la saisie de renseignements personnels de celle d'information publique, c'est que tout renseignement que nous recueillons pour lequel il y a une attente raisonnable de protection de la vie privée ou dont la possession risque de nuire à la vie privée tombe dans la portée de l'autorisation ministérielle et de l'examen secondaire du commissaire au renseignement.

Cela nous autorise à entreprendre une série d'activités pour appuyer le mandat de renseignement étranger.

Mme Pam Damoff: Je parle de la divulgation de cette information. Supposons que vous transmettez l'information au SCRS. À l'heure actuelle, il doit en faire la demande, vous acceptez et vous la leur transmettez. Y a-t-il déjà une autorisation ministérielle dans le cadre de ce processus en vertu duquel vous divulguez des renseignements sur des Canadiens à un autre organisme du gouvernement?

M. Scott Millar: Tout ce que je peux dire, c'est que l'autorisation ministérielle énonce des mesures de protection des renseignements personnels. De plus, la Loi sur le Centre de la sécurité des télécommunications proposée prévoit que le ministre désignera qui peut recevoir cette information. Ceci est un nouvel élément dans le cadre de cette désignation ministérielle, alors le ministre participera. Le commissaire participera en procédant à l'examen des activités entreprises dans le cadre d'une autorisation ministérielle, et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement en fera également l'examen.

● (1135)

M. Malcolm Brown: C'est une question vraiment importante, et pas seulement au chapitre de la méthodologie entourant les activités du Centre de la sécurité des télécommunications ou d'autres organismes semblables dans d'autres pays.

La réalité, c'est qu'il y a des couches de protection pour le transfert de renseignements afin de protéger la vie privée, mais également pour faire en sorte que cette information soit transmise rapidement, sans compter que tout cela fait l'objet d'examens. Nous avons toutes les mesures décrites par Scott et Shelly qui régissent cette divulgation. On ne transmet pas de renseignement n'importe comment, à gauche et à droite.

Mme Pam Damoff: Non, ce n'est pas ce que je voulais dire.

M. Malcolm Brown: Je le sais, mais je tenais à ce que ce soit clair.

L'organisme qui reçoit l'information a également toute une série d'obligations régissant la façon dont il traite cette information. Notre ami le commissaire à la protection de la vie privée joue un rôle important dans tout cela. De plus, les gens qui, comme moi, dirigent ces ministères ont des obligations sérieuses pour protéger la façon dont l'information est utilisée ainsi que pour justifier sa rétention pour la période que nous jugeons nécessaire.

Mme Pam Damoff: Je crois que le monde a évolué; il y a 20 ans, la conversation aurait été bien différente. On parle de conversations personnelles. Il peut s'agir de conversations téléphoniques. De nos jours, il y a tellement de renseignements personnels sur Internet, et l'information qu'on peut y recueillir est bien plus vaste. Par conséquent, c'est une conversation très différente de celle qu'on aurait tenue il y a même 10 ans.

M. Malcolm Brown: Oui et non. La manière dont les mandats sont utilisés de nos jours par les autorités et tout le processus que ces organismes doivent suivre pour accéder à l'information est une longue tradition. Oui, c'est différent, mais les principes sous-jacents et le fondement dans la loi sont les mêmes pour ce qui est de la façon dont l'information est traitée. Nous devons mettre nos procédures et nos pratiques à jour, les examiner de temps en temps et nous assurer qu'elles demeurent pertinentes. Je crois que le projet de loi C-59 montre toute une capacité à absorber et à proposer du changement. Il est important de ne pas croire que les choses sont si différentes qu'il faille passer à un nouveau cadre de travail. Cela ne serait pas une solution dans l'immédiat, car nous devons songer aux conséquences.

Je crois que la difficulté, c'est de trouver le bon équilibre de sorte que la façon dont nous gérons l'information tienne compte des préoccupations que vous décrivez, à savoir que l'information n'est pas transmise n'importe comment à gauche et à droite. Les couches de protection inscrites dans le projet de loi sont si considérables que je crois... Nous verrons bien. Je vais m'arrêter, car j'accapare votre temps de parole, mais c'est une question importante. Vous avez entendu des témoins qui estiment que les couches de protection inscrites dans le projet de loi représentent un fardeau trop lourd.

Le président: Oui. Merci, monsieur Brown. Je rappelle aux collègues que nous avons une deuxième heure et que vous pourrez revenir sur ces questions si elles vous préoccupent.

Monsieur Motz, vous disposez de cinq minutes, je vous prie.

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

Merci aux fonctionnaires d'être ici.

Je comprends votre rôle en tant que bureaucrates et votre hésitation à parfois vous exprimer librement devant un comité comme celui-ci sur une question comme celle-ci. Cependant, nous savons qu'il s'agit d'une question de sécurité nationale et que, alors que nous étudions le projet de loi avant la deuxième lecture, c'est une occasion d'apporter tout changement qui est, évidemment, probablement nécessaire.

Je commencerai par vous, madame Bruce, et je poserai la même question à M. Brown.

Vous avez parlé des cyberopérations actives et défensives. Les dispositions législatives prévues dans ce projet de loi énoncent des limites très claires concernant les pouvoirs du CST. De plus, selon ce que je comprends, elles prévoient que les cyberopérations actives ne peuvent viser des Canadiens, peu importe où ils se trouvent dans le monde, ni des personnes se trouvant au Canada.

Êtes-vous convaincue que ces limites et ces interdictions sont appropriées, étant donné le climat actuel de menaces nationales concernant des Canadiens en sol canadien?

● (1140)

Mme Shelly Bruce: Je vous remercie de votre question.

Dans le projet de loi, je crois que les pouvoirs accordés au Centre de la sécurité des télécommunications témoignent de notre domaine d'expertise, c'est-à-dire les cibles étrangères situées à l'extérieur du Canada et les infrastructures étrangères.

Si une menace se matérialise au Canada, la Gendarmerie royale du Canada et le Service canadien du renseignement de sécurité disposent déjà des pouvoirs appropriés afin de gérer ce genre de menace. Je pense que les pouvoirs accordés exploitent les forces du CST et la position qu'il occupe naturellement dans ce réseau mondial.

M. Malcolm Brown: La réponse courte est oui. Je peux répondre oui avec enthousiasme. Je crois que nous sommes bien placés pour être en mesure de gérer la situation. La loi prévoit un éventail beaucoup plus complet de pouvoirs, de même que les protections appropriées. Si vous leur posez la question, je pense que les représentants du Service canadien du renseignement de sécurité ont un avis à ce sujet.

M. Glen Motz: Oui, pour poursuivre sur le même sujet, je veux certainement demander aux représentants du Service canadien du renseignement de sécurité et de la Gendarmerie royale du Canada qui sont ici s'ils sont aussi enthousiastes et offrent le même appui au projet de loi, qui prévoit le soutien législatif dont ils ont besoin pour protéger les Canadiens du terrorisme national.

Mme Tricia Geddes: Oui, je m'exprimerai d'abord au nom du Service.

Je dirais que cela illustre clairement nos pouvoirs et nos outils: l'analyse de données, la réduction des menaces et la façon dont nous travaillons avec des sources humaines. Je pense que les précisions qui ont été apportées sont très importantes.

En ce qui concerne la question posée à Mme Bruce, je dirais que c'est là où nos mandats sont assez complémentaires. En effet, le mandat de réduire les menaces et notre rôle dans les cyperopérations sont évidemment permis au Canada. Par conséquent, c'est là où je pense qu'il existe une belle synergie entre ce que le Centre de la sécurité des télécommunications est en mesure de faire et ce que nous sommes en mesure de faire.

S.-comm. Gilles Michaud: Je peux peut-être ajouter quelque chose du point de vue de l'application de la loi. Le projet de loi porte davantage sur les modifications à apporter au Code criminel et certaines des dispositions qui existent afin de nous aider à assurer la sécurité des Canadiens.

Il ne règle pas les enjeux technologiques auxquels nous sommes confrontés, et la nature de vos questions en est la prémisse. Du point de vue de l'application de la loi, la plus grande lacune est de ce côté; c'est dans notre capacité de travailler, dans le cadre de notre mandat, dans ce nouvel environnement et de composer avec ces nouveaux enjeux.

Cependant, je ne suis pas certain que ce projet de loi permette de régler ces enjeux.

M. Glen Motz: Je vous remercie.

Je vous prie de m'excuser. Au début de mon intervention, j'ai utilisé le terme « bureaucrates ». J'aurais dû dire « fonctionnaires », et je m'en excuse. Cela ne se voulait pas du tout une insulte. Je suis désolé.

Des préoccupations légitimes ont été exprimées au sujet de l'ingérence étrangère dans notre processus électoral qui se serait prétendument produite lors des élections au pays en 2015.

Le projet de loi C-59 contient-il suffisamment de pouvoirs de surveillance pour que nous puissions faire face aux menaces étrangères contre notre processus électoral?

M. Malcolm Brown: Toute la question de l'ingérence étrangère est très complexe. Pour être honnête, il s'agit d'un mélange entre numérique et analogique. En réalité, les objectifs sont les mêmes. Souvent, probablement, les acteurs sont les mêmes. En ce qui concerne les pouvoirs supplémentaires que vous avez déjà abordés avec Shelly Bruce, je dirais qu'ils comblent manifestement une lacune.

Pour ce qui est des autres pouvoirs, l'ingérence est et demeure une préoccupation de longue date des services qui relèvent du portefeuille de la Sécurité publique. Je pense que, grâce à la mise à jour, à la modernisation des outils dans l'ensemble du ministère, nous serons dans une bien meilleure position pour relever ces défis.

Est-ce le dernier mot? Je pense qu'il est risqué de dire que nous avons terminé et que nous n'avons plus besoin d'y penser. C'est une situation que nous étudions de façon permanente, comme c'est le cas avec chaque menace, et nous fournirons des conseils au gouvernement dans l'éventualité de problèmes dus à des lacunes.

● (1145)

Le président: Je vous remercie.

[*Français*]

Monsieur Picard, vous disposez de cinq minutes.

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

Ma question s'adresse aux représentants du Centre de la sécurité des télécommunications.

Ce n'est pas une initiation pour les personnes qui se présentent devant le Comité pour la première fois, mais votre organisme suscite beaucoup d'intérêt dans le cadre légal qui nous intéresse. On parle ici des menaces qui proviennent de l'étranger, étant donné que vous ne vous occupez pas de ce qui se prépare en territoire canadien. Si, dans le cadre de votre travail de surveillance et d'interception, vous tombez sur une conversation qui implique un citoyen canadien, vous êtes obligés de détruire cette information. La défense des droits et libertés et la protection de la vie des Canadiens sont toujours les prétextes invoqués. Cependant, vous devez prouver qu'il y a une menace ou un doute raisonnable de menace pour obtenir les mandats nécessaires pour enquêter.

Comment pouvez-vous prouver qu'une menace existe si, en détruisant des renseignements qui concernent des Canadiens, vous perdez de l'information sur des comportements ou des schèmes de comportement susceptibles de prouver qu'une menace est en train de se développer?

Évidemment, ma question implique que la source est à l'étranger, mais qu'elle compte sur la collaboration d'éléments canadiens.

Mme Shelly Bruce: Je vous remercie de votre question.

[*Traduction*]

Si nous avons intercepté un renseignement étranger qui contient de l'information pertinente au sujet d'un Canadien et qui indique la présence d'un vecteur de menace au Canada ou d'un motif raisonnable de croire que cela pourrait être lié à une menace, nous conservons cette information. Nous ne la détruisons pas.

Je comprends qu'au fil du temps des tendances peuvent se développer, mais ce sont les règles que nous avons. Si, au moment de l'examen, nous déterminons que l'information conservée n'est pas liée au renseignement étranger, à une menace envers le Canada, nous détruirons cette information afin de protéger la vie privée des Canadiens.

[*Français*]

M. Michel Picard: Votre prémisse est bonne dans la mesure où vous considérez que l'information interceptée constitue déjà une menace possible. Cela dit, une personne qui tente de recruter un Canadien ne lui demande pas, lors de leur première conversation, s'il est prêt à tuer pour son pays. C'est rare. Ces gens testent le marché, testent les gens et tiennent des conversations anodines, peu importe la nature des gens qu'ils recrutent. La conversation ne représente aucun intérêt, pour ce qui est d'une menace éventuelle, parce que ces gens ne font que tester le marché.

Cela ne représente-t-il pas une difficulté? À quel moment la conversation anodine fait-elle place à la menace?

[*Traduction*]

Mme Shelly Bruce: Comme nous ciblons des entités étrangères à l'extérieur du Canada, nous devons être très convaincus qu'elles sont liées à une menace étrangère ou à une priorité du gouvernement relative au renseignement étranger. Ce n'est pas parce qu'une personne parle une fois à quelqu'un et que leur conversation est inoffensive que nous arrêtons de cibler l'entité étrangère. Par conséquent, toute conversation subséquente avec cette entité étrangère fera aussi l'objet d'un examen. De plus, au fil du temps, si les analystes de ces cibles perçoivent un changement de comportement, ou s'ils établissent qu'un Canadien est impliqué, ils sauront que cette personne risque davantage de se radicaliser.

[*Français*]

M. Michel Picard: Je vous remercie.

J'aimerais poser une dernière question, plus générale.

Le dernier rapport du ministère sur la menace terroriste fait encore état d'un niveau modéré. Cela n'a pas changé depuis environ quatre ans; le dernier rapport de 2014 faisait aussi état d'un niveau modéré.

Le projet de loi C-59 donne-t-il les outils nécessaires pour maintenir la menace terroriste à un niveau modéré? Avez-vous aussi des outils pour nous aider à réduire cette menace?

M. Malcolm Brown: Bien sûr, j'espère que oui. Sérieusement, il ne fait aucun doute que le projet de loi contient de nouveaux outils importants à cette fin.

● (1150)

[*Traduction*]

C'est un peu un environnement régi par la demande. Est-ce possible de dire qu'aujourd'hui, il y a, disons, 15 menaces, mais qu'avec l'adoption du projet de loi C-59 — ou d'une version du projet de loi —, il n'y aura plus que 14 menaces dans un an? Non, ce n'est pas possible.

Est-ce que je crois — et je pense que c'est l'opinion des organismes — que le projet de loi C-59 prévoit des outils et des atouts importants qui contribueront à réduire les menaces envers le Canada? Ma réponse est la même que celle que j'ai fournie plus tôt: oui, assurément. Est-ce que le projet de loi permettra de réduire toutes les menaces? Non.

Le président: Merci, monsieur Picard.

[*Français*]

Monsieur Paul-Hus, vous avez cinq minutes.

M. Pierre Paul-Hus: Je vous remercie, monsieur le président.

J'ai une brève question à vous poser.

Je voudrais revenir sur le financement étranger. Je sais qu'Affaires mondiales Canada peut avoir une certaine influence, et je regrette que le Comité ait refusé que nous invitions des gens de ce ministère à venir témoigner.

Pour contrer le financement étranger, votre ministère ou un de vos organismes est-il en relation avec Affaires mondiales Canada?

[*Traduction*]

M. Malcolm Brown: Il existe un vaste groupe interministériel qui s'attaque à ces enjeux: le ministère des Finances, Affaires mondiales, le Centre d'analyse des opérations et déclarations financières du Canada, la Gendarmerie royale du Canada, le Service canadien du renseignement de sécurité, notre ministère, de même que certains de nos collègues ici. Il y a un vaste groupe qui se penche sur le financement des organisations terroristes étrangères.

[*Français*]

M. Pierre Paul-Hus: Merci.

J'aimerais avoir des explications et je ne sais pas lequel d'entre vous pourra me les donner.

Plusieurs organismes doivent rendre compte au ministre. Il y a le commissaire au renseignement, le commissaire à la protection de la vie privée, le nouveau Comité des parlementaires. Plusieurs groupes doivent rendre des comptes, tout cela dans le but de protéger la vie privée, mais qu'en est-il du point de vue opérationnel? Je veux savoir comment vous allez interagir avec tous ces groupes et comment cela va fonctionner, surtout dans le cas du SCRS.

Mme Tricia Geddes: Je vous remercie de votre question.

[*Traduction*]

Je suis d'avis que nous avons une obligation envers notre ministre, celle de satisfaire à toutes ces attentes lorsqu'il est question de la protection de la vie privée. Nous sommes tout à fait à l'aise avec l'examen. Nous avons eu une longue relation avec le Comité de surveillance des activités de renseignement de sécurité. Il a été très efficace pour s'assurer que nous respectons les politiques et les procédures concernant la vie privée des Canadiens. D'ailleurs, le nouveau projet de loi prévoit un certain nombre de nouveaux mécanismes pour veiller à ce que les obligations en matière de vie privée soient assumées par le service.

Comme je l'ai dit au début, il est extrêmement important pour nous de faire en sorte que les Canadiens aient confiance en leurs organismes de sécurité. Je ne pense donc pas que ce soit une préoccupation. Les réponses relatives à la protection de la vie privée que nous fournirions au commissaire à la protection de la vie privée ou à nos organismes d'examen seraient les mêmes.

[*Français*]

M. Pierre Paul-Hus: Nous convenons que la protection de la vie privée est importante au Canada, mais tous ces nouveaux éléments peuvent-ils représenter une contrainte pour la sécurité? Le fait qu'il y ait beaucoup d'éléments ne risque-t-il pas de compromettre la sécurité nationale? L'équilibre entre la protection de la vie privée et la sécurité nationale est-il un enjeu pour vous?

[*Traduction*]

Mme Tricia Geddes: Non, pas à mon sens. Comme je l'ai dit, je crois sincèrement qu'il est essentiel d'avoir la confiance des Canadiens. Je pense que les opérations peuvent être ralenties si les organismes de sécurité perdent la confiance des Canadiens ou si, par exemple, nous devons nous arrêter et sécuriser les données. Par conséquent, il est essentiel d'avoir la confiance de la population si nous souhaitons agir rapidement sur le plan opérationnel.

[*Français*]

M. Pierre Paul-Hus: Dans une perspective plus large, on a renvoyé au Comité le projet de loi C-59 avant que ce dernier franchisse l'étape de la deuxième lecture à la Chambre des communes. Le ministre voulait que nous vérifiions si des améliorations pouvaient être apportées à certains éléments de cet énorme projet de loi. En tant que fonctionnaires, c'est vous qui avez travaillé à l'élaboration de ce projet de loi.

Maintenant, avec le recul, diriez-vous au Comité que la situation a changé ou qu'il y a des éléments auxquels vous n'avez pas pensé à l'époque? Vous savez comment les choses se passent présentement. Y a-t-il des modifications que nous pourrions proposer sous forme d'amendements?

● (1155)

[*Traduction*]

Le président: Monsieur Paul-Hus, il est plus probable que vous répondiez au ministre sur cette question.

M. Malcolm Brown: En bons bureaucrates...

Des voix: Oh, oh!

M. Malcolm Brown:... et je m'exprimerai ici pour tout le monde... Vous comprendrez que les conseils que nous fournissons à ce sujet sont transmis au Cabinet fédéral par l'entremise de nos ministres. Cependant, je pense que le ministre a dit clairement que, comme le ministre Sajjan, il est ouvert aux suggestions sur la manière d'améliorer le projet de loi. Nous attendons ces conseils avec impatience. Je pense que nous l'avons tous deux dit: nous discutons avec des intervenants, et ces conversations se poursuivent. Nous sommes impatients de recevoir les conseils du Comité concernant les amendements éventuels. Lorsque nous les aurons reçus, nous répondrons.

Le président: Je vous remercie, monsieur Paul-Hus.

Je donne maintenant la parole à Mme Dabrusin.

Mme Julie Dabrusin (Toronto—Danforth, Lib.): Merci.

Nous avons parlé de nombreux enjeux relatifs à l'attente raisonnable en matière de protection de la vie privée. Je pourrais commencer par cela. C'est une question qui concerne la partie 3 du projet de loi. J'ai lu des choses là-dessus ici et là. Je crois que M. Forcese et la British Columbia Civil Liberties Association ont proposé des amendements aux paragraphes 23(3) et 23(4). Cette modification ajouterait certains mots.

Le paragraphe 23(1) actuel dit ceci:

> Les activités menées par le Centre dans la réalisation des volets de son mandat touchant le renseignement étranger, la cybersécurité et l'assurance de l'information, les cyberopérations défensives ou les cyberopérations actives ne peuvent viser des Canadiens ou des personnes se trouvant au Canada.

L'amendement proposé ajouterait les mots « porter sur l'acquisition de renseignements à l'égard desquels des Canadiens ou des personnes se trouvant au Canada pourraient avoir une attente raisonnable en matière de protection de la vie privée ».

Puis le texte reviendrait au libellé actuel du paragraphe 23(3), c'est-à-dire « à moins d'être menées au titre d'une autorisation délivrée en vertu des paragraphes 27(1) ou 41(1) ».

Puisqu'il est abondamment question de l'attente raisonnable en matière de protection de la vie privée et de notre façon de gérer les contraintes découlant de cet ajout, croyez-vous que cette préoccupation est couverte ailleurs dans le projet de loi? Dans la négative, croyez-vous que ce serait une bonne chose que d'apporter cette précision? Je ne pose pas la question du point de vue de la politique. Je cherche seulement à savoir si, d'après vous, cet aspect est couvert ailleurs dans le projet de loi.

M. Malcolm Brown: Je crois que c'est une proposition du professeur Forcese, n'est-ce pas? En tant que fonctionnaires, nous sommes, me semble-t-il, un peu contraints de répondre à cela. Vous dites que votre question ne concerne pas la dimension politique, mais à vrai dire, c'est précisément ce qu'elle fait.

Je vais laisser à Scott le soin de tenter de répondre à l'aspect technique de votre question.

M. Scott Millar: Nous sommes assujettis à la Charte, et ce ne sont pas tous les éléments de la Charte qui sont abordés ici. Toutes les lois et toutes les activités sont assujetties à la Charte. En ce qui concerne l'endroit où nous interférons quant à l'attente raisonnable en matière de protection de la vie privée, disons qu'à l'heure actuelle, nous procédons selon le précepte que toute information, quelle qu'elle soit, est assujettie à une autorisation ministérielle. Pour répondre à la suggestion de mention explicite de M. Forcese, je dirais que cela n'est pas incompatible avec l'obligation implicite d'attente raisonnable en matière de protection de la vie privée, et que cette information doit être assujettie à l'autorisation ministérielle.

Mme Julie Dabrusin: D'accord. Merci.

J'ai lu quelque chose d'intéressant que le Citizen Lab a publié au sujet du CST. On y disait que la prestation de services défensifs pourrait un jour ou l'autre donner lieu à l'achat de logiciels malveillants ou d'autres choses de ce type. Comment nous protégerions-nous des gens qui mettent au point ces pièges qui nous forcent précisément à mener ces activités défensives?

● (1200)

Mme Shelly Bruce: L'achat de logiciels malveillants ne se fait pas nécessairement auprès des personnes qui les mettent au point. Il existe des organismes — des sociétés légitimes qui se spécialisent dans les logiciels antivirus — qui nous permettent d'acheter l'information qu'elles colligent grâce à leurs propres analyses, à leurs propres travaux. Nous travaillons en étroite collaboration avec cette communauté afin de bien cerner les menaces qui sont couvertes par les logiciels commerciaux et les services connexes, de manière à ce que nous puissions nous focaliser sur les menaces qui ne sont pas couvertes, sur ces menaces plus sophistiquées qui ne sont pas prises en charge par le dispositif de défense actuel.

Mme Julie Dabrusin: Nous avons parlé un peu de l'information accessible au public. Je crois que l'une des choses qui rendent cela un peu compliqué, c'est l'existence de différentes strates à propos de ce que les gens considèrent comme étant public. L'une des préoccupations qui ont été soulevées, c'est la possibilité qu'un incident de piratage fasse en sorte que l'information soit soudainement rendue publique. L'information qui était censée être privée se retrouve tout à coup accessible à tous. Comment cela relève-t-il de l'information publique? Quelles sont les mesures de sécurité à cet égard?

Mme Shelly Bruce: Dans le cas du CST, cette information — tout ce qui a été piraté ou volé, puis mis en vente — n'est pas incluse dans la définition de ce que l'on appelle de l'information accessible au public.

Le président: Merci, madame Dabrusin.

Monsieur Dubé, vous avez les cinq dernières minutes de cette série.

M. Matthew Dubé: Merci beaucoup.

À propos des cyberopérations actives, c'est le ministre de la Défense qui mène le bal, si vous me permettez cette expression, et vous existez par l'intermédiaire du ministère de la Défense. Or, le CST — et je connais la réponse à cela, mais je veux que la chose soit consignée dans le compte rendu — est un organisme civil, n'est-ce pas?

Mme Shelly Bruce: C'est exact.

M. Matthew Dubé: Lorsque des cyberopérations sont menées... Dans votre exposé, si je me fie aux notes, vous parlez de « cyberattaques perpétrées par des États étrangers ». Vous ne décrivez pas une cyberattaque comme étant un acte de guerre proprement dit. Vous parlez également de freiner les « cyberattaques perpétrées par des États étrangers ». Comme le CST est un organisme civil qui relève du ministre de la Défense, y a-t-il un risque que les actions essentiellement offensives qu'il mènera contre d'autres États soient perçues comme un acte de guerre? Quelles conséquences juridiques cela pourrait-il avoir? Nous avons reçu des témoins qui nous ont exposé cette situation. Sur le plan juridique, le CST est perçu comme étant une organisation civile, ce qui complique considérablement la donne. Les préoccupations émanent en grande partie de cet état de fait. Je n'ai pas vraiment l'impression d'avoir entendu parler de cela dans votre exposé.

Mme Shelly Bruce: Il ne fait aucun doute que le Canada et ses alliés doivent faire face à une menace grandissante de la part d'intervenants d'États hostiles ou d'intervenants non alignés de par le monde. Nous travaillons en étroite collaboration avec le ministère de la Défense et, comme vous l'avez mentionné, nous relevons effectivement de lui. Lors du récent examen de la politique en matière de défense, l'armée a indiqué qu'elle souhaitait travailler dans le domaine cybernétique, et qu'elle voulait à cette fin se donner un cadre et une plateforme. Vous remarquerez également que le projet de loi a été conçu de manière à permettre au CST d'épauler les Forces armées canadiennes. Cela fait partie de notre mandat d'assistance. Selon les conditions et les circonstances des activités qu'il faudra déployer, nous serons en mesure de travailler de plus près avec eux. Une collaboration plus étroite est envisageable en ce qui a trait à la prestation de capacités sur le plan militaire.

M. Matthew Dubé: Par souci de clarté, si vous étiez ministre de la Défense, comment répondriez-vous si nous avions besoin d'une contre-attaque pour faire face à un geste hostile posé par un acteur d'un État étranger et que l'armée était en train de développer des capacités semblables à celles du CST? Vous adresseriez-vous à l'armée ou au CST? Si l'armée se met à développer ses propres capacités, pourquoi demanderait-elle à un organisme civil de réagir à sa place, c'est-à-dire d'intervenir contre un acteur d'un État étranger?

Mme Shelly Bruce: Cela dépend des circonstances qui entourent l'activité en cause. Dans de nombreux cas, on ne serait pas en mesure d'attribuer cette activité à une personne en particulier. Sauf que ce qui est le plus important, c'est d'empêcher que cette activité se produise avant qu'elle ne provoque une crise ou avant qu'elle ne se matérialise dans le périmètre de sécurité du Canada.

M. Matthew Dubé: Il s'agirait donc d'opérations défensives et non d'opérations actives.

M. Scott Millar: J'ajouterais que le CST a déjà cette capacité. L'une des raisons pour lesquelles la Défense nationale et les Forces armées canadiennes ont été ajoutées à notre mandat d'assistance, c'est qu'elles auront la possibilité de mettre nos capacités à contribution dans l'éventualité où elles devraient mener des cyberopérations en appui à des opérations militaires approuvées par le gouvernement. Lorsqu'il s'agit d'un contexte militaire, utilisez-nous; lorsqu'il ne s'agit pas d'un contexte militaire...

Il faut garder à l'esprit que certaines des choses dont nous discutons ici seraient... Par exemple, si une entreprise canadienne se faisait voler des renseignements en matière de propriété intellectuelle, nous pourrions peut-être arriver à remonter à la source de l'attaque et à rendre cette information illisible. Il ne s'agit pas toujours d'agression, de cyberguerre ou d'autres choses de ce genre. Il y a des utilisations civiles, et il y a des interdictions pour nous garder dans le bon couloir, comme des interdictions de blessures corporelles et d'autres semblables. L'obligation d'obtenir l'approbation du ministre de la Défense et du ministre des Affaires étrangères est là pour assurer que les activités que nous mettrons en oeuvre seront conformes aux priorités internationales et au droit international.

● (1205)

Le président: Merci.

Voici qui termine cette première série de questions, sauf que, fidèles à la réputation que nous avons d'être le comité le plus travaillant de la Colline, nous ne prendrons pas de pause pour dîner et nous allons tout de suite passer à la deuxième série de questions.

J'aimerais cependant avoir votre avis. Sans changer de formule, pourrions-nous passer à des questions de cinq minutes, en passant d'un côté à l'autre, comme tout à l'heure? Cela nous permettra peut-être d'ajouter deux questions.

Monsieur Dubé.

M. Matthew Dubé: En utilisant la même rotation, je me retrouverais cinquième ou sixième sur la liste, avec une intervention de seulement cinq minutes. Est-ce que c'est ce que cela signifie?

Le président: Eh bien, si vous regardez l'heure qu'il est, vos chances sont nulles si je garde la même structure. Je ferais deux séries de cinq minutes plutôt qu'une série de sept minutes.

M. Matthew Dubé: J'échangerais mes sept et cinq minutes pour deux interventions de cinq minutes chacune, c'est bien cela?

Le président: Oui. Je sais que la générosité dont vous faites preuve à l'égard de votre temps de parole est très appréciée.

Monsieur Fragiskatos, pour cinq minutes.

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

Merci de tout le travail que vous faites ainsi que de votre présence ici aujourd'hui.

Ma première question s'adresse à Mme Bruce. Pouvez-vous énumérer de nouveau les types d'actions qui compteraient pour une cybercapacité offensive, et nous donner des exemples?

Mme Shelly Bruce: Bien sûr.

Je dirais tout d'abord que les cyberopérations actives visent à atteindre un objectif que le gouvernement a établi, et qu'il s'agit d'un sport d'équipe. Cela signifie que nous venons tous à cette table avec nos mandats, nos pouvoirs et nos capacités. En fait, c'est une façon de travailler ensemble afin de déterminer qui a l'autorité voulue pour s'attaquer au bon problème au bon moment, en fonction de ses compétences, de son mandat et de ses pouvoirs.

En ce qui concerne le CST, j'ai parlé de certaines de ces opérations dans ma déclaration liminaire, comme le fait d'interrompre ou de perturber les communications et les réseaux de Daech, de saboter ses appareils médiatiques de manière à freiner la planification d'attaques avant que les choses n'atteignent le stade de crise. Il y a aussi les actions qui visent à stopper la progression des logiciels rançonneurs dans le monde entier et celles qui visent à mettre un terme à la subversion à l'endroit du processus démocratique. Comme l'a dit mon collègue, certains systèmes canadiens se sont déjà fait voler des renseignements délicats, et ces renseignements sont maintenant utilisés par des systèmes situés à l'étranger. Dans cette optique, nous pourrions trouver des façons d'altérer ces données ou de les rendre inutilisables pour ceux que voudraient les exploiter à leur propre compte.

M. Peter Fragiskatos: Trouver des façons de protéger les systèmes bancaires, trouver des façons de se prémunir d'attaques potentielles sur nos systèmes d'approvisionnement en électricité, par exemple, est-ce que cela fait partie de ce que vous faites?

Mme Shelly Bruce: Oui, les infrastructures névralgiques font partie de cela. Aux termes du projet de loi proposé, le CST se verrait donner le pouvoir d'utiliser les compétences, la technologie et les capacités qui ont été développées pour protéger les réseaux du gouvernement du Canada et de mettre ce savoir-faire, cette orientation et ces services à la disposition des propriétaires d'infrastructures névralgiques. Il faudra pour cela que le propriétaire de l'élément d'infrastructure névralgique ait demandé l'aide du CST, et que le ministre ait désigné cet élément comme étant admissible à cette aide.

M. Peter Fragiskatos: J'ai posé la question parce que je pense qu'il est très important de démystifier certaines des idées qui circulent sur ce qui constitue réellement une cybercapacité offensive. À l'évidence, il s'agit d'une nouvelle façon d'assurer la sécurité nationale, et je crois que certains mythes circulent à cet égard.

Par exemple, le Comité a entendu des témoignages d'organismes comme OpenMedia et la BC Civil Liberties Association... Lors de son témoignage, OpenMedia a laissé entendre de façon assez directe que le Comité et les Canadiens en général devaient être aux aguets, parce que le CST pourrait utiliser cette cybercapacité offensive pour saper le processus démocratique d'autres États. Là n'est pas l'intention, n'est-ce pas?

Mme Shelly Bruce: Non. Les cyberopérations actives dirigées vers des entités étrangères situées à l'extérieur du Canada nécessitent l'approbation du ministre de la Défense nationale ainsi que celle du ministre des Affaires étrangères. Au nombre des facteurs qu'ils doivent prendre en considération, il y a la nécessité et le caractère raisonnable de l'activité ainsi que sa proportionnalité compte tenu de la nature de l'objectif à atteindre. L'objectif ne saurait être atteint d'aucune autre façon; l'activité ne peut causer ni lésion corporelle ni décès. En outre, l'activité ne peut servir à renverser ou à bloquer une démocratie, ni à entraver le cours de la justice. Il y a une interdiction explicite à cet égard.

● (1210)

M. Peter Fragiskatos: D'accord. Merci beaucoup de me rassurer à ce sujet.

Avec les nouvelles cybercapacités proposées dans le projet de loi C-59, où nous situerons-nous par rapport aux capacités de nos alliés du Groupe des cinq dans ce domaine particulier?

Mme Shelly Bruce: Je ne suis pas une spécialiste en ce qui concerne les pouvoirs de tous nos alliés dans ce domaine, mais, de manière générale, ces dispositions nous permettront d'exercer les mêmes activités et les mêmes pouvoirs qu'eux, et de prendre part à des coalitions présidant au déploiement d'activités qui dépasseront le cadre national.

M. Peter Fragiskatos: Merci beaucoup.

Si vous me le permettez, ma dernière question s'adresse à qui voudra bien y répondre. J'ai lu le Rapport public de 2017 sur la menace terroriste pour le Canada qu'a préparé Sécurité publique Canada. À quelques reprises, le rapport fait allusion à l'extrémisme de droite et explique ce que cela signifie pour le Canada au chapitre de la menace terroriste. Le rapport signale qu'un module dédié à la question des groupes d'extrême droite est en cours d'élaboration sous la direction de l'équipe du programme de sensibilisation des premiers intervenants au terrorisme. Selon le rapport, bien que les activités de l'extrême droite et l'extrémisme de droite aient toujours été une préoccupation, c'est la première fois — du moins, c'est que le rapport laisse entendre — qu'une démarche dédiée prend forme. Cela signifie-t-il que le ministère de la Sécurité publique est particulièrement inquiet — plus que jamais en fait — de la menace qu'exerce l'extrémisme de droite au Canada?

Le président: Malheureusement, le temps de parole de M. Fragiskatos est écoulé, ce qui est un peu de ma faute, mais je vais quand même vous demander de répondre, à condition de faire très vite, car nous voulons être en mesure de poser le plus de questions possible.

M. Malcolm Brown: Très rapidement, je ne sais pas si je peux dire « plus que jamais », mais adressez-vous à Gilles Michaud; il pourra vous répondre avec plus de précision que moi.

S.-comm. Gilles Michaud: En fait, ce module est un coup de collier en matière d'application des lois. Nous avons constaté une recrudescence des activités, et je crois que la situation actuelle est due en partie au fait que nous nous sommes détournés de cela pendant un certain nombre d'années. Il y a vraiment un effort particulier pour examiner ces choses de plus près. Notre service de police est celui qui a la compétence voulue pour faire cela — après tout, c'est surtout dans la sphère fédérale que ces activités se produisent et c'est à cet ordre de gouvernement que la responsabilité incombe —, c'est-à-dire essayer de mieux comprendre la nature et l'ampleur de cette menace.

Le président: Merci, monsieur Fragiskatos.

Monsieur Motz, vous avez la parole pour cinq minutes.

M. Glen Motz: Merci, monsieur le président.

Merci encore à nos témoins pour leur présence.

Le 30 novembre dernier, alors que nombre d'entre vous étaient ici, j'ai demandé un examen complet des coûts de la mise en oeuvre de ce projet de loi. À ma connaissance, aucun examen de la sorte n'a été soumis au Comité. Si vous l'avez fait, tant mieux. Si vous ne l'avez pas fait, je vous saurais gré de le faire. Idéalement, ce serait formidable que l'examen fasse état des exigences en matière de conformité et des coûts supplémentaires associés à ce projet de loi. Merci.

Je voudrais aborder la question de...

Le président: Monsieur Motz, un instant je vous prie. Demandez-vous que cela soit un engagement à l'égard du Comité?

M. Glen Motz: Oui, c'est ce que je demande.

Le président: Monsieur Brown, est-ce oui ou non?

M. Malcolm Brown: C'est oui.

Le président: D'accord.

M. Malcolm Brown: Peut-on vraiment refuser?

Des voix: Oh, oh!

M. Malcolm Brown: Nous allons nous efforcer de fournir...

Le président: Vous pourriez évoquer quelque vague secret ministériel ou quelque chose du genre.

M. Malcolm Brown: Il y a certaines contraintes, mais je crois que nous pouvons fournir un peu plus de renseignements à ce sujet. Hier, lorsque je me suis préparé à la présente séance, je me suis aperçu que vous avez effectivement fait cette demande et que nous n'y avons pas répondu. Alors, nous allons nous amender, et certains autres... Vous n'aurez pas nécessairement toute l'information d'un seul coup, mais nous allons vous donner des réponses.

M. Glen Motz: À la lumière des récentes attaques terroristes qui ont eu lieu au Royaume-Uni, en Europe et, évidemment, ici, au Canada, et qui impliquaient l'acquisition et l'utilisation d'objets accessibles à tous — produits chimiques, véhicules, etc. —, le gouvernement a-t-il passé en revue les modifications prévues au projet de loi C-59 pour s'assurer que ledit projet de loi permette le déploiement d'activités perturbatrices d'urgence — surtout par le SCRS —, y compris la possibilité de procéder sans mandat, au besoin? Êtes-vous satisfaits des pouvoirs de perturbation que vous confère le projet de loi?

Mme Tricia Geddes: Oui, je crois que nous le sommes. Nous sommes heureux de voir que le gouvernement a réaffirmé son engagement à l'égard des pouvoirs qui nous sont conférés. Je crois que c'est une nouvelle trousse d'outils que le gouvernement se donne pour être en mesure de réagir adéquatement, surtout si l'on tient compte de l'évolution très rapide des menaces et du fait qu'elles peuvent parfois se manifester à un rythme effréné. De toute évidence, nous travaillons en étroite collaboration avec la GRC, mais le projet de loi est assurément un outil efficace.

● (1215)

M. Glen Motz: Je vais poser une question complémentaire à ce sujet, et je vais demander aux deux témoins de la GRC d'y répondre aussi.

Y a-t-il quoi que ce soit que nous pourrions améliorer dans ce domaine, dans ce projet de loi, quelque chose que nous pourrions ajouter et qui n'est pas déjà là? Y a-t-il des aspects auxquels vous avez pensé après coup, des dispositions que vous souhaiteriez maintenant voir ajouter au projet de loi?

Le président: Je ne crois pas qu'ils peuvent vraiment répondre à cette question.

M. Glen Motz: Je comprends ce que vous me dites, mais, par souci de faire les choses comme il faut, on serait porté à croire qu'il devrait y avoir une telle marge de manoeuvre.

M. Malcolm Brown: Si vous me le permettez, je dirais que nous sommes heureux de recevoir des conseils de la part du Comité quant à la façon d'améliorer ce projet de loi et, par la suite, de laisser le gouvernement procéder à l'examen de ces suggestions.

M. Glen Motz: J'aimerais à nouveau utiliser le terme bureaucratique, mais je vais m'en abstenir.

M. Malcolm Brown: Parfois, quand ça en a l'air et la chanson...

M. Glen Motz: Tout juste.

Merci.

Donc, la GRC est aussi d'avis que le projet de loi contient les dispositions nécessaires et qu'il permet, au besoin, de déployer sans mandat les activités perturbatrices d'urgence qui s'imposent?

S.-comm. Gilles Michaud: Beaucoup de ces pouvoirs existent à l'extérieur du projet de loi, et nous avons déjà ce qu'il nous faut pour intervenir et perturber n'importe quel type de menace en puissance.

M. Glen Motz: Par conséquent, avec ce projet de loi, les agents du SCRS auraient le pouvoir, dans des situations d'urgence définies, de recourir à des activités perturbatrices afin de prévenir une attaque, et ce, sans mandat?

Mme Tricia Geddes: Permettez-moi un instant de consulter mes collègues.

Merydee, allez-y.

Mme Merydee Duthie (conseillère spéciale, Service canadien du renseignement de sécurité): Les mesures de réduction de la menace peuvent être appliquées avec ou sans mandat. Le projet de loi ne dit rien au sujet des situations d'urgence. Des mesures peuvent être appliquées sans mandat, mais à vrai dire, la contrainte de temps est une question interne, compte tenu de tous les processus qui doivent être suivis et des consultations qui doivent être menées auprès de nos partenaires afin de nous assurer du bien-fondé des mesures envisagées.

M. Glen Motz: Merci.

Je vous en prie.

Mme Tricia Geddes: Je veux seulement préciser que dans ces situations d'urgence, c'est plutôt la GRC qui serait appelée à intervenir.

M. Glen Motz: Merci.

Je suis certain qu'il me reste encore un peu de temps.

J'ai une question à laquelle il faut répondre par « oui » ou par « non ». Nous avons reçu un témoin qui a formulé quelque réserve et qui a laissé entendre que l'adoption du projet de loi C-59 dans sa forme actuelle allait permettre au CST d'intervenir dans le processus électoral démocratique d'un autre pays.

Madame Bruce, pouvez-vous nous confirmer que le CST n'a pas l'intention d'utiliser ses nouveaux pouvoirs pour s'immiscer dans le processus électoral démocratique d'autres pays?

Mme Shelly Bruce: Oui, monsieur. En fait, le projet de loi comporte une disposition explicite pour interdire l'utilisation de cyberopérations actives dans le but de corrompre ou d'entraver le cours de la justice ou de la démocratie.

M. Glen Motz: Merci.

Le président: Je peux penser à au moins un chef d'État qui serait soulagé de cela.

Monsieur Dubé, c'est à vous.

M. Matthew Dubé: J'imagine que ce n'est pas une position de parti.

Ma question s'adresse d'abord au CST, puisque vous avez parlé de cela dans votre exposé, mais aussi au SCRS, parce qu'il est mentionné dans la partie 4 du projet de loi tout autant que dans la partie 3. Il s'agit de la définition de l'« information accessible au public ».

Aux dires de personnes qui connaissent cela mieux que moi et qui ont témoigné ici, il semble que ni le droit canadien ni la jurisprudence n'ont à ce jour défini ce qu'est l'information accessible au public.

Selon vous, il s'agit de ressources publiques auxquelles toute personne au Canada peut accéder. Selon l'Association du Barreau canadien, un exemple de cela serait les renseignements que Facebook vend aux annonceurs — renseignements qui seraient sans doute accessibles à tous ceux qui sont dans ce domaine. Je ne sais pas exactement si nous parlons de quelqu'un qui chercherait dans Google à en savoir plus sur une personne dont la page Facebook aurait peu de restrictions en matière de confidentialité, ou si nous parlons de choses qui, techniquement, sont accessibles à n'importe qui, mais sans vraiment l'être.

Ma première question est donc: pouvez-vous étayer cette définition? Ma deuxième question est la suivante: pourquoi ne trouve-t-on aucune définition de cela dans le projet de loi ou dans le droit canadien, et n'y aurait-il pas lieu, par souci de clarté, d'inclure une définition de cette réalité dans le projet de loi?

M. Scott Millar: Il y a différents aspects à cela. Il faut entre autres clarifier le fait que cet élément rend explicite quelque chose qui se passe déjà avec le CST. Nous utilisons de l'information sur l'infrastructure, qui, comme le dit le projet de loi, peut être liée à une personne identifiable.

Nous faisons cela pour comprendre l'infrastructure mondiale de l'information dans laquelle nous intervenons. Comme Shelly l'a indiqué dans sa déclaration liminaire, nous utilisons cette information d'autres façons, conformément à notre mandat. Nous ne sommes pas un organisme d'enquête national. Nous ne constituons pas des dossiers sur les citoyens et nous ne sommes pas en mesure de croiser des données dans le but d'en apprendre davantage sur les activités de tel ou tel particulier.

De plus, comme cela a été dit, nous ne pourrions pas nous servir de renseignements volés ou piratés. J'attire votre attention sur l'énoncé concernant la Charte que le ministère de la Justice a publié lors de la présentation du projet de loi, énoncé où il était question de l'information accessible au public et des raisons qui font que cette information est différente de celle qui ferait l'objet d'une attente raisonnable de protection en matière de vie privée et qui serait assujettie au processus d'autorisation ministériel.

● (1220)

M. Matthew Dubé: J'ai une question complémentaire, mais allez-y.

Mme Tricia Geddes: En ce qui concerne votre question sur les médias sociaux, sachez que la collecte et l'utilisation que nous faisons de l'information continueront d'être guidées par la Charte et par l'attente raisonnable de protection en matière de vie privée des personnes, ce qui, comme vous le savez, se transforme au fil du temps. Nous allons nous assurer de rester fidèles à ces préceptes.

De plus, sachez que nous ne considérons pas les ensembles de données piratés ou volés comme étant de l'information accessible au public. Il serait cependant possible d'envisager un scénario où nous chercherions à obtenir le pouvoir de retenir un ensemble de données piraté ou volé auquel nos adversaires pourraient avoir accès, mais cela ne pourrait se faire que par le processus d'autorisation normal. Dans le cas de renseignements concernant des Canadiens, il nous faudrait passer par la Cour fédérale. Dans le cas de données de l'étranger, la demande serait acheminée au commissaire à l'information.

M. Scott Millar: Puis-je ajouter quelque chose?

Je m'excuse, monsieur, mais la réponse que je vous ai donnée n'était pas complète.

M. Matthew Dubé: Allez-y rondement parce que j'ai certains...

M. Scott Millar: La notion d'« information accessible au public » est définie à la partie 3 du projet de loi. Il en existe donc une définition particulière.

M. Matthew Dubé: Je m'excuse, je n'ai pas cela devant moi. Quelle est cette définition?

M. Scott Millar: Comme vous n'avez pas le projet de loi sous les yeux, je vais vous la lire:

> L'information accessible au public est l'information publiée ou diffusée à l'intention du grand public, accessible au public dans l'infrastructure mondiale de l'information ou ailleurs ou disponible au public sur demande, par abonnement ou achat.

M. Matthew Dubé: Très bien. Merci.

Lorsqu'il est question d'information acquise incidemment, y a-t-il une raison pour laquelle cette information serait retenue? Pour l'instant, le paragraphe 24(4) proposé fait état d'information acquise incidemment au cours d'activités de recherche. Y a-t-il quelque raison pour laquelle vous retiendriez cette information plutôt que de la laisser aller, plutôt que de remettre le poisson à l'eau, le cas échéant?

Je ne comprends pas tout à fait les autorisations dont il est question à l'article 24 proposé. Je comprends très bien les autorisations qui portent sur l'information acquise incidemment en ce qui concerne les ensembles de données du SCRS, mais je comprends moins bien celles qui sont décrites à la partie 3.

M. Scott Millar: Je me contenterai de dire que, lorsqu'il convient de tenir compte de l'attente raisonnable de protection en matière de vie privée, toute information que nous utilisons... Tout élément d'information échappant à la définition d'information accessible au public, tout ce qui pourrait cautionner une « attente raisonnable » doit faire l'objet d'une autorisation ministérielle.

Nous aurons quand même cet élément de protection de la vie privée qui s'applique à l'information accessible au public dans les cas où le besoin de protection est suscité, mais encore une fois, étant donné que la Loi sur la protection des renseignements personnels exige que nous limitions la collecte, l'utilisation et la rétention d'information à ce qui est conforme à notre mandat, nous ne pouvons pas outrepasser ces limites et utiliser cette information d'autres façons.

Bien entendu, tout ce que nous ferons dans ce contexte sera évalué en fonction du caractère raisonnable, de la nécessité et de l'élément de protection de la vie privée. Par conséquent, toute préoccupation sur ce que nous allons faire dorénavant sera cernée par l'organisme chargé de mener cet examen, et portée à l'attention de notre ministre.

Le président: Merci.

Monsieur Spengemann, c'est à vous.

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

Madame Bruce, lors de la première série de questions, nous avons manqué de temps au moment où vous alliez demander à votre collègue, M. Millar, de répondre à la question au sujet des règles présidant au déploiement de cyberopérations actives à l'étranger. Vous avez ensuite eu une discussion de suivi avec mon collègue, M. Fragiskatos.

Monsieur Millar, avez-vous quelque chose à ajouter quant au cadre utiliser pour mener des cyberopérations actives à l'étranger et aux garde-fous connexes?

M. Scott Millar: Non, je crois que tout a été dit. La seule précision que je ferais, c'est que notre loi utilise les adjectifs « actif » et « défensif ». Le terme « offensif » relève davantage de la sphère militaire. C'est le terme qu'utiliseraient les Forces armées canadiennes, ou qui serait utilisé pour elles.

M. Sven Spengemann: Merci.

Monsieur Brown, en ce qui concerne la violence familiale, le terrorisme, l'extrémisme, la radicalisation — on pourrait par exemple se servir du cas isolé qui s'est produit à Sainte-Foy il y a un peu plus d'un an —, à votre avis, dans quelle mesure le travail proactif effectué auprès des jeunes Canadiens est-il important? Je crois comprendre que la vaste majorité de ces cas sont le fait de jeunes de moins de 35 ans. Selon ma connaissance partielle du monde, les soixantenaires et les septuagénaires ne s'autoradicalisent pas. Que pouvons-nous faire à l'intérieur du cadre dont nous disposons? Dans quelle mesure le travail pour contrer la violence et la radicalisation est-il important, et quels en sont les principaux éléments?

● (1225)

M. Malcolm Brown: Il ne fait aucun doute que ce travail est très important. Le gros de ce travail est mené par le Centre canadien d'engagement communautaire et de prévention de la violence, qui évolue en marge du ministère. Le Centre travaille avec des groupes communautaires locaux. Il finance et soutient des initiatives d'un peu partout au pays — à Montréal, à Calgary, à Toronto et ailleurs —, en partant du principe que les solutions doivent être adaptées aux conditions locales. C'est vraiment l'un des éléments centraux de notre réponse à l'égard de ce groupe d'âge particulièrement vulnérable.

M. Sven Spengemann: Le Canada est-il à l'avant-garde quant au traitement de ce problème ou y a-t-il des expériences dont nous pourrions nous inspirer pour mettre au point notre propre cadre d'intervention? Je pense par exemple à ce qui se fait dans d'autres pays, notamment ceux de la collectivité des cinq.

M. Malcolm Brown: Je dirais en fait que nous sommes les meneurs. Nous travaillons de près avec nos partenaires de la collectivité des cinq — surtout avec eux, mais pas seulement avec eux — afin de comprendre les tendances, mais comme pour l'exemple de tout à l'heure à propos des villes, les interventions qui s'appliquent ailleurs ne conviennent pas nécessairement pour le Canada. Je dirais que nous sommes en très bonne posture par rapport à nos collègues. J'ajouterais même que, selon les échanges que nous avons eus lors de la réunion du G7 de l'automne dernier, il est très clair que le Canada est un leader dans ce domaine.

M. Sven Spengemann: Merci beaucoup.

Ma dernière question s'adresse à M. Breithaupt. En présumant que les menaces terroristes, la radicalisation et les menaces extrémistes constatées au Canada sont principalement associées aux adolescents, avez-vous des observations à formuler au sujet des dispositions mises de l'avant dans le projet de loi quant à la Loi sur le système de justice pénale pour les adolescents, c'est-à-dire les articles 159 à 167?

Avez-vous des choses à proposer pour améliorer ces dispositions, ou êtes-vous d'avis qu'elles seront en mesure de protéger adéquatement nos adolescents?

M. Douglas Breithaupt (directeur et avocat général, Section de la politique en matière de droit pénal, ministère de la Justice): Je vous remercie de cette question.

Je traiterai brièvement des amendements proposés. La Loi sur le système de justice pénale pour les adolescents admet que les jeunes bénéficient de garanties particulières au chapitre des droits et libertés, et contient un certain nombre de mesures de protection juridiques importantes pour faire en sorte qu'ils soient traités équitablement et que leurs droits soient protégés. La Partie 8 du projet de loi vise à garantir que tous les jeunes qui ont des démêlés avec le système de justice pénale en raison d'un comportement lié au terrorisme aient droit à des mesures de protection renforcées sur le plan de la procédure et à d'autres égards en vertu de la Loi sur le système de justice pénale pour les adolescents. Par exemple, le projet de loi stipule que les mesures de protection des jeunes s'appliquent aux engagements et précise que les tribunaux pour adolescents ont le pouvoir exclusif d'imposer des engagements aux jeunes.

Par exemple, si un jeune non représenté par un avocat comparaissait devant un tribunal pour adolescents concernant une demande d'engagement de ne pas troubler l'ordre public lié au terrorisme, les amendements exigeraient que ce tribunal l'informe de son droit de mandater un avocat, le dirige vers un programme d'aide juridique disponible et, si le jeune ne peut obtenir les services d'un avocat par l'entremise de ce programme, fasse en sorte qu'il soit représenté par un avocat de l'État s'il en fait la demande.

À l'échelle internationale, on discute aussi des effets du terrorisme sur le système de justice pour mineurs, et les amendements qu'on propose d'apporter à la Loi sur le système de justice pour adolescents visent à renforcer la protection des jeunes au cours des procédures quand il faut tenir compte des conditions d'un engagement de ne pas troubler l'ordre public lié au terrorisme. Ils prévoient toutefois aussi l'accès aux dossiers des adolescents en application du Décret sur les passeports canadiens, le tout devant faire l'objet de mesures de protection de la vie privée de la loi.

Le président: Merci beaucoup.

[*Français*]

Monsieur Paul-Hus, vous disposez de cinq minutes.

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

Je vais parler des combattants islamiques. On sait que 180 Canadiens ont décidé d'aller faire le djihad un peu partout dans le monde, surtout en Iraq et en Syrie, mais ailleurs aussi, notamment en Afrique. De ce nombre, une soixantaine sont connus et sont revenus au Canada. Dix d'entre eux sont suivis de plus près par nos services de police et le SCRS, mais il y a un problème d'ordre légal. Le projet de loi C-59 aidera-t-il le Canada à prendre des mesures pour pouvoir poursuivre ces gens, quitte à déporter ceux qui ont une double nationalité?

● (1230)

[*Traduction*]

M. Malcolm Brown: Le projet de loi C-59 ne contient pas de dispositions précises concernant la question des voyageurs extrémistes violents. Certains de ses éléments accordent aux organismes des outils et des mesures qui amélioreront leur capacité de protéger le Canada des menaces pouvant se manifester. Sachez également qu'un éventail d'outils s'offre au gouvernement, à nous tous ici présents et à d'autres intervenants pour gérer et évaluer la situation, prendre les mesures nécessaires pour protéger la population canadienne et veiller, lorsqu'il existe des preuves, à ce que l'on puisse entamer des poursuites contre les personnes concernées.

[*Français*]

M. Pierre Paul-Hus: Il y a un exemple que je voudrais examiner avec vous.

Jack Letts, alias Jihadi Jack, a la citoyenneté canadienne ainsi que la citoyenneté britannique. La Grande-Bretagne ne veut évidemment pas le recevoir. On a appris vendredi que M. Letts et sa mère tentent d'exercer des pressions sur notre gouvernement pour qu'il soit accueilli ici, au Canada. Il y a un problème en ce qui concerne la preuve. Si M. Letts entre au Canada, il sera libre dans le temps de le dire, parce que nous avons un problème: nous n'avons pas les preuves nécessaires pour le retenir.

Êtes-vous en relation avec les gouvernements du Groupe des cinq, ou d'autres pays — j'imagine que oui —, auprès desquels il serait possible d'obtenir les preuves qui pourraient l'incriminer ici, ou n'avons-nous pas les moyens d'agir?

[*Traduction*]

M. Malcolm Brown: Nous sommes tous soumis à des contraintes lorsque nous discutons d'une affaire précise; je pense donc que nous devons répondre à votre question d'une manière générale.

Sur ce, je céderai la parole à M. Michaud.

[*Français*]

S.-comm. Gilles Michaud: C'est un exemple parmi tant d'autres. Lorsque vient le temps d'enquêter sur des Canadiens qui sont partis à l'étranger, le travail commence à l'étranger. Nous avons des relations avec différents corps de police, soit ceux du Groupe des cinq ou d'autres pays. Nous commençons alors à colliger l'information relativement à la preuve. Une fois que l'individu arrive au pays, nous pouvons mettre d'autres mesures en place pour poursuivre notre travail et pour essayer d'établir si cet individu pose effectivement une menace et si nous avons les preuves nécessaires pour porter des accusations.

Il y a donc un aspect criminel. Il y a aussi celui de la prévention. Certains des individus qui reviennent au pays n'ont pas nécessairement un passé criminel. Ils ont eu d'autres rôles à jouer pour la cause. Dans ce cas, nous faisons affaire avec d'autres organismes pour intervenir et tenter de leur permettre d'avancer dans le dossier de leur retour au Canada.

M. Pierre Paul-Hus: Je vous remercie.

Je veux parler du rôle du CST. Actuellement, à moins que je ne me trompe, le lien entre le CST et le ministère de la Défense nationale en est un de financement et d'opérations. En vertu du projet de loi C-59, il va y avoir un transfert, soit une dissociation entre le CST et le ministère de la Défense nationale, ce qui va faire que Sécurité publique Canada aura davantage de responsabilités.

Est-ce bien le cas?

[*Traduction*]

M. Scott Millar: Oui. Notre organisme est indépendant et relève du portefeuille du ministre de la Défense nationale. Comme je l'ai fait remarquer, le projet de loi l'indique lui-même.

[*Français*]

M. Pierre Paul-Hus: Au bout du compte, je veux savoir si, selon vous, les dispositions du projet de loi C-59 vont changer les choses, ou si votre fonction va demeurer la même sans présenter de changements significatifs.

[*Traduction*]

Le président: Pourriez-vous répondre brièvement, je vous prie?

M. Scott Millar: Vous voulez savoir si notre statut d'organisme indépendant va changer?

M. Pierre Paul-Hus: Je parle du point de vue opérationnel.

M. Scott Millar: Non. À l'évidence, le mandat comprendrait de nouvelles responsabilités, mais notre fonctionnement au sein du portefeuille resterait le même. En fait, ces dispositions d'ordre administratif figurent dans le projet de loi. Autrefois, notre organisme était indépendant aux termes d'un décret pris en 2011. Nous serons maintenant plus une entité issue de la loi régie par une mesure législative distincte. Ici encore, le projet de loi rendra transparentes un certain nombre des dispositions auxquelles nous sommes assujettis.

[*Français*]

Le président: Merci, monsieur Paul-Hus.

Monsieur Picard, vous disposez de cinq minutes.

● (1235)

M. Michel Picard: Ma question s'adresse au SCRS et à la GRC. On constate, dans l'ensemble du projet de loi, l'absence du CANAFE. Ce n'est pas un oubli. Le financement du terrorisme est une réalité, on ne le nie pas. Cela dit, la tendance actuelle veut que les attentats terroristes soient de moins en moins coûteux. Par exemple, on vole un camion pour foncer sur une foule. La dimension financière a changé.

Dans les circonstances actuelles, modernes, y aurait-il lieu de revoir le lien avec le CANAFE? Nos moyens légaux de travailler avec l'organisation sont-ils suffisants, de sorte qu'il n'est pas nécessaire de prévoir un lien quelconque avec le CANAFE dans le projet de loiC-59?

S.-comm. Gilles Michaud: Je crois que ce qui existe actuellement dans le cadre de notre relation avec le CANAFE et dans la législation en place, nous permettent de faire notre travail. D'ailleurs, cela nous offre une certaine flexibilité. La menace peut augmenter et se faire d'une certaine façon pendant un certain temps, et la méthode peut changer par la suite. Nous pouvons toujours échanger de l'information avec le CANAFE. La loi nous permet ces échanges dans n'importe quelle circonstance.

M. Malcolm Brown: Je voudrais ajouter qu'il y a maintenant un examen après cinq ans de la loi sur le terrorisme...

[*Traduction*]

John, quel est le titre intégral de la loi?

M. John Davies (directeur général, Politiques de la sécurité nationale, ministère de la Sécurité publique et de la Protection civile): La Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes fait actuellement l'objet d'un examen quinquennal. Le ministère des Finances a publié un document de discussion, réclamant des propositions sur la manière de l'améliorer.

Mme Tricia Geddes: Je suis d'accord avec mon collègue.

Nous collaborons très étroitement avec le CANAFE. Je ne pense pas que des changements s'imposent ici. Nous investissons dans les enquêtes sur le terrorisme, en ce qui concerne notamment le financement des activités terroristes.

M. Michel Picard: Merci.

[*Français*]

Monsieur Brown, le projet de loi C-59 remanie les pouvoirs de surveiller les différentes agences qui y sont mentionnées.

Quelle incidence cela aura-t-il sur la Commission civile d'examen et de traitement des plaintes relatives à la GRC?

M. Malcolm Brown: Je pense que cette question a été soulevée au cours de la première heure. Bien sûr, cela aura une incidence positive parce que les

[*Traduction*]

organismes auront une idée plus nette des attentes.

À dire vrai, il s'agit d'une question dont nous avons discuté aux premiers jours des délibérations sur la législation. Admettant que le régime de responsabilité comportait des lacunes, nous voulions nous assurer que ces dernières seraient corrigées de manière à ne pas avoir d'incidence directe ou néfaste sur les capacités opérationnelles des organismes. Nous l'avons fait notamment en clarifiant les choses et en précisant les attentes.

L'autre attente est limpide et figure dans la Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement, par exemple. Nous nous attendons à ce que ce comité et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement se consultent mutuellement et collaborent pour éviter les chevauchements inutiles et assurer la coordination de leurs activités.

Il ne fait aucun doute que ces mesures favoriseront une plus grande transparence et permettront à la population de mieux comprendre nos activités quotidiennes; je pense d'ailleurs que c'est là un des objectifs visés.

Nous prenons également des mesures pour simplifier le processus dans le cadre de l'initiative de transparence pour que les renseignements qui ne devraient pas être retenus soient rendus publics. Il ne devrait ainsi plus être nécessaire de passer par le processus d'accès à l'information ou d'autres processus pour divulguer l'information. Si nous la publions de manière proactive, nous allégeons le fardeau.

J'admets volontiers que certaines remarques ont été formulées sur l'augmentation du fardeau, mais, comme Tricia l'a souligné, tous les sous-ministres ont indiqué qu'ils accueillent favorablement le cadre de surveillance et d'examen proposé, et qu'ils peuvent y fonctionner efficacement.

Le président: Merci, monsieur Picard.

Monsieur Motz, vous disposez de cinq minutes.

● (1240)

M. Glen Motz: Merci, monsieur le président.

Mon collègue a lancé la discussion, et un témoin a soulevé la question devant le Comité. Il s'agit de la question du renseignement et de la preuve, et de l'incapacité d'utiliser les renseignements recueillis ailleurs à titre de preuve devant les tribunaux sans compromettre la sécurité nationale, un informateur ou autre chose. Le présent projet de loi fait-il quoi que ce soit qui habilite les agents d'exécution de la loi ou les procureurs de la Couronne sur le plan des questions de sécurité nationale?

M. Malcolm Brown: Vous avez peut-être remarqué certains hochements de tête et quelques mines longues. La question est fort complexe.

M. Glen Motz: En effet.

M. Malcolm Brown: Lorsque nous travaillons avec nos amis du ministère de la Justice, nous avons des échanges et des discussions, et nous dialoguons avec nos collègues des provinces et des territoires pour les questions qui concernent la justice et la sécurité publique. Nous nous entendons généralement pour dire que nous devons faire mieux, mais le projet de loi C-59 ne propose pas de changements. Comme je l'ai dit, nous collaborons activement avec nos collègues du ministère de la Justice afin de trouver des moyens d'améliorer le statu quo, et ces discussions incluent les autorités provinciales également.

M. Glen Motz: Merci, monsieur Brown.

Si j'ose interpréter ce que vous venez de me dire, se pourrait-il que le projet de loi C-59 doive être renforcé à cet égard?

M. Malcolm Brown: Eh bien, c'est au Comité qu'il revient d'en décider.

M. Glen Motz: Oui, j'en suis conscient.

M. Malcolm Brown: Je dirai que c'est une question fort complexe qui, à dire vrai, requiert le point de vue et la participation des fonctionnaires. Je ne pense pas que je révèle quoi que ce soit... je le fais probablement, mais...

Des voix: Ah, ah!

M. Malcolm Brown: Je ne pense pas révéler quoi que ce soit sur nos délibérations avec nos collègues provinciaux. Nous discutons activement de la question sans en arriver à un consensus, et c'est un problème, un défi pour nous tous.

M. Glen Motz: Je n'irai pas plus loin sur le sujet, mais j'aurai le courage de dire que le projet de loi C-59 devrait inclure des dispositions pour que vous travailliez avec les autres ministères pour atteindre vos objectifs. Le projet de loi devrait être renforcé, si je vous comprends bien.

M. Malcolm Brown: Je ne suis pas certain que nous ayons besoin d'une disposition législative pour cela. C'est une question vraiment importante, et nous agissons activement, comme je l'ai souligné. À dire vrai, le défi vient du fait qu'il existe bien des problèmes profonds concernant la manière dont l'information est recueillie, les contraintes relatives à l'échange de renseignements, le degré d'efficacité de ces activités et leurs répercussions sur le fonctionnement des systèmes juridiques fédéral et provinciaux.

Des discussions et des processus sont en cours, et je dirais que les fonctionnaires s'efforcent de réaliser des progrès. Le problème, c'est que chacun a des opinions bien tranchées.

M. Glen Motz: Merci, monsieur Brown.

Je dirai enfin que je ne vois rien dans le projet de loi qui porte vraiment sur des questions comme la prise de contrôle d'Aecon et la vente d'actifs nationaux ou de nature délicate à la Chine ou à des pays semblables. Pourriez-vous nous expliquer le rôle que le SCRS pourrait jouer dans le cadre de ce processus et nous indiquer s'il faut apporter des amendements au projet de loi pour améliorer la situation?

Les représentants des autres ministères peuvent également donner leur son de cloche dans le temps qu'il me reste.

Mme Tricia Geddes: Cela s'inscrit certainement dans notre mandat, et nous prodiguons des conseils au gouvernement avec d'autres organismes et ministères gouvernementaux. Ces conseils sont bien entendu du plus haut secret, mais le gouverneur en conseil peut certainement autoriser, révoquer ou imposer des mesures d'atténuation au chapitre des investissements. Vous savez probablement comment le processus fonctionne. Le SCRS est en mesure de soutenir ces démarches, mais, comme vous le faites remarquer, il s'agit d'un domaine où les pressions sont fortes et où une somme considérable d'efforts est exigée du Service.

M. Glen Motz: Le projet de loi C-59 renforce-t-il en quoi que ce soit votre rôle dans ce processus?

Mme Tricia Geddes: À mon avis, les outils et les pouvoirs qu'il nous confère, notamment en vertu de la disposition sur l'analyse des données, nous aideront certainement à cet égard.

● (1245)

Le président: Madame Damoff, vous disposez de cinq minutes.

Mme Pam Damoff: Merci, monsieur le président. Je n'ai qu'une question afin de donner suite à celles que mon collègue a posées.

Quelle incidence les modifications apportées au projet de loi C-59 concernant la Commission civile d'examen et de traitement des plaintes et la GRC plus précisément auront-elles sur cette dernière? Considérez-vous que le projet de loi permettra à la GRC de mieux travailler? Pouvez-vous nous donner un peu plus d'informations à ce sujet?

Monsieur Brown, je ne sais pas si c'est vous ou la GRC qui devrait répondre à cette question.

M. Malcolm Brown: Je dirais très brièvement que d'une certaine manière, nous tentons de départager les responsabilités de la Commission civile d'examen et de traitement des plaintes et celles de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement sur le plan des examens de la sécurité nationale. Je pense que les choses ont été éclaircies en ce qui concerne le traitement des plaintes et ce genre de tâches.

Gilles.

S.-comm. Gilles Michaud: Pour les organismes, ce changement est le bienvenu, car nous faisons rarement cavalier seul lorsque nous exécutons leur mandat de sécurité nationale. Nous collaborons toujours avec nos partenaires ici présents, l'Agence des services frontaliers du Canada et d'autres organismes. Comme certaines de nos activités doivent faire l'objet d'un examen, un seul organisme peut difficilement mener à bien cette tâche à moins de s'intéresser à l'éventail des parties concernées.

Pour notre part, nous considérons ce changement d'un oeil favorable.

Mme Pam Damoff: Merci. Je n'ai pas d'autres questions.

Le président: Merci.

Monsieur Dubé, vous disposez de cinq minutes, puis, aussi choquant que cela puisse paraître, j'exercerai peut-être ma prérogative de président pour poser moi-même une ou deux questions.

M. Matthew Dubé: Merci, monsieur le président.

Ma question s'adresse peut-être aux représentants du ministère de la Justice. Dans l'énoncé sur le respect de la Charte, il est question des attentes relatives au droit à la vie privée en ce qui a trait aux renseignements publics, lesquelles seraient considérées comme peu élevées pour ce genre de renseignements.

Comment ce concept a-t-il évolué dans la loi en ce qui concerne les attentes des gens? Je pose cette question à titre de personne qui n'est pas avocate. Autrement dit, pour en revenir à l'exemple, je pense que bien peu de gens savent que des renseignements peuvent être achetés légalement alors qu'ils pourraient cadrer avec cette définition. Les attentes raisonnables quant au droit à la vie privée sont-elles différentes si on utilise des outils comme les médias sociaux, où d'aucuns pourraient faire valoir que les connaissances sont lacunaires à cet égard?

M. Scott Millar: Je sais que Doug témoigne plus au sujet des politiques qu'à titre d'expert de la Charte; je me ferai donc un plaisir de répondre à cette question.

Il faut garder certaines choses à l'esprit. Sachez tout d'abord que le projet de loi fera l'objet d'un examen pour en vérifier la légalité. En ce qui concerne les autorisations ministérielles que nous aurons ou que nous réclamerons et qui contiendront des renseignements que nous aurons recueillis, il y aura des attentes raisonnables quant au droit à la vie privée. Lorsque nous préparons ces autorisations, le ministère de la Justice étudie les documents, lesquels s'apparentent à des affidavits, pour s'assurer que nous avons pris les précautions suffisantes.

Pour ce qui est du traitement des renseignements rendus publics dans le projet de loi, on considère qu'il s'agit d'informations publiques destinées à être publiées; ainsi, tous les renseignements que nous recueillons en vertu de ces dispositions devront satisfaire aux critères, des critères qui feront l'objet d'un examen et de commentaires dans l'avenir.

M. Matthew Dubé: Pouvez-vous m'expliquer ce que cela signifie précisément si on évalue la nationalité d'une personne ou d'une organisation, par exemple?

Mme Shelly Bruce: Comme mon collègue l'a déjà souligné, ce n'est rien de nouveau. Le Centre de la sécurité des télécommunications doit examiner des entités et des éléments d'information inconnus pour tenter d'en comprendre la nature exacte. Il pourrait simplement effectuer des recherches sur Google ou dans d'autres bases de données pour l'aider à comprendre de quoi il s'agit. Dans le cas d'une adresse IP, il existe des registres en ligne qui indiquent leur pays d'enregistrement.

M. Matthew Dubé: Quand vous dites « d'autres bases de données », c'est assez vague. Pouvez-vous me donner un exemple de base de données? Avec tout le respect que je vous dois, je trouve ce genre de formulation troublant.

Mme Shelly Bruce: Le mieux que je puisse faire pour vous rassurer, c'est probablement vous dire qu'un commissaire examine depuis plus de 20 ans les activités du Centre en matière de droit à la vie privée. Lorsqu'il évalue ces activités pour en vérifier la légalité, il étudie ce genre de démarches et les recherches dans les sources ouvertes que nous effectuons à l'appui de nos activités, car un grand nombre d'entre elles exigent que les recherches soient efficaces. À ce que je sache, il n'a jamais décelé de problème quant au degré des recherches effectuées par le Centre, aux sources que nous avons consultées ou à la manière dont nous avons traité et géré l'information.

● (1250)

M. Scott Millar: Non, en effet.

J'ajouterais que nous accomplissons ces activités à l'appui de notre mandat. Je pense qu'il importe de souligner quelque chose dont nous n'avons pas beaucoup eu l'occasion de parler jusqu'à présent. Gardez à l'esprit que dans le cadre de certaines de ces activités, nous assurons la cybersécurité des réseaux et des systèmes du gouvernement du Canada. Ce sont ces mêmes réseaux qui renferment les renseignements sur les contribuables et l'assurance-emploi; il s'agit donc de renseignements personnels canadiens de nature très délicate. Nos détecteurs bloquent jusqu'à un milliard d'interventions malintentionnées par jour. Ces cybermenaces visent à détecter des points vulnérables ou à commettre carrément des attaques.

Si je vous dis cela, c'est parce que j'admets que lorsqu'on discute de la mesure dans laquelle les renseignements personnels sont protégés, il faut savoir si on traite la sécurité et le caractère secret de l'information de manière raisonnable et proportionnelle. Je ferais aussi remarquer que notre mandat consiste également à protéger les renseignements personnels des Canadiens. Nous accomplissons ces activités dans la mesure nécessaire à l'exécution de ce mandat de protection de l'information.

M. Matthew Dubé: En ce qui concerne les mesures que vous prenez à l'insu de la population, c'est un défi, n'est-ce pas? Vous avez indiqué que vous entreprenez certaines démarches pour protéger les renseignements personnels, en ce qui concerne, par exemple, ce qui est proposé à l'article 25 et ce genre de chose. Existe-t-il un moyen pour que les parlementaires soient informés de ce qu'il se passe? Malheureusement, après avoir lu le projet de loi, il me semble que des mesures sont prévues et vous dites que vous les appliquez, mais nous n'en savons pas nécessairement plus à cet égard.

Mme Shelly Bruce: Nous publions sur notre site Web une fiche technique qui souligne les mesures que nous prenons pour protéger la vie privée. Au fur et à mesure qu'évolue la technologie et que les informations deviennent disponibles, nous veillons à nous tenir au courant et à adopter des mesures de plus en plus efficaces pour protéger la vie privée. Elles ne sont pas précisées dans la mesure législative, mais elles le sont dans les autorisations ministérielles. Dans le cadre de ces autorisations, qui doivent être renouvelées chaque année, le ministre peut fixer ses attentes et les élever et modifier les paramètres entourant nos activités.

M. Scott Millar: Si vous me le permettez, j'ai omis quelque chose dans ma réponse à la question précédente concernant les changements qu'entraînerait pour nous cette mesure législative. Nous avons parlé, entre autres, de mandats. Les mesures de reddition de comptes et d'examen s'appuient sur des mesures solides déjà existantes et mises en place par le commissaire du CST, mais cet élément de l'OSASNR, l'office de surveillance, avec le comité des parlementaires permet à ceux qui en sont autorisés de voir tout ce que nous faisons, que ce soit dans un environnement classifié ou non et d'examiner tous ces éléments de proportionnalité et le caractère raisonnable de ces éléments.

Cette mesure législative est aussi plus transparente — aussi transparents que peut l'être une mesure législative —, sur nos activités, les restrictions auxquelles nos activités sont assujetties et les diverses interdictions. Nous tentons d'ajouter des informations sur notre site Web. Nous sommes un organisme clandestin qui doit agir de façon clandestine afin de comprendre la menace et de protéger le Canada. Mais, nous sommes de plus en plus présents. Nous sommes sur Twitter. Nous publions des rapports sur des institutions démocratiques et les menaces qui pèsent contre ces institutions. Nous chercherons toujours de nouvelles façons de partager davantage d'informations sur ce que nous faisons.

Mme Shelly Bruce: J'ajouterais que...

Le président: M. Dubé a largement dépassé son temps d'intervention.

Si vous me le permettez, j'aurais une question à poser. J'aimerais revenir sur l'échange entre Mme Bruce et M. Fragiskatos concernant l'infrastructure privée.

La discussion porte principalement sur l'infrastructure publique. Cela me rappelle une conversation que j'ai eue la semaine dernière avec un représentant du secteur bancaire. Selon lui, lorsque nous fournissons des informations aux services de sécurité, cette information disparaît et nous n'en entendons plus parler. À mon avis, cette cyberinfrastructure est partagée entre les secteurs privé et public, mais le projet de loi C-59 ne parle pas de l'infrastructure privée — enfin, pas de façon évidente. Cette question a rongé les Britanniques. Le gouvernement britannique est intervenu activement pour protéger l'infrastructure privée.

Premièrement, qu'apporte le projet de loi C-59 en ce qui a trait à un cadre? Deuxièmement, quelle est la prochaine étape, disons, pour régler cette situation?

● (1255)

Mme Shelly Bruce: Le projet de loi ne fait pas directement référence à l'infrastructure critique, mais je crois qu'il fait référence aux systèmes non gouvernementaux qui sont essentiels à l'infrastructure critique, car, comme vous le dites, notre infrastructure mondiale d'information est composée d'entreprises du secteur privé et public.

Dans cet environnement, le CST, qui se concentre actuellement à défendre l'infrastructure gouvernementale et à bloquer certaines activités, peut uniquement conseiller et orienter les propriétaires d'infrastructures critiques de façon à ce que l'information soit accessible au grand public.

À cet égard, le projet de loi C-59 permet au CST d'utiliser l'expertise existante — les outils, les capacités.... D'ailleurs, certaines de ces capacités ont été présentées aux propriétaires d'infrastructures critiques sous forme d'un outil appelé « Assembly Line ». Ces informations sont connues. Cet outil a été développé à l'interne, mais d'autres peuvent s'en servir pour trier et comprendre les logiciels malveillants qui pourraient attaquer leurs systèmes.

Le CST pourrait même aller plus loin avec cette mesure législative pour aider les propriétaires d'infrastructures critiques qui demandent notre aide et que le ministre a désignés comme étant admissibles à recevoir l'aide du CST.

Le président: Quel sera le processus officiel? Je sais que certaines institutions ont des structures massives, possiblement plus importantes que les structures gouvernementales. Comment tout cela fonctionnera-t-il sur le plan pratique afin que les intérêts de tous soient protégés?

Mme Shelly Bruce: C'est une bonne question.

Au fur et à mesure que la législation sera renforcée et que nous comprenons sa portée, si ces autorités reçoivent l'autorisation nécessaire, il reviendra au CST de travailler avec Sécurité publique, les propriétaires d'infrastructures critiques et le ministre afin de définir les risques et d'établir des priorités, car, comme vous le soulignez, il sera impossible de calmer toutes les inquiétudes et d'examiner toutes les infrastructures qui existent au pays.

M. Malcolm Brown: Cela fait partie du mandat du ministre de la Sécurité publique. Vous posez une question-cadre sur la façon dont le gouvernement approchera la situation. Il s'agit d'un élément fondamental. C'était une lacune du mandat du CST qui limitait l'aide qu'il pouvait apporter dans le contexte actuel.

Comme je l'ai déjà dit, le gouvernement effectue un examen de la cybersécurité. Les résultats de cet examen seront disponibles bientôt, enfin, je l'espère. Un des éléments clés de cet examen — et j'ajouterais que Sécurité publique gère la relation avec le secteur des infrastructures critiques — est de savoir où aller, vers qui se tourner lorsqu'il y a un problème. La taille du système importe peu; il faut avoir les bons contacts. Actuellement, on communique parfois avec le CST ou le Centre canadien de réponse aux incidents cybernétiques, le CCIRC, de Sécurité publique. Nous devons faire un meilleur travail pour coordonner le tout.

Une bonne partie de cette information se trouve dans un écosystème où l'information doit être partagée très rapidement et il s'agit d'un rôle clé que le CST peut jouer. C'est une question d'expertise technique. Je vais utiliser l'analogie d'un incendie. Nous demandons à des pompiers d'éteindre un incendie. Dans ce cas-ci, un seul pompier pourrait suffire, car tout ce qu'il faut, c'est un lien pour permettre aux gens de comprendre qu'il existe une solution et que cette solution peut s'appliquer à toute l'infrastructure.

Une grande société américaine inconnue a géré beaucoup de données confidentielles de citoyens. Une solution simple n'avait pas été mise en place, ce qui a eu un impact important sur toute l'organisation.

Il est important de bien encadrer le tout. À mon avis, il y aura de nouveaux développements au cours des prochains mois. Il s'agit d'un élément fondamental.

Le président: Merci, monsieur Brown, pour cette avant-dernière intervention.

Mesdames et messieurs les membres du comité, il nous reste une autre séance sur ce sujet. Nous devons accueillir deux autres témoins jeudi, mais un universitaire inconnu a proposé d'inviter la Commission civile d'examen et de traitement des plaintes contre la GRC. La Commission serait disponible. Je propose donc de l'ajouter à la liste. Cela complétera l'ordre du jour de la séance de jeudi. Je propose également que le sous-comité se réunisse jeudi après-midi, après les témoignages, afin d'établir le calendrier qui nous mènera vers l'étude article par article.

Ceci dit, je tiens à remercier tous ceux qui ont participé à ces délibérations. Vous êtes certainement très compétents et avez été très attentifs à toutes les questions des membres.

La séance est levée.