CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 093 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 30 janvier 2018

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mardi 30 janvier 2018

● (1100)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Mesdames et messieurs, la séance est ouverte.

Bienvenue à la 93e séance du Comité permanent de la sécurité publique et nationale. Pendant la première heure, nous entendrons l'honorable Jean-Pierre Plouffe, du Bureau du commissaire du Centre de la sécurité des télécommunications. Il est accompagné de M. Gérard Normand et de M. William Galbraith.

Vous êtes un habitué de notre comité, et je vais donc vous laisser faire votre déclaration liminaire. Comme vous le savez, les députés vous poseront ensuite des questions. Nous sommes impatients d'entendre votre déclaration, monsieur Plouffe.

Merci.

L'hon. Jean-Pierre Plouffe (commissaire, Bureau du commissaire du Centre de la sécurité des télécommunications): Merci, monsieur le président.

[*Français*]

Monsieur le président, mesdames et messieurs les députés, je suis heureux de comparaître de nouveau devant ce comité, cette fois au sujet du projet de loi C-59. Je suis accompagné par M. William Galbraith, qui est directeur exécutif de mon bureau, et par Me Gérard Normand, qui est conseiller juridique spécial et avocat général.

Je suis le commissaire du Centre de la sécurité des télécommunications, le CST, depuis plus de quatre ans. Je suis responsable de procéder à des examens concernant les activités du CST pour en contrôler la légalité, dans un premier temps. Cela comprend naturellement tout ce qui concerne la protection de la vie privée des citoyens et des personnes qui se trouvent au Canada. Je suis un juge à la retraite de la Cour supérieure du Québec et de la Cour d'appel de la cour martiale du Canada. Comme j'aime le dire souvent quand je comparais devant vous,

[*Traduction*]

Je suis un jeune de 75 ans.

[*Français*]

Lorsqu'on parle d'un juge à la retraite, il ne faut pas s'attendre à ce qu'il s'agisse d'une personne âgée de 40 ou de 50 ans. Pour prendre notre retraite, il faut que nous ayons au moins 69 ou 70 ans. Cela explique mon âge quelque peu avancé.

La loi exige effectivement que le commissaire du CST soit un juge surnuméraire, c'est-à-dire un juge qui siège à temps partiel, ou un juge à la retraite d'une cour supérieure. Mon mandat actuel prendra fin à la mi-octobre de cette année, soit en 2018.

[*Traduction*]

Cependant, une fois que le projet de loi C-59 aura reçu la sanction royale, mon rôle changera pour devenir une toute nouvelle — et j'insiste là-dessus — fonction dans le domaine du renseignement au Canada.

En effet, le commissaire ne procédera plus à l'examen des activités du CST après coup. Le commissaire au renseignement exercera plutôt un rôle quasi judiciaire d'examen et d'approbation des autorisations délivrées par les ministres pour certaines activités du CST et du SCRS avant que ces activités ne puissent être menées.

Plus précisément, le commissaire devra déterminer si les conclusions du ministre sur lesquelles repose l'autorisation de l'activité sont raisonnables. Les conclusions devront être jugées raisonnables. C'est essentiellement semblable à la fonction exercée par un tribunal dans le cadre de ce que nous appelons une « révision judiciaire ».Il s'agit selon moi d'un rôle crucial, qui vise à assurer l'examen quasi judiciaire des activités menées par les organismes du renseignement qui peuvent avoir une incidence sur la Charte ou la vie privée.

● (1105)

[*Français*]

La partie 2 du projet de loi C-59, qui édicte la Loi sur le commissaire au renseignement, prévoit expressément la transition du rôle du commissaire du CST au nouveau rôle de commissaire au renseignement. Les fonctions d'examen à postériori des activités du CST dont je m'acquitte actuellement incomberont au nouvel Office de surveillance des activités en matière de sécurité nationale et de renseignement, comme c'est également proposé dans le projet de loi C-59.

[*Traduction*]

J'ajoute que le projet de loi exige aussi que le commissaire au renseignement soit un juge à la retraite d'une juridiction supérieure, ce qui est indiqué selon moi compte tenu de la fonction quasi judiciaire du nouveau poste. Par contre, le projet de loi ne prévoit pas la possibilité de nommer un juge surnuméraire, comme c'est le cas dans la Loi sur la défense nationale pour le commissaire du CST. Je suis d'opinion que le projet de loi devrait maintenir cette possibilité de nommer un juge surnuméraire, en partie pour assurer un meilleur bassin de candidats potentiels. J'étais juge surnuméraire lorsque j'ai été nommé commissaire du CST il y a quatre ans, et j'ai pris ma retraite comme juge peu de temps après.

Le problème est le suivant. Le bassin de candidat pour ce poste, le nouveau poste de commissaire au renseignement, est très limité. Il faut trouver un juge à la retraite qui a la bonne expérience — par exemple en matière de sécurité ou de défense nationale. Le bassin est très limité. C'est la raison pour laquelle je propose de garder dans le projet de loi ce que nous avons dans la Loi sur la défense nationale concernant la nomination d'un commissaire au renseignement. Autrement dit, un juge surnuméraire devrait être nommé commissaire au renseignement avant de prendre sa retraite quelques mois plus tard. Ce serait une mesure transitoire. Je peux envisager que dans l'éventualité où un juge en exercice demeurerait commissaire au renseignement pendant des années, il pourrait avoir des problèmes de conflits d'intérêts et ainsi de suite. Je crois en revanche que cela pourrait être très utile à des fins transitoires.

Avant l'audience, j'ai présenté au Comité une copie de propositions d'amendements au projet de loi C-59. Ces observations ont été transmises à votre président le 6 décembre 2017. Je vais aussi vous soumettre aujourd'hui des listes comprenant des propositions d'amendements substantielles et techniques que j'ai déjà envoyées aux ministres Goodale et Sajjan. Je soulignerai dans mon allocution plusieurs de ces propositions.

[*Français*]

Le processus que le gouvernement a choisi d'adopter en ce qui concerne ce projet de loi revêt de l'importance en ce qu'il permet d'accueillir, comme l'a dit le ministre Goodale, la présentation de nouvelles idées et d'autres suggestions avant l'étape de la deuxième lecture à la Chambre.

[*Traduction*]

Dans ce contexte, je traiterai des changements que je propose à trois parties de ce projet de loi: la partie 2, la Loi sur le commissaire au renseignement; la partie 3, la Loi sur le Centre de la sécurité des télécommunications; et la partie 4, qui modifie la Loi sur le Service canadien du renseignement de sécurité. J'estime qu'en règle générale, le projet de loi est bien ficelé et qu'il répond à la plupart des recommandations mises de l'avant par mes prédécesseurs et moi-même pour modifier la partie V.1 de la Loi sur la défense nationale. Par contre, je crois toutefois, après l'avoir analysé en profondeur et après avoir discuté avec des fonctionnaires et des organismes directement concernés, que certaines modifications devraient être proposées. Je décrirai donc sept propositions sur le fond que je considère comme les plus importantes parmi celles que je propose.

Premièrement, j'estime que le commissaire au renseignement devrait jouer un rôle dans l'approbation des autorisations de cyberopérations actives et de cyberopérations défensives du CST, qui pourraient aussi avoir une incidence sur des intérêts de nature privée. Certains commentateurs ont fait remarquer qu'il s'agit là d'un nouveau mandat très étendu pour le CST et qu'il est trop permissif. En comparaison, la Loi sur le Service canadien du renseignement de sécurité exige du SCRS qu'il porte, dans certains cas, l'affaire devant un juge de la Cour fédérale afin d'obtenir un mandat pour des activités similaires.

● (1110)

[*Français*]

Deuxièmement, tel que le projet de loi est libellé actuellement, la décision du ministre de prolonger d'une autre année la période de validité d'une autorisation touchant le renseignement étranger ou la cybersécurité délivrée au CST n'est pas assujettie à l'approbation du commissaire au renseignement. J'estime que le commissaire devrait être impliqué dans cette demande de prolongation, étant donné qu'il aura joué un rôle dans l'approbation de l'autorisation initiale. Autrement, la période de validité de toute autorisation serait, en pratique, pour une période de deux ans. Or, ce n'est pas ce que prévoit la loi. Elle prévoit que ce genre d'autorisation est valable pour un an au maximum. Si le ministre approuvait de façon quasi automatique la demande de renouvellement sans que le commissaire soit impliqué, on pourrait se retrouver avec une durée de deux ans, au lieu de la durée d'un an prévue par la loi.

[*Traduction*]

Troisièmement, les autorisations en cas d'urgence qui sont délivrées au CST par le ministre et qui se rapportent au renseignement étranger et à la cybersécurité devraient également être assujetties à l'examen du commissaire tout de suite après leur délivrance. Une telle approche serait semblable à celle prévue dans la loi britannique, la Investigatory Powers Act. En vertu de cette loi, la période de validité des autorisations en cas d'urgence est de cinq jours, tout comme dans le projet de loi C-59. Cependant, toujours en vertu de la loi britannique, le commissaire judiciaire en Grande-Bretagne est appelé à réviser et à décider de l'approbation de la mesure d'urgence pendant ce délai.

Le président: Nous devrons malheureusement... Pouvez-vous résumer vos quatre derniers points en moins de 30 secondes?

L'hon. Jean-Pierre Plouffe: Si vous me donnez deux ou trois minutes, je pense que je pourrais vous les résumer.

Le président: Ce qui me pose problème, c'est que lorsque je vous donne deux ou trois minutes, je dois ensuite faire face au mécontentement de tous mes collègues. Je peux vous donner une minute pour conclure.

L'hon. Jean-Pierre Plouffe: Je vais essayer de finir les propositions, car je sais qu'une des questions portera sur ces points.

Le président: Bien.

L'hon. Jean-Pierre Plouffe: J'ai été prévenu.

Le président: Bien, merci.

[*Français*]

L'hon. Jean-Pierre Plouffe: Quatrièmement, j'estime que le commissaire devrait avoir le pouvoir, lorsqu'il se livre au processus d'examen et d'approbation, de demander des précisions sur les renseignements qui lui sont présentés et qui ont été utilisés par le ministre pour rendre sa décision. Sans cette capacité de demander des précisions, le commissaire, s'il s'interroge sur certains renseignements, pourrait bien n'avoir d'autre choix que celui d'établir que la conclusion du ministre sur laquelle repose l'autorisation n'était pas raisonnable.

[*Traduction*]

Cinquièmement, à mon avis, le commissaire au renseignement devrait pouvoir approuver une autorisation sous certaines conditions, et il appartiendrait alors au ministre d'accepter d'ajouter la condition définie par le commissaire.

Il ne m'en reste plus que deux.

[*Français*]

Sixièmement, le commissaire au renseignement devrait établir un rapport annuel public à l'intention du premier ministre, qui serait déposé devant les deux Chambres. Ce rapport marquerait bien l'indépendance du commissaire et renforcerait la transparence et la confiance du public.

[*Traduction*]

Septièmement et finalement, je crois qu'un pouvoir de réglementation devrait être enchâssé dans la Loi sur le commissaire au renseignement afin d'assurer le respect des objectifs et des dispositions de la loi.

[*Français*]

Je vous remercie de m'avoir donné l'occasion de comparaître devant vous aujourd'hui. Nous serons heureux de répondre à vos questions.

Merci, monsieur le président.

[*Traduction*]

Le président: Je vous remercie de votre exposé rigoureux et bien préparé.

Je vais maintenant donner la parole à M. Spengemann, pour sept minutes.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Je ne crois pas que c'est l'ordre convenu, monsieur le président.

Le président: Vous devez avoir une liste différente de la mienne.

C'est donc Mme Dabrusin. Merci.

Mme Julie Dabrusin (Toronto—Danforth, Lib.): Merci beaucoup de votre exposé. C'était très intéressant, car lorsque j'ai demandé aux gens de ma collectivité ce qu'ils voulaient voir dans notre régime de sécurité nationale, ils ont entre autres parlé d'une meilleure surveillance. Ils y accordent une attention particulière. Il m'est très utile d'en apprendre davantage sur vos idées et sur la façon dont le projet de loi vise à atteindre cet objectif, et j'en suis très reconnaissante.

J'ai consulté un rapport préparé par le Citizen Lab de la Munk School of Global Affairs. Il contient plusieurs recommandations concernant le commissaire à l'information et la surveillance. Comme vous avez oeuvré un peu dans le système et que vous comprenez comment il fonctionne, je me demandais si vous pouviez me donner une idée de l'applicabilité de ces recommandations.

Je crois que l'une d'elles porte sur les derniers points que vous avez soulevés, qu'elle pourrait cadrer avec ces points. Le rapport recommande que les autorisations en cas d'urgence proposées à l'article 41 soient examinées a posteriori par le commissaire au renseignement. Comment cette recommandation cadre-t-elle avec vos propositions? Pensez-vous que cela fonctionnerait bien dans le cadre de ce que vous proposez aujourd'hui?

● (1115)

L'hon. Jean-Pierre Plouffe: Je vais demander au conseiller juridique général de répondre. J'ai abordé la question dans ma déclaration liminaire...

Mme Julie Dabrusin: Oui.

L'hon. Jean-Pierre Plouffe: ... mais je vais demander à Normand de répondre.

M. Gérard Normand (conseiller juridique spécial, Bureau du commissaire du Centre de la sécurité des télécommunications): Essentiellement, ce n'est pas aussi détaillé que ce que nous avons prévu, car nous nous sommes inspirés de la loi britannique, mais l'idée est la même. En gros, le ministre pourrait prendre une décision dans des situations d'urgence, mais elles seraient revues dans les cinq jours par le commissaire. Ensuite, en fonction de l'examen mené et de la décision, il y aurait ou non des répercussions sur l'autorisation en cours. D'une certaine façon, nous proposons essentiellement la même chose.

Mme Julie Dabrusin: C'est la même idée. Parfait.

L'autre proposition était d'exiger des raisons écrites lors de l'approbation d'une autorisation, pas seulement en cas de refus. Que pensez-vous de cette proposition?

L'hon. Jean-Pierre Plouffe: Le projet de loi prévoit qu'en cas de refus par le commissaire au renseignement de la demande que lui présente le ministre — ou, je devrais dire, de sa décision —, le commissaire doit donner des raisons. En revanche, il n'a pas à en donner s'il approuve l'autorisation délivrée par le ministre.

En tant que juge à la retraite, je n'ai pas d'objection à fournir des raisons. C'est ce que j'ai fait toute ma vie. On en fournit quand on prononce un jugement, quel qu'il soit. Je ne suis pas contre la proposition voulant que le commissaire fournisse des raisons même lorsqu'il approuve la décision du ministre de délivrer une autorisation. De toute évidence, ces raisons seraient plutôt courtes comparativement à celles présentées lorsque les conclusions du ministre sont jugées irraisonnables par le commissaire au renseignement, mais je ne suis pas contre cette proposition.

M. Gérard Normand: À vrai dire, surtout au cours des premières années, je pense que les raisons seraient utiles pour permettre aux organismes de comprendre la réflexion du commissaire dans le cadre du processus visant à déterminer le caractère raisonnable des décisions.

Mme Julie Dabrusin: Merci de ces explications.

Dans vos observations, vous avez mentionné avoir vu le commissaire à l'information autoriser des cyberopérations actives et des cyberopérations défensives. Je me demande si vous pouvez en dire plus long. Comment percevez-vous ce rôle? À quoi ressemble-t-il?

L'hon. Jean-Pierre Plouffe: C'est une question complexe. Les dispositions du projet de loi relativement aux cyberopérations actives et défensives sont complexes.

Mme Julie Dabrusin: J'ai le projet de loi en main. Donc, si vous voulez...

L'hon. Jean-Pierre Plouffe: On m'a essentiellement expliqué que le commissaire au renseignement n'aurait pas de rôle à jouer, car, contrairement à ce qui se fait dans le cadre de cyberopérations actives ou défensives, aucun renseignement n'est recueilli. On laisse entendre qu'aucun droit garanti par le Charte ou droit à la vie privée ne serait touché par les techniques qui seraient utilisées à l'extérieur du Canada. Je parle ici du CST.

Malheureusement, je ne suis pas nécessairement d'accord, tout comme le ministère de la Justice, qui est le conseiller juridique du gouvernement. Je vais citer une partie de l'avis juridique du ministère de la Justice, qui se trouve à la page 9 d'un document intitulé « Énoncé concernant la Charte - Projet de loi C-59 ». C'est court, mais cela explique ma position.

> Les dispositions autorisant les cyberopérations actives ne feraient intervenir par définition aucun droit ou liberté protégé par la Charte. Cependant, certaines des activités qui seraient autorisées par le ministre en vertu de ce régime pourraient potentiellement mettre en jeu des droits et libertés. Les considérations qui appuient la conformité avec la Charte de ce volet sont très similaires à celles qui appuient la conformité du mandat concernant les cyberopérations défensives. Une différence est toutefois l'objectif distinct des cyberopérations actives, qui serait de réaliser les objectifs impérieux du gouvernement liés aux affaires internationales, à la défense ou à la sécurité du Canada [...]

Aucune information n'est recueillie, mais les communications privées des gens seront perturbées, influencées et entravées, ce qui peut très bien, selon moi, avoir une incidence sur des Canadiens au même titre que la collecte par inadvertance de renseignements sur des Canadiens à l'étranger. À mon avis, il ne devrait y avoir aucune distinction entre la collecte de communications de Canadiens à l'étranger et la perturbation et l'entrave de communications de Canadiens à l'étranger, donc...

● (1120)

Mme Julie Dabrusin: J'interviens uniquement parce que je sais que je n'aurai bientôt plus de temps...

L'hon. Jean-Pierre Plouffe: C'est ma réponse...

Mme Julie Dabrusin: Je voulais juste savoir quel rôle alors le commissaire à l'information devrait jouer selon vous.

L'hon. Jean-Pierre Plouffe: Je pense que le commissaire au renseignement devrait participer à ces opérations.

M. Gérard Normand: Permettez-moi d'ajouter que le rôle serait similaire. L'examen et l'approbation seraient essentiellement les mêmes que pour les autres autorisations. On examinerait les faits présentés aux ministres ainsi que les aspects de la loi qui seraient utiles pour prendre la décision, pour s'assurer qu'elle repose sur les faits.

Le président: Je peux voir que j'aurai de la difficulté à faire respecter le temps de parole. C'est une importante discussion.

Avant de donner la parole à M. Motz, vous avez cité un... Je me demande si vous pouvez le transmettre au Comité, s'il ne peut pas déjà le consulter? Est-ce un bulletin?

L'hon. Jean-Pierre Plouffe: Je vais vous le remettre après.

Le président: Bien. Je vous en suis reconnaissant.

Monsieur Motz, vous avez sept minutes.

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

Je vous remercie, monsieur le commissaire, ainsi que les membres de votre équipe, d'être ici aujourd'hui.

Si je comprends bien, l'article 61 qui est proposé dans la Loi sur le Centre de la sécurité des télécommunications donne au Cabinet le pouvoir de modifier des passages de la Loi. C'est ce qu'on appelle communément la clause Henri VIII. L'article 61 qui est proposé...

L'hon. Jean-Pierre Plouffe: Vous parlez de l'article 61 qui est proposé dans la Loi sur le Centre de la sécurité des télécommunications, n'est-ce pas?

M. Glen Motz: ... accorde au Cabinet le pouvoir de modifier des passages de la Loi. C'est une pratique qui date de plusieurs siècles.

Pourquoi est-il nécessaire pour le Cabinet d'avoir le pouvoir de jouer le rôle du Parlement?

Dans la même veine, si c'est ce que le Parlement fait, ce que fait le Cabinet, une partie des modifications qu'ils veulent apportées — la Loi, les paramètres relatifs à la réglementation, à ce genre de choses — ne devrait-elle pas figurer dans des règlements pour faire en sorte que si... Nous savons que le cyberespace change rapidement, et s'il est nécessaire de rendre la Loi plus souple, ne serait-il pas préférable, plutôt que de donner ce pouvoir au Cabinet, de l'inscrire dans la réglementation pour que ce soit possible?

Qu'en pensez-vous, monsieur?

L'hon. Jean-Pierre Plouffe: J'ai proposé que le gouverneur en conseil prenne des règlements pour la raison suivante. Lorsque le projet de loi a été adopté et qu'il a reçu la sanction royale, dans une des dispositions — je ne me souviens plus exactement laquelle —, il est écrit que le ministre concerné doit fournir au commissaire au renseignement toute l'information qu'il a en main.

Ce n'est pas défini. On ne sait pas exactement ce qu'entend le législateur. Parlons-nous de séances d'information? Parlons-nous de rapports? Nous ne le savons pas. À mon avis, on pourrait prévoir une règle selon laquelle le bureau du commissaire au renseignement, à l'intention du bureau du ministre, établirait ce qui doit lui être transmis, à savoir toute l'information.

Pour ceux qui ont une formation juridique, c'est semblable aux pratiques des tribunaux. Nous parlons de procédure. Nous parlons, dans ce cas précis, de ce qu'on entend par « toute l'information », et je pense que cela donne une marge de manoeuvre dans le projet de loi.

● (1125)

[*Français*]

En français, je dirais que c'est de la cuisine.

[*Traduction*]

Comme le commissaire au renseignement a un rôle quasi judiciaire, on a besoin de règles de procédure équivalentes.

M. Glen Motz: Si je vous comprends bien, vous dites qu'il pourrait être nécessaire de modifier l'article 61 pour ajouter ces paramètres, pour ainsi dire, dans le but de fournir des éclaircissements dans la réglementation et d'éviter d'avoir une disposition qui accorde un pouvoir exclusif au Cabinet. Vous ai-je bien compris?

L'hon. Jean-Pierre Plouffe: Oui.

M. Glen Motz: Merci.

Une des choses qui m'intriguent, ce sont vos réflexions sur l'utilité des cyberattaques offensives, d'après votre expérience dans votre poste et vos antécédents à la magistrature. Je sais que c'est un sujet qui préoccupe certaines personnes, mais en ce qui a trait à notre sécurité nationale et publique, que pensez-vous personnellement d'une loi qui autorise les cyberattaques offensives ou les cyberopérations?

L'hon. Jean-Pierre Plouffe: Je n'essaie pas d'esquiver la question, mais je crois qu'il serait préférable de la poser au Centre de la sécurité des télécommunications, ou CST.

Je peux par contre dire qu'il s'agit d'un très vaste mandat pour le CST, et je trouve raisonnable que des commentateurs et des législateurs comme vous soulèvent le point et posent des questions. Au fond, avons-nous besoin de ce genre de technique en matière de sécurité? Dans l'affirmative, comment devrait-on la limiter? Devrions-nous exercer un rôle de surveillance sur ces pouvoirs?

Comme je l'ai dit, c'est très vaste.

M. Glen Motz: Vous avez parlé du Service canadien du renseignement de sécurité, ou SCRS. Comment comptez-vous coordonner votre travail entre le CST et le SCRS, pour éviter que les deux organismes se chevauchent dans vos efforts de prévention des attaques? Comment coordonnez-vous ces activités à l'heure actuelle? À votre avis, en quoi le texte législatif améliorera-t-il la situation à l'avenir?

L'hon. Jean-Pierre Plouffe: Comme vous le savez peut-être, la tâche première du commissaire au renseignement serait d'examiner et d'approuver les autorisations accordées par les ministres respectifs. C'est le premier point.

Par ailleurs, vous avez parfois besoin de l'avis d'experts — ce qui ressemble encore une fois à ce qu'un tribunal ferait. C'est pourquoi j'ai besoin de spécialistes à mon bureau — autrement dit, des gens qui savent ce que fait le SCRS, et d'autres qui savent ce que fait le CST — qui sont en mesure de me conseiller en conséquence. C'est un peu comme un juge qui demande l'aide de témoins experts venant le conseiller au tribunal, étant donné que le juge n'est pas un spécialiste.

Nous sommes d'ailleurs en train de restructurer mon bureau, et j'ai bel et bien ce genre de spécialistes à mes côtés.

M. Glen Motz: Merci, monsieur.

J'ai une dernière question. Mon temps est limité.

Vous nous avez déjà soumis sept recommandations de choses que vous aimeriez changer, et vous avez également des propositions techniques. Dans un monde idéal, si on vous accordait une marge de manoeuvre, que retireriez-vous du projet de loi? Qu'y ajouteriez-vous que vous n'avez peut-être pas eu la chance de mentionner?

L'hon. Jean-Pierre Plouffe: Dans mes observations liminaires, j'ai formulé sept propositions concrètes. Elles se trouvent dans le document que j'ai envoyé au président. J'ai insisté sur cinq ou six d'entre elles dans mon exposé. Aimeriez-vous que je les répète?

M. Glen Motz: Non.

J'ai une dernière question.

À votre avis, comment nous portons-nous comparativement à nos partenaires du Groupe des cinq dans la lutte contre les cybermenaces? Le projet de loi C-59 nous rendra-t-il encore plus agiles à ce chapitre?

Le président: C'est une question extrêmement vaste, et nous avons déjà dépassé le temps alloué. Pouvez-vous répondre en 15 secondes?

● (1130)

M. Gérard Normand: Oui.

Nous avons essentiellement examiné les dispositions législatives de quatre autres pays. Après avoir vu ce que les autres font, nous croyons savoir que les lois visent principalement les activités de défense et l'octroi d'aide à d'autres organismes. L'article proposé 31 permet au CST d'agir par lui-même et d'interrompre des activités qui se rapportent aux affaires internationales, à la défense ou à la sécurité, mais pas nécessairement dans un rôle d'aide ou de défense, que le Centre peut assumer aussi. Il semble y avoir une différence par rapport aux autres pays.

Le président: Merci, monsieur Motz.

[*Français*]

Monsieur Dubé, vous disposez de sept minutes.

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

Messieurs, je vous remercie d'être ici aujourd'hui.

J'ai une question, mais j'ai l'impression que vous ne voudrez pas trop vous avancer à répondre.

Pour ce projet de loi, on a manqué de temps. Ce n'est pas un reproche, au contraire, mais cela explique que des changements extrêmement importants soient proposés.

Vos propositions touchent principalement trois différentes parties du projet de loi, soit les parties 2, 3 et 4. Selon vous, aurait-il été approprié que les parties qui créent de nouvelles structures et qui élargissent énormément les pouvoirs du CST fassent l'objet d'un projet de loi distinct, plutôt que d'être compris dans un projet de loi de 130 pages qui vise plusieurs objectifs?

L'hon. Jean-Pierre Plouffe: Encore une fois, c'est au gouvernement de décider de cela.

Je sais que, à un moment donné, il y a eu des discussions pour déterminer s'il fallait diviser le projet de loi et étudier ses différentes parties séparément. Le gouvernement a pris la décision que ce n'était pas nécessaire. Il faut donc étudier le projet de loi dans son ensemble. Il va de soi que c'est plus complexe, mais cela ne nous empêche pas de faire des suggestions et de proposer les modifications qui s'imposent.

M. Matthew Dubé: Bien sûr.

Dans les réponses que vous avez fournies à certains de mes collègues, il a été question du mandat du CST. Mme Bossenmaier, qui est chef du CST, a comparu devant nous et je lui ai posé des questions notamment sur le paragraphe 24(1) proposé, où le premier alinéa parle d'exceptions dans le cas d'information accessible au public. Cela nous préoccupe, de même que les alinéas suivants. Mme Bossenmaier a mentionné que le mandat du CST touchait essentiellement les entités étrangères, et non les Canadiens. Il y a plusieurs questions que j'aimerais vous poser à ce sujet.

Premièrement, le mandat est-il légal ou est-il compris de facto par le CST?

En outre, des exceptions de ce genre sont incluses dans le projet de loi, mais on n'est pas vraiment en mesure de nous expliquer pourquoi. Par exemple, on dit ceci: « Le ministre peut, par arrêté, désigner comme étant importante pour le gouvernement fédéral de l'information électronique, des infrastructures de l'information [...] » Toutes ces questions sont vagues et on n'est pas en mesure de justifier l'ampleur de la portée.

J'ai abordé plusieurs questions, certaines sous forme de commentaires. J'aimerais simplement connaître votre point de vue sur ces sujets.

Quel est le mandat du CST? Le projet de loi est-il en train de le faire évoluer sans toutefois qu'on soit en mesure d'en justifier concrètement les raisons ni le but visé?

L'hon. Jean-Pierre Plouffe: Le mandat du CST n'est pas de cibler les Canadiens ou les gens au Canada. Le CST doit, selon la loi, cibler des entités étrangères. Cela ne change pas. Si d'aventure le CST décidait de cibler des Canadiens, ce serait illégal. À mon avis, c'est ce qui donne leur importance aux agences de surveillance, qu'il s'agisse du nouveau comité proposé ou du commissaire au renseignement, dont le nom devrait plutôt être « commissaire judiciaire au renseignement », à mon avis, étant donné qu'il joue un rôle quasi judiciaire. Je propose cette modification, soit dit en passant.

Il est nécessaire de considérer un ensemble de données pour s'assurer que le rôle de nos agences de renseignement, dont les activités sont en partie secrètes, est scruté par des agences de surveillance dignes de ce nom. Ainsi, on maintient la confiance du public à l'égard de ces agences.

M. Matthew Dubé: Même si le mandat n'est pas de cibler les Canadiens, certains aspects du projet de loi sont préoccupants à ce sujet. Je vais donc aborder plusieurs points rapidement.

Au paragraphe 22(1) proposé, on dit ceci:

> 22(1) Le ministre peut, par arrêté, désigner comme étant importante pour le gouvernement fédéral de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information.

Même si l'on cible des entités étrangères, l'infrastructure désignée peut se situer dans un écosystème global et être utilisée par les Canadiens.

L'autre élément sur lequel je veux attirer votre attention et obtenir vos commentaires, c'est l'article 23 proposé, qui parle précisément des exceptions concernant le ciblage des Canadiens. Cependant, on dit ceci au paragraphe 24(1) proposé:

> 24(1) Malgré les paragraphes 23(1) et (2), le Centre peut mener les activités ci-après dans la réalisation de son mandat :
>
> a) acquérir, utiliser, analyser [...] l'information accessible au public [...]

On précise ceci plus loin:

> Information acquise incidemment
>
> (4) Le Centre peut acquérir incidemment de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada au cours d'activités menées au titre d'une autorisation délivrée en vertu des paragraphes 27(1), 28(1) ou (2) ou 41 (1).

Malgré le mandat et ce qui est compris par l'organisme, il y a beaucoup d'échappatoires. Des Canadiens pourraient être touchés.

Compte tenu de l'échange d'information entre les organismes ainsi qu'avec nos alliés, notamment les Américains, et de l'absence de prescription quant à la durée de rétention des données, ne croyez-vous pas que des risques seraient encourus?

● (1135)

L'hon. Jean-Pierre Plouffe: Le directeur exécutif ou le conseiller juridique pourront sûrement répondre, mais juste avant, je voudrais préciser un point. À l'heure actuelle — et ce sera encore le cas si le projet de loi est adopté —, si le CST fait du ciblage à l'étranger et que, de façon auxiliaire, il intercepte des conversations ou des communications de Canadiens, il doit chaque fois obtenir une autorisation du ministre. Ce dernier doit personnellement autoriser ces activités. En outre, n'oubliez pas que l'autorisation, une fois qu'elle est accordée par le ministre, est révisée par les agences de surveillance. On veut ainsi s'assurer que tout est conforme à la loi. C'est donc dire que des paramètres sont établis pour s'assurer que les activités des agences sont légales et ne vont pas à l'encontre de la vie privée des Canadiens.

D'après votre question, je constate que le public a un peu de difficulté à cerner certains aspects, du fait qu'une partie des activités est secrète. Cela va de soi, étant donné que ce sont des agences de renseignement.

[*Traduction*]

Le président: Merci, monsieur Dubé.

Monsieur Picard, allez-y.

[*Français*]

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

Je trouve cela passionnant. Je vais passer directement à mes questions, parce que je veux laisser plus de temps aux invités pour approfondir le sujet.

D'abord, j'aimerais obtenir quelques précisions. Dans votre...

L'hon. Jean-Pierre Plouffe: Excusez-moi, monsieur Picard, mais je vous entends mal. C'est peut-être une question d'âge, je ne le sais pas.

M. Michel Picard: Je vous confirme que vous ne faites pas vos 75 ans.

Selon votre sixième proposition, le commissaire au renseignement devrait établir un rapport annuel public à l'intention du premier ministre. À cet égard, j'ai un doute et j'aimerais obtenir une précision.

Dans votre rôle actuel, est-ce que le rapport annuel est émis au Parlement ou au premier ministre?

L'hon. Jean-Pierre Plouffe: Actuellement, le commissaire du CST que je suis produit un rapport annuel par l'intermédiaire du ministre de la Défense nationale, lequel, selon la loi, doit le déposer devant les deux Chambres du Parlement dans un délai imparti dans la loi.

Étant donné que, selon le nouveau projet de loi, c'est le premier ministre qui recommande la nomination du commissaire au renseignement, je propose qu'un rapport public soit soumis chaque année et que, de la même façon que le ministre de la Défense nationale le fait actuellement, le premier ministre s'engage, selon la loi, à le déposer devant les deux Chambres. Il faut qu'il y ait un rapport public, selon moi. Or le projet de loi ne mentionne rien à ce sujet.

À quoi sert un rapport public? Premièrement, cela souligne l'indépendance du commissaire. Deuxièmement, c'est une question de confiance du public. Non seulement le public, mais également les parlementaires et les commentateurs veulent savoir ce que fait le commissaire au renseignement.

M. Michel Picard: Puisque vous intervenez, la version remise au premier ministre devra être modifiée en vue qu'on en fasse une distribution publique, en raison de la nature quelquefois très sensible de l'information.

L'hon. Jean-Pierre Plouffe: C'est le commissaire qui fait ce travail. Cela serait fait en amont, un peu comme nous le faisons aujourd'hui. En d'autres termes, nous pourrions produire deux rapports, en théorie: un rapport classifié à l'intention du premier ministre ou du comité de parlementaires, et un rapport public destiné au public en général.

Je pense que cela est essentiel pour assurer la confiance du public et aussi la reddition de comptes.

● (1140)

M. Michel Picard: J'aimerais vous ramener à un autre point au sujet duquel le débat a été assez limité. Votre deuxième proposition concerne la fameuse prolongation d'un an de la période de validité d'une autorisation touchant le renseignement étranger.

Si l'activité a déjà été approuvée par vous au départ et que c'est simplement une question de validation, en quoi est-ce nécessaire de vous demander de nouveau la permission pour une activité qui continue? Avez-vous pris en compte le fait qu'il est probable que les circonstances changent au cours de l'année et que cela pourrait vous faire changer d'idée, peut-être même au point où vous n'auriez pas autorisé la mission au départ si vous aviez su un certain nombre de choses?

L'hon. Jean-Pierre Plouffe: Ma philosophie est la suivante: s'il est nécessaire que le commissaire au renseignement approuve la demande initiale, qui est valide pour une durée d'un an, je ne vois pas pourquoi il ne devrait pas être impliqué un an plus tard lorsqu'on fait une demande de renouvellement de la période de validité.

Pourquoi fait-on une demande de renouvellement un an plus tard? Il faut présumer que des faits nouveaux sont survenus, puisqu'on veut renouveler. À ce moment-là, l'agence en question sera obligée de soumettre une demande écrite au ministre, qui devra déterminer si les motifs invoqués par l'agence sont suffisants pour qu'on autorise la prolongation d'une année.

Je ne comprends pas le raisonnement selon lequel le commissaire est impliqué au départ, mais ne l'est pas lors du renouvellement. Je vais faire une analogie. C'est comme lorsqu'on comparaît devant un juge pour demander l'émission d'un mandat de perquisition. C'est beau, mais un an plus tard, si on veut obtenir une prolongation du mandat, on doit de nouveau se présenter devant le juge et lui soumettre une requête. C'est un peu dans ce style.

M. Michel Picard: Merci.

J'aimerais revenir sur votre première recommandation. C'est une discussion philosophique, mais je n'arrive jamais à me faire une tête quant au principe: on parle de cyberopérations actives, au pire, et de cyberopérations défensives. On est prudent dans le choix des mots en disant qu'on n'attaque pas de façon cybernétique dans des circonstances particulières.

J'avais établi toute une série de questions, mais je vais commencer à l'envers. La première question est peut-être un peu bébête: le fait de mener une cyberopération qui vise un pays étranger constituerait-il un acte de guerre?

L'hon. Jean-Pierre Plouffe: Je ne suis pas expert dans le domaine. Ce sont plutôt les gens du CST qui pourraient répondre à votre question.

Je ne sais pas si M. Galbraith a une réponse à donner.

M. Michel Picard: Sur le plan légal, s'agit-il d'un acte de guerre? À mon avis, il y a toute la question légale.

Peu importe le nombre de lois impliquées, si une organisation qui est par définition une organisation du gouvernement mène une opération à l'étranger, de la même manière que nous sommes victimes d'opérations de l'étranger qui justifient grandement les cyberopérations défensives, est-ce qu'on joue sur le terrain de jeu des actes de guerre?

L'hon. Jean-Pierre Plouffe: Dans un premier temps, de concert avec le CST, le gouvernement détermine que, dans le domaine de la sécurité nationale et internationale, il est essentiel de donner au CST les pouvoirs mentionnés précédemment, soit les pouvoirs défensifs et offensifs.

Selon moi, le mandat est très large et il peut y avoir des répercussions sur la Charte et sur la vie privée des gens. C'est la raison pour laquelle je dis qu'il faut absolument une surveillance quelconque de la part d'un organisme indépendant. Présentement, cet organisme indépendant, c'est le commissaire au renseignement. Je comprends mal qu'on dise que le commissaire au renseignement devrait être exclu de cette surveillance parce que, soi-disant, on ne collecte pas d'informations.

Comme je l'ai mentionné dans mes remarques, et le ministère de la Justice semble être d'accord aussi, il peut y avoir des répercussions sur la Charte et sur la vie privée. Il me semble que, pour cette raison, il serait bon qu'une surveillance quelconque soit faite.

M. Gérard Normand: Monsieur Picard, j'ajouterais que le Parlement se donne les lois qu'il veut bien se donner.

Le projet de loi C-44, qui a clarifié le mandat du SCRS d'agir à l'extérieur, a également donné l'autorité aux juges des cours fédérales d'émettre des autorisations visant des activités à l'étranger. C'est une chose que l'on n'aurait pas vue auparavant, mais qui est maintenant insérée dans la Loi sur le Service canadien du renseignement de sécurité. Ce sont les mêmes raisons qui expliquent la proposition de ces nouveaux pouvoirs du CST. S'ils sont acceptés, ils feront partie du système légal, même si, en cours de route, il faudra se pencher sur des questions liées à la Charte.

● (1145)

[*Traduction*]

Le président: Merci.

[*Français*]

Monsieur Paul-Hus, vous disposez de cinq minutes.

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

Merci, messieurs.

Premièrement, je vous remercie pour le document très complet que vous avez soumis au Comité. Le projet de loi C-59 est effectivement complexe à étudier, et le document que vous nous avez remis contient des éléments très importants.

J'aimerais revenir sur un point, soit le processus d'approbation.

Le problème actuellement, ce sont les cybermenaces. En cyberdéfense, il y a un maximum de ressources qui peuvent être au courant et qui peuvent contrecarrer les cyberattaques. Nous travaillons ensemble là-dessus. Cependant, lorsqu'on parle d'opérations actives, c'est-à-dire lorsque le Canada mène des opérations cybernétiques, je trouve qu'il commence à y avoir beaucoup de niveaux d'intervention, compte tenu de l'aspect secret des renseignements. Si l'on veut mener une opération, c'est qu'on a besoin de collecter des renseignements ou de faire des interventions informatiques dans les systèmes.

Ce matin, j'ai participé à la réunion du Comité permanent de la défense nationale. Nous avons entendu les témoignages de gens qui travaillent aux opérations cybernétiques. Selon eux, sur le plan de la défense, l'important est d'assurer une protection. En cas d'attaques, ils vont surtout se tourner du côté du CST.

Selon le projet de loi C-59, quand on parle de mener des opérations, on demande l'approbation du ministre des Affaires étrangères. De votre côté, vous demandez aussi d'avoir une supervision de la part du commissaire au renseignement.

Ne trouvez-vous pas qu'il y a trop d'intervenants lorsqu'il s'agit d'opérations secrètes?

L'hon. Jean-Pierre Plouffe: C'est difficile pour moi de répondre à la question, puisque je ne connais pas exactement tout ce que cela implique sur le plan opérationnel.

Toutefois, selon ce que j'en sais, comme le CST cible les entités étrangères, j'imagine qu'on a pensé, en ce qui a trait aux opérations actives et passives en matière de cybersécurité, qu'il faudrait également impliquer le ministre des Affaires étrangères. Parce que c'est quelque chose qui se passe à l'étranger, on pense que le ministre devrait consentir à ces opérations ou en être le demandeur. Je n'y vois pas de problème. Toutefois, comme je l'ai dit tantôt, j'ai un problème lorsqu'on dit que le commissaire au renseignement ne devrait pas être impliqué pour réviser le tout, que ce soit sur le plan de la Charte ou sur le plan de la protection de la vie privée.

M. Pierre Paul-Hus: Aux fins de renseignement du Comité, pouvez-vous donner deux exemples d'opérations que le Canada pourrait demander à mener à l'étranger? Pourrait-il s'agir, par exemple, d'une collecte de renseignements de télécommunications dans des circonstances particulières? J'aimerais avoir des exemples. Actuellement, le débat est théorique, et personne ne s'avance à dire quelles opérations actives le Canada aurait besoin de faire.

Avez-vous des exemples à nous donner?

M. Gérard Normand: Dans le projet de loi actuel, l'article 27 proposé prévoit la collecte de renseignements étrangers. Quant à l'article 28 proposé, il concerne la cybersécurité. Pour sa part, l'article 31 proposé concerne les mesures actives, comme vous l'avez dit plus tôt. Les mesures actives, telles qu'elles sont définies dans la loi, ne sont pas là pour que l'on procède à la collecte d'information. Nous ne sommes pas là pour faire rien d'autre qu'interférer avec le système.

Les exemples sont variés. Il pourrait y en avoir à des fins militaires. À ce moment, le CST serait l'outil dont se serviraient les militaires pour atteindre leur but, ce qui est correct. Le CST pourrait également prêter assistance à d'autres agences.

Ce qu'indique l'article 31 proposé, c'est que le CST pourrait mener des activités où il interférerait avec des communications, par exemple à des fins de relations internationales. Cela tombe en dehors du cadre d'autres pays où les buts sont la sécurité et la défense. Le terme « affaires internationales » peut vouloir dire beaucoup de choses.

Il faut tenir compte du fait que le commissaire va être impliqué dans des décisions similaires. Selon l'article 27 proposé, sur le plan de la collecte d'information, le même genre d'activités pourra être mené, et il va y avoir un rôle de révision. Nous ne comprenons vraiment pas la raison pour laquelle le commissaire serait exclu quand vient le temps des opérations actives. Comme vous le dites, c'est quelque chose de nouveau.

M. Pierre Paul-Hus: Comme il ne me reste qu'une minute, je terminerai mon intervention en soulignant, à l'intention des membres du Comité, la proposition n^{o} 7. C'est une proposition importante qui concerne la Loi sur la défense nationale. Cette loi mentionne que « la valeur des renseignements étrangers que l'on espère obtenir grâce à l'interception justifie l'interception envisagée ». Par contre, cette disposition ne se retrouve pas dans le projet de loi C-59. Il s'agit donc d'une bonne recommandation et je vous en remercie.

● (1150)

[*Traduction*]

Le président: Je vous remercie.

[*Français*]

Madame Damoff, vous avez la parole pour cinq minutes.

[*Traduction*]

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

Je vous remercie tous d'être avec nous aujourd'hui. Les échanges ont été fort éclairants, et nous vous remercions des recommandations que vous nous avez soumises.

Vous n'êtes pas sans savoir que le mandat actuel du CST consiste à obtenir et utiliser des renseignements tirés de l'infrastructure mondiale de l'information. Dans l'infrastructure existante, il n'y a vraiment pas d'indications claires quant à la possibilité de recueillir les renseignements d'un citoyen ou d'un résident canadien.

Selon vous, serait-il avantageux de recommander que le projet de loi C-59 soit modifié de façon à exiger une autorisation ministérielle lorsque le CST obtient des renseignements au moyen de l'infrastructure mondiale de l'information, alors qu'un citoyen ou un résident canadien a des attentes raisonnables en matière de vie privée?

L'hon. Jean-Pierre Plouffe: Pourriez-vous résumer votre question? Veuillez m'excuser, mais je n'ai pas compris exactement ce que…

Mme Pam Damoff: Un Canadien ou un résident canadien a des attentes quant à la protection de ses renseignements personnels, mais il n'est pas véritablement protégé. Croyez-vous qu'il serait préférable d'exiger une autorisation ministérielle lorsque vous recueillez ce genre de renseignements?

L'hon. Jean-Pierre Plouffe: Parlez-vous du CST?

Mme Pam Damoff: Oui.

L'hon. Jean-Pierre Plouffe: Et bien, conformément à son mandat actuel, de même qu'à celui qui est prévu au projet de loi C-59, le CST ne peut cibler ni les Canadiens ni les personnes au Canada. Il ne peut pas le faire. Il peut seulement viser des personnes ou des entités à l'étranger.

Mme Pam Damoff: Si je suis en vacances en Écosse…

L'hon. Jean-Pierre Plouffe: Et bien, vous serez à l'étranger.

Mme Pam Damoff: Estimez-vous qu'une autorisation doive être requise pour les Canadiens dans une telle situation?

L'hon. Jean-Pierre Plouffe: À vrai dire, le CST ne peut pas cibler les Canadiens

Allez-y, William.

M. J. William Galbraith (directeur exécutif, Bureau du commissaire du Centre de la sécurité des télécommunications): Si vous êtes en vacances en Écosse, le CST pourrait intercepter une communication à laquelle vous participez seulement s'il cible une entité à l'étranger. Toutes les autres mesures de protection de la vie privée applicables seraient en place, et c'est ce que le commissaire vérifierait.

Pour une telle question, vous feriez peut-être mieux de demander des précisions au CST lui-même.

Mme Pam Damoff: Bien.

L'hon. Jean-Pierre Plouffe: Autrement dit, dans cet exemple, la conversation ne serait interceptée qu'incidemment, peut-être parce que vous discutez avec une autre personne ou entité à l'étranger, et que le CST souhaite cibler cette autre entité, mais pas vous. Si vous vous trouvez là par hasard, c'est ce que nous appelons acquérir « incidemment ». Lorsqu'il cible des entités étrangères, le CST pourrait intercepter incidemment des communications privées de Canadiens. C'est pourquoi il faut l'autorisation du ministre pour le faire, voyez-vous? La cible première n'est pas les Canadiens, mais bien l'entité étrangère.

Mme Pam Damoff: D'accord. Voilà qui m'amène à ma question suivante.

L'information accessible au public fait partie des renseignements que vous pouvez recueillir, et je doute que les Canadiens comprennent très bien la quantité de renseignements personnels que nous divulguons publiquement.

Lorsque que je me branche à une application qui demande d'utiliser Facebook, pouvez-vous acheter ces renseignements, comme mes photos Facebook ou les informations que j'ai partagées sans me rendre compte qu'elles étaient privées?

L'hon. Jean-Pierre Plouffe: M. Normand va vous répondre.

M. Gérard Normand: Pour le moment, la définition englobe les renseignements que vous pouvez acheter. Certains ont fait valoir qu'ils ne devraient pas être compris. Par exemple, notre Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE, ne considère pas que ce genre de renseignement fait partie de l'information accessible au public. Encore une fois, il incombe essentiellement au gouvernement de décider ce qu'il souhaite y inclure.

Je dirais aussi que si vous examinez la définition de la proposition de Loi sur le SCRS, vous constaterez que c'est encore plus vague puisque la disposition renvoie à un article, de sorte que c'est circulaire. Le texte ne définit pas du tout le concept. D'ailleurs, je pense que votre comité devrait s'assurer que la définition choisie s'applique aux deux lois.

● (1155)

Le président: Merci, madame Damoff.

Monsieur Motz, allez-y pour la dernière intervention de cinq minutes. Merci.

M. Glen Motz: Merci, monsieur le président.

Je vous remercie encore de vos remarques.

Monsieur le commissaire, j'aimerais vous poser une question à propos de votre troisième recommandation. Je vous suis reconnaissant de votre désir de participer aux approbations. Vous devez intervenir dans bon nombre d'entre elles pour faire votre travail efficacement.

Vous parlez des autorisations en cas d'urgence délivrées par le ministre et, si j'ai bien compris, vous dites que vous devriez aussi les examiner dès leur obtention, c'est-à-dire avant qu'elles ne soient exécutées. Si c'est exact, une telle procédure n'ajouterait-elle pas un délai ou un obstacle supplémentaire en cas d'urgence, ce qui pourrait empêcher l'organisme chargé de la sécurité de faire son travail et peut-être même d'écarter une menace imminente?

M. Gérard Normand: La disposition que nous visons ne viendrait pas suspendre l'exécution de l'autorisation en attendant que le commissaire au renseignement ait examiné le dossier. On y donnerait suite immédiatement, puis l'examen a posteriori aurait pour but de confirmer que la décision était bel et bien raisonnable. L'examen doit être fait dans les cinq jours; si le commissaire trouve la situation déraisonnable après deux ou trois jours, il devra interrompre le processus, mais il ne l'empêchera pas de commencer.

L'hon. Jean-Pierre Plouffe: En fait, la procédure ressemble à celle du Royaume-Uni. Autrement dit, l'opération suit son cours pour un maximum de cinq jours, mais, dans ce cas précis, le commissaire au renseignement pourrait intervenir après deux ou trois jours. Il pourrait décider que c'est dommage, mais que ce qui a été fait au cours des deux ou trois derniers jours est déraisonnable et doit s'arrêter. C'est l'essence même du processus, d'une certaine façon.

M. Glen Motz: Je vois. Si je comprends bien, vous dites que l'autorisation sera tout de même exécutée en cas de menace imminente. L'examen permettra toutefois de rectifier le tir la prochaine fois.

L'hon. Jean-Pierre Plouffe: C'est exact.

M. Glen Motz: Bien. Merci.

Lorsque vous tenez compte de vos ressources et de ce que le projet de loi C-59 propose, avez-vous confiance en vos capacités? Avez-vous suffisamment de ressources pour surveiller tous ceux qui sont considérés comme une menace? Sinon, vos ressources vous permettent-elles seulement de vous attaquer aux menaces les plus graves?

M. J. William Galbraith: Pour ce qui est de savoir si nous avons suffisamment de ressources, les dispositions transitoires du projet de loi sont bien claires. Tout ce que nous avons — le commissaire, les employés et les crédits du Parlement — passera au commissaire au renseignement et à son bureau.

Quelles sont les exigences? Il faut avoir une connaissance profonde des activités du CST et de celles du SCRS. Nous connaissons manifestement le CST grâce au travail que nous effectuons actuellement dans l'examen de ses activités, mais, aussi, nous comptons désormais des employés ayant une expérience et des connaissances du SCRS. Nous avons eu l'occasion d'embaucher du personnel au cours de la dernière année, du moins depuis le mois de juin, et nous avons sélectionné des candidats qui avaient des connaissances et une expérience des activités du SCRS. Nous avons également engagé un conseiller juridique spécial, qui est avec nous aujourd'hui, pour nous y retrouver dans la complexité du projet de loi C-59.

Pour ce qui est de savoir si le personnel répondra aux besoins à l'avenir, nous ne connaissons toujours pas le nombre d'autorisations qui seront exigées par le SCRS ou le CST. Ce n'est qu'une fois le projet de loi adopté et les activités en route que nous aurons une idée du volume d'autorisations, mais les décideurs ont manifestement estimé que nous avions un fondement raisonnable. Les auteurs du libellé et le gouvernement ont dû juger que nos ressources étaient au moins un bon début pour effectuer la transition vers la nouvelle organisation.

● (1200)

M. Glen Motz: Au sujet de la transition, comprenez-vous bien l'incidence du nouveau comité parlementaire, son rôle dans le milieu du renseignement, du SCRS et des opérations connexes, ainsi que la façon dont les choses vont se dérouler? En êtes-vous satisfaits?

Le président: Veuillez répondre très brièvement.

M. J. William Galbraith: Nous étudions tous les aspects du comité parlementaire et surveillons sa création. Nous rencontrons des représentants du SCRS et du CST pour savoir comment les organisations se préparent et, dans la mesure du possible, nous nous tenons au courant de leur travail relatif aux nouveaux pouvoirs.

Le président: Merci, monsieur Motz.

Voilà qui met fin à la première heure de notre séance. Au nom des membres du Comité, je tiens à vous remercier de votre collaboration. Comme vous pouvez le constater, le temps joue contre nous, et la plupart des points que vous avez soulevés doivent assurément faire l'objet d'une réflexion approfondie de la part du Comité. Je vous remercie encore de votre contribution à notre étude.

Nous allons maintenant suspendre la séance un instant, après quoi nous reprendrons aussi vite que possible.

● (1200)

(Pause)

● (1200)

Le président: Reprenons. Bienvenue à la deuxième partie de notre séance.

Nous sommes en présence de Raymond Boisvert, qui représente le ministère de la Sécurité communautaire et des Services correctionnels de l'Ontario, ainsi que Micheal Vonn, qui représente l'Association des libertés civiles de la Colombie-Britannique.

J'ignore qui souhaite commencer, mais allez-y dès maintenant. Vous avez 10 minutes.

● (1205)

Mme Micheal Vonn (directrice de la politique, Association des libertés civiles de la Colombie-Britannique): Je serai heureuse de commencer. Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie de cette invitation.

Mon allocution écrite porte sur la collecte de données en vrac du CST et du SCRS.

Dans son témoignage devant votre comité, M. Craig Forcese a soulevé un point très important au sujet des seuils d'autorisation pour la collecte de données du CST.

L'article 23 proposé de ce qui sera la nouvelle Loi sur le CST précise que les activités réalisées par le CST dans le cadre de ses divers mandats ne doivent pas viser des Canadiens ou des personnes au Canada. Cela s'inscrit bien sûr dans la continuité de la situation actuelle, c'est-à-dire que le CST est tenu de ne pas orienter ses activités en ce sens.

Pourtant, il est bien connu et admis que l'information des Canadiens et des personnes au Canada est recueillie, parce que la collecte de certaines données, qui n'est absolument pas négligeable, est inévitable en raison de la complexité des réseaux de communication. Par conséquent, les données des Canadiens sont recueillies incidemment ou inévitablement.

Dans le cadre du nouveau régime proposé afin de protéger les intérêts personnels des Canadiens, on exige que le CST demande une autorisation ministérielle qui sera ensuite approuvée par le commissaire au renseignement. Ce processus d'autorisation et d'approbation du commissaire au renseignement se mettrait en branle lorsque les activités du CST contreviendraient à une loi du Parlement.

Nous sommes d'accord avec M. Forcese pour dire que ce facteur déclenchant a une portée trop limitative, un point de vue qui est maintenant repris par le *Citizen Lab*, la Clinique d'intérêt public et de politique d'Internet du Canada et d'autres.

Comme M. Forcese le souligne, certains craignent que le seuil proposé ne garantisse pas, par exemple, que le processus d'autorisation soit lancé pour des activités qui recueillent incidemment les métadonnées des Canadiens, ce qui est évidemment d'une importance cruciale.

Craig Forcese propose d'élargir la portée de l'élément déclencheur, de façon à ce que le processus d'autorisation s'applique aux activités qui contreviendraient à toute autre loi du Parlement, ou qui pourraient « entraîner la collecte d'informations pour lesquelles les Canadiens ou une personne au Canada peut s'attendre raisonnablement à ce qu'elles soient protégées », un seuil qui a déjà été mentionné.

Voici ce que nous reprochons simplement à cet ajout proposé: que les données exactes pour lesquelles on « peut s'attendre raisonnablement à ce qu'elles soient protégées » deviennent au coeur de presque tout enjeu relatif à la vie privée, et que ce seuil soit établi au sein du CST.

Grâce aux années de rapports du commissaire du CST, entre autres, nous savons que les litiges relatifs à l'interprétation des normes et des définitions juridiques ont toujours été une source de préoccupation, et que les activités liées à la sécurité nationale en général sont ravagées par le problème des « lois secrètes », où le libellé d'une loi ou d'une directive est interprété d'une façon parfois obscure ou très troublante, des interprétations qui peuvent ne pas être mises au jour avant des années. Nous sommes donc d'avis qu'un élément déclencheur qui comporte une définition spécieuse est fondamentalement problématique.

Cependant, le dernier rapport du commissaire du CST indiquait que le CST a obtenu seulement trois autorisations ministérielles depuis 2015 pour mener ses activités de renseignement électromagnétique. Il semble que ces autorisations permettent un large éventail d'activités. Nous croyons savoir que, compte tenu de la fréquence et de la portée de l'information acquise incidemment, la plupart, voire la totalité des autorisations, sont susceptibles d'au moins mettre en cause des données de Canadiens. Autrement dit, il y a un petit nombre d'autorisations seulement, et presque toutes sont susceptibles de nécessiter le régime d'autorisation et l'approbation du commissaire aux renseignements.

Pour veiller à ce que le processus d'autorisation tienne compte de tout ce que nous espérons, il est sans doute préférable, et encore tout à fait possible et efficace, d'avoir une approbation uniforme du processus d'autorisation par le commissaire au renseignement qui s'appliquerait à toutes les activités en dehors du mandat de soutien technique et opérationnel, qui est son domaine d'activité, comme vous le savez.

● (1210)

Pour tout le reste, nous recommandons que la question du seuil soit résolue en éliminant la nécessité d'établir un seuil et en veillant à ce que chaque catégorie d'activités autorisées soit assujettie à la nouvelle procédure de reddition de comptes d'autorisation et d'approbation ministérielle par le commissaire au renseignement.

J'aimerais maintenant parler de la collecte de données de masse effectuée par le SCRS. À la suite de la consultation sur la sécurité nationale, nous étions certainement préoccupés à l'idée qu'en réponse aux scandales liés aux données de masse du SCRS, le gouvernement se contenterait d'accorder à l'organisme le pouvoir de faire ce qu'il faisait auparavant de façon illégale sans tenir un débat démocratique pertinent sur l'acquisition des données de masse dans le contexte de la sécurité nationale. Nous reconnaissons certainement que l'attribution d'un fondement législatif à la collecte de données de masse permettra d'améliorer la transparence, mais le seuil peu élevé proposé dans le projet de loi C-59 nous préoccupe énormément et bien honnêtement, nous craignons que cet enjeu extrêmement important ne reçoive pas suffisamment d'attention dans le contexte d'un projet de loi omnibus.

C'est seulement récemment que le CSARS a mené son tout premier audit des programmes de collecte de données de masse du SCRS. Selon le CSARS, la collecte de données de masse effectuée par le SCRS peut être appropriée lorsqu'elle répond à la norme de stricte nécessité pour la collecte de données établie dans l'article 12 de la Loi sur le SCRS. À notre avis, il est difficile d'imaginer un organisme qui serait mieux placé pour évaluer cela, à la fois du point de vue de la reddition de comptes et du respect de la primauté du droit et du point de vue des besoins opérationnels du SCRS.

La proposition du SCRS sur les normes et les critères visant la collecte de données de masse comporte trois volets. Tout d'abord, il faut clairement établir le lien avec une menace à la sécurité du Canada, deuxièmement, aucun moyen moins intrusif ne doit être accessible et enfin, il faut mener une évaluation objective de la valeur des renseignements visés.

Maintenant, veuillez comparer ces critères aux critères établis dans le projet de loi C-59. En effet, le projet de loi C-59 permet au SCRS de recueillir des ensembles de données accessibles au public, sans définir ce terme, sur le fondement de la norme de pertinence. Le critère auquel il faut satisfaire pour acquérir des ensembles de données canadiens — qui, il ne faut pas l'oublier, sont définis expressément comme étant des ensembles de données qui contiennent des renseignements personnels qui ne sont pas directement et immédiatement liés à des activités représentant une menace à la sécurité du Canada — consiste simplement à démontrer que les résultats produits par leur recherche ou leur exploitation pourraient être pertinents et il faut que cette évaluation soit raisonnable.

On pourrait faire valoir que la vaste portée dont profite la collecte des données de masse est au moins limitée par l'exigence d'une autorisation judiciaire visant la conservation de ces ensembles de données, mais plutôt que d'offrir une protection efficace, cette autorisation intensifie simplement les effets des critères très peu élevés qui l'ont engendrée. Les renseignements personnels qui ne sont pas directement et immédiatement liés à des menaces à la sécurité du Canada peuvent être recueillis s'ils « peuvent être pertinents », si cette évaluation est « raisonnable », et si le ou la juge décide ensuite que les ensembles de données peuvent être conservés parce qu'ils répondent au critère selon lequel « ils sont susceptibles d'être utiles ».

Ce sont donc les seuils de ce que la plupart des Canadiens qualifieraient de surveillance de masse, et nous croyons que la plupart des Canadiens rejetteraient ces seuils, car ils sont beaucoup trop bas. Ainsi, une bonne occasion d'améliorer ces pratiques de surveillance est gaspillée dans le projet de loi C-59.

Les critères proposés représentent une érosion importante des protections de la vie privée qui découlent du critère de stricte nécessité qui s'applique actuellement. Nous recommandons que les dispositions sur les données de masse du SCRS soient révisées pour qu'elles soient expressément visées par le critère de stricte nécessité au lieu de représenter une exception à ce critère. Nous recommandons également que des critères de collecte de données de masse — comme ceux établis par le CSARS, qui sont pragmatiques et dotés de principes — soient établis dans le projet de loi.

C'est ce qui termine mon exposé. Merci.

Le président: Merci, madame Vonn.

Allez-y, monsieur Boisvert.

M. Raymond Boisvert (sous-ministre associé, Bureau du conseiller de la sécurité provinciale, ministère de la Sécurité communautaire et des Services correctionnels de l'Ontario): Merci beaucoup, monsieur le président. J'aimerais également vous remercier de me donner l'occasion de comparaître devant le Comité aujourd'hui.

Comme vous le savez, je suis conseiller de la sécurité provinciale de l'Ontario depuis janvier 2017. Avant cela, pendant presque cinq ans, j'ai été consultant auprès d'organismes privés et publics dans le domaine des risques liés à la sécurité nationale, notamment les cybermenaces. Et auparavant, j'ai travaillé au Service canadien du renseignement de sécurité, ou SCRS. Lorsque j'ai quitté cet organisme en 2012, j'occupais le poste de directeur adjoint.

Étant donné que j'ai commencé à travailler au SCRS au moment de sa création, en 1984, j'ai assisté à un très grand nombre de jalons qui ont façonné le milieu du renseignement de sécurité au Canada, plus précisément en ce qui concerne les organismes au centre des interventions en cas de menace au Canada.

Nous sommes à nouveau sur le point de vivre un changement — et il s'agit manifestement d'un changement important. En effet, même si en général, on considère que la Loi sur le SCRS représente un modèle de loi efficace en matière de sécurité et de renseignements, il a fallu lui apporter des rajustements de temps à autre, peut-être pas pour remédier à des défaillances particulières, mais plutôt parce qu'il était nécessaire de l'adapter aux changements sociaux, culturels et politiques et, maintenant plus que jamais, aux changements techniques.

Parmi tous les éléments importants dans le projet de loi C-59, il est temps d'envisager d'apporter des changements essentiels à un organisme pour lequel je n'ai pas travaillé, mais avec lequel j'ai maintenu une connectivité opérationnelle importante pendant de nombreuses années. En effet, il est temps que le CST ait sa propre loi habilitante, car son mandat a maintenant 16 ans.

L'élément le plus important de cette transformation de la mission et du mandat concerne le domaine des cybermenaces. Le Canada doit maintenant se joindre à la communauté des nations aux vues similaires qui sont déterminées à résister à la menace croissante de l'entreprise criminelle mondialisée, au vol de propriété intellectuelle ou à l'interférence dans notre société menée par d'autres nations, et au potentiel de destruction catastrophique des infrastructures essentielles, que ce soit à cause d'une guerre de la cinquième dimension ou d'attaques terroristes. Nous devons appuyer nos alliés et entretenir des liens et la paix avec eux, de l'Australie à l'Union européenne. Ils ont eux-mêmes reconnu la nature de ce nouveau contexte de menace du XXI^{e} siècle.

Les nations qui n'appuient pas ces valeurs ou qui n'y croient pas ont certainement découvert les avantages de la guerre hybride ou de la guerre de la cinquième dimension. Elles ciblent très activement nos infrastructures essentielles et notre future prospérité en volant la meilleure et la plus importante propriété intellectuelle que le pays peut offrir. Elles ont également remarqué qu'il était très facile de nuire à nos processus démocratiques en minant la confiance des gens à l'égard de nos institutions, ainsi que notre capacité de mener un dialogue respectueux et constructif, et que cela produisait des avantages immédiats.

Il y a plusieurs domaines à explorer au cours de la discussion d'aujourd'hui, mais tout d'abord, permettez-moi de dire que je fais depuis longtemps la promotion du renforcement de la reddition de comptes visant la communauté du renseignement de sécurité. La création du Comité des parlementaires sur la sécurité nationale et le renseignement et de l'Office de surveillance des activités en matière de sécurité nationale et de renseignements répondra à la majorité de mes préoccupations liées à la nécessité d'améliorer la reddition de comptes et la transparence dans le milieu de la sécurité.

Toutefois, dans le cadre de mon exposé, permettez-moi maintenant de parler plus directement de certains éléments liés à la menace et de la nécessité de répondre efficacement à cette réalité.

Nous vivons dans une époque sans précédent. En effet, au cours de ma carrière, qui s'étend sur un peu plus de trois décennies, je n'ai jamais observé un tel ensemble de défis locaux et mondiaux, qu'il s'agisse du changement climatique et de la sécurité alimentaire ou de la migration irrégulière et du nombre sans précédent de réfugiés, en passant par les soulèvements sociaux et politiques, les menaces nucléaires et les changements dans l'hégémonie mondiale. Des auteurs de menaces situés partout dans le monde ciblent maintenant le Canada avec facilité. De plus, les Canadiens qui ont l'intention de causer du tort à d'autres ou de cibler des intérêts canadiens à l'étranger peuvent maintenant opérer à partir de régions éloignées du monde, et n'ont pas à se limiter aux zones de conflits habituelles.

Dans cet aspect du renseignement de sécurité équivalant à la mondialisation, il est extrêmement important que le CST continue d'appuyer le SCRS, le ministère de la Défense nationale et les organismes d'application de la loi dans les enquêtes légales ou les exigences de missions, peu importe où des menaces émergent dans le monde. Qu'il faille aider le SCRS à recueillir des renseignements sur un réseau violent extrémiste émergent qui cible les voyageurs canadiens ou les diplomates à l'étranger, aider les Forces canadiennes à protéger une unité déployée qui donne de la formation ou peut-être même aider la GRC à amener des trafiquants de personnes devant les tribunaux, nous devons offrir les meilleurs outils disponibles. Les capacités ou les outils dont je parle peuvent seulement être obtenus auprès de nos organismes de renseignement d'origine électromagnétique.

● (1215)

Il est tout aussi important — et à mon avis, essentiel — que le Canada compte sur les capacités qu'il contrôle et qu'il peut vérifier plutôt que sur les efforts ou les compétences d'autres nations qui ne partagent peut-être pas toutes nos normes et nos intentions.

En ce qui concerne la partie 3 du projet de loi, plus précisément la partie sur la cybersécurité et l'assurance de l'information, permettez-moi de vous dire qu'à titre de conseiller de la sécurité provinciale de l'Ontario, ce volet me préoccupe grandement, car il concerne la cybermenace qui cible nos investissements substantiels dans les infrastructures essentielles.

Au-delà de la protection de la propriété intellectuelle acquise directement ou indirectement, si l'on souhaite assurer notre prospérité actuelle et future, il est nécessaire de protéger nos infrastructures essentielles à la survie, qu'elles soient publiques ou privées. Ainsi, la capacité renforcée du CST de nous aider à protéger notre infrastructure vitale est essentielle pour les Ontariens et, je crois, pour tous les Canadiens.

Je crois que c'est vrai, car nous vivons actuellement dans un environnement dangereux où plus de 400 nouvelles menaces informatiques sont produites chaque minute et où une personne est attaquée par un rançongiciel quelque part dans le monde toutes les 10 secondes. Plus près de nous, chaque mois, l'équipe des opérations de cybersécurité du gouvernement de l'Ontario gère approximativement 40 milliards d'incidents liés à la sécurité. Oui, des milliards d'incidents chaque mois. Même si nous respectons les normes de l'industrie, plus de 90 % des courriels que reçoit la fonction publique de l'Ontario sont bloqués en raison de réseaux de zombies ou de menaces de pourriels.

Sur le plan des opérations de cyberdéfense, je crois que seul le CST peut fournir la technologie, le savoir-faire et les données liés aux menaces nécessaires pour bâtir la résilience en matière de cybersécurité efficace qui est nécessaire dans ce type d'environnement. En raison des conversations que j'ai eues avec les intervenants de l'industrie privée et avec ceux de grands organismes gouvernementaux indépendants, par exemple les organismes qui s'occupent de l'énergie, des soins de santé, de l'éducation et du transport, je sais qu'ils ressentent tous les effets des cybermenaces omniprésentes. Essentiellement, nous ne pouvons plus agir seuls — et eux non plus. Nous sommes en présence d'un phénomène de menace mondiale qui exige une stratégie et des capacités de niveau national.

En ce qui concerne les cyberopérations actives, permettez-moi simplement de dire que la meilleure défense commence toujours par une bonne offensive. Lorsqu'on signale que plus de cinq douzaines de pays renforcent activement leurs capacités cyberopérationnelles, à mon avis, nous devons élaborer des mesures offensives en matière de cybersécurité pour répondre à ces menaces, et parfois, cela signifie qu'il faut aller au-delà de nos frontières.

Des tactiques offensives cybernétiques ont été mises au point et sont appliquées par les meilleures entreprises de sécurité privées dans le monde. Depuis un certain temps, il est courant d'avoir recours au Web invisible ou au Darknet pour recueillir des renseignements avant une attaque et pour protéger les systèmes, par exemple ceux du secteur financier. Je le sais, car j'ai travaillé directement dans ce secteur. Lorsqu'il sera temps de faire face à une attaque ciblée qui vise à manipuler les systèmes d'exploitation d'une centrale énergétique en vue de causer une défaillance ou peut-être même de détruire quelque chose, comme nous l'avons vu en Ukraine, en Allemagne et même dans l'État de New York, nous aurons besoin du CST afin de « réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités » de ces menaces ou de leurs responsables.

Plus communément, pour vous donner un autre exemple, la fréquence et les exploits des soi-disant attaques par déni de service ou incidents de DDOS s'intensifient. Je prévois que le CST devra bientôt aider un fournisseur de service canadien ou un gouvernement infranational à contrer une attaque par déni de service.

Depuis l'arrivée de l'Internet des objets, nous avons déjà assisté à la création de réseaux de zombies à partir d'appareils intelligents qui ont été utilisés pour lancer des attaques d'un téraoctet par seconde contre des institutions habituellement associées au partage de l'information, contre des installations anti-pourriels, des réseaux sociaux, des travailleurs des droits de la personne et des médias grand public. Il ne fait aucun doute que la situation ne fera qu'empirer, surtout lorsque nous faisons face à des régimes autocratiques qui n'ont aucune inhibition ailleurs dans le monde.

Mon rôle actuel de conseiller de la sécurité provinciale représente un exemple important de la façon dont le monde a changé et de la nécessité, pour le Canada, de modifier la façon dont il se perçoit et dont il fonctionne. L'Ontario ne représente que l'une des 14 compétences principales du pays. À elle seule, l'économie de l'Ontario se situerait au 18e rang dans le contexte du G20. Il ne fait aucun doute que, comme l'Ontario, toutes les compétences infranationales sont conscientes des multiples menaces qui continuent d'avoir des répercussions négatives sur la prospérité et la sécurité.

À mon avis, une initiative de sécurité établie par voie législative qui concilie les exigences en matière de sécurité avec les exigences en matière de reddition de comptes, de transparence et de respect des droits des Canadiens permettra à notre nation de tirer son épingle du jeu dans un monde de plus en plus tumultueux.

Merci.

● (1220)

Le président: Merci, monsieur Boisvert.

Nous passons maintenant aux questions.

Madame Damoff, vous avez sept minutes. Allez-y.

Mme Pam Damoff: Merci, monsieur le président.

J'aimerais remercier les deux témoins d'être ici aujourd'hui.

Madame Vonn, je suis heureuse de vous revoir. Ma première question s'adresse à vous. Je crois que vous étiez présente lorsque j'ai posé une question aux représentants du CST. J'aimerais savoir si vous pouvez répondre à la question que je leur ai posée. Si les renseignements d'un Canadien ou d'une personne qui réside au Canada et qui se trouve à l'étranger sont visés par les activités du CST, et que cette personne a des attentes raisonnables liées à la protection de la vie privée, à votre avis, une autorisation ministérielle devrait-elle être exigée?

● (1225)

Mme Micheal Vonn: C'est essentiellement ce que nous proposons, c'est-à-dire qu'il faut trouver une façon de mettre en oeuvre le mécanisme de reddition de comptes qui est proposé pour la collecte de tous les renseignements des Canadiens, que ces renseignements fassent l'objet ou non d'une attente raisonnable liée à la protection de la vie privée. Comment réussira-t-on à obtenir cet arbitrage à moins d'avoir un mécanisme en place? Cela devient un argument circulaire, car selon ce que nous comprenons, ce qui est fréquemment recueilli, ce sont des métadonnées, lorsqu'il ne s'agit pas d'une interception directe. À notre avis, c'est certainement l'un des enjeux essentiels pour maintenir la confiance des Canadiens à l'égard des propositions. Il sera toujours préférable qu'une autorisation soit soumise à une reddition de comptes plus élevée que moins élevée.

Mme Pam Damoff: À votre avis, les Canadiens se font-ils une idée fausse de la situation? Pensent-ils aux gens qui envoient peut-être des courriels et qui font des appels à l'étranger, par exemple un terroriste qui parle à un Canadien qui participe à un complot comparativement à... Je sais qu'avant de faire partie de ce comité, je n'avais jamais vraiment compris à quel point ces métadonnées avaient une portée universelle. Pensez-vous que les Canadiens comprennent comment ils peuvent se retrouver dans cette situation parce qu'ils vont sur Facebook ou Instagram ou Twitter ou une plateforme de ce type où l'on recueille des renseignements que les Canadiens pensent confidentiels, mais qui ne le sont pas?

Mme Micheal Vonn: Les Canadiens réalisent certainement de plus en plus que ce qui représente une collecte fortuite — encore une fois, en raison de la nature des réseaux de communications — pourrait certainement les toucher. Je dirais qu'on est de plus en plus conscient de cela au Canada, et qu'il y a un problème lorsque nous entendons sans cesse... Il est juste de dire que le CST ne cible pas, mais le déroulement des opérations fait certainement souvent intervenir les données des Canadiens. Ce n'est pas une collecte sans importance, encore une fois, et les Canadiens commencent à s'en rendre compte, et ils souhaitent donc qu'on mette en oeuvre des mécanismes suffisamment robustes pour offrir le type de mesures qui pourraient les protéger.

Mme Pam Damoff: Même si je suis d'accord avec vous, je crois que si un plus grand nombre de Canadiens comprenait ce qu'on recueille, ils seraient plus nombreux à en parler.

Cela m'amène à parler de la collecte de données. Je sais que vous avez déjà parlé de la collecte de données et de la période de temps pendant laquelle ces données devraient être conservées, ainsi que de la question de savoir si on devrait mettre en oeuvre des mécanismes de destruction des données recueillies. Croyez-vous qu'on devrait amender le projet de loi pour ajouter un critère de nécessité pour la conservation des renseignements personnels, ainsi qu'une obligation de destruction visant les renseignements personnels qui ne satisfont pas au critère de nécessité? Cela aiderait-il à accroître la transparence et à protéger la vie privée des gens?

Mme Micheal Vonn: Est-ce une question directement liée au CST...?

Mme Pam Damoff: Elle vise le projet de loi dans son ensemble, car c'est le CST qui recueille les données, n'est-ce pas?

Mme Micheal Vonn: C'est juste. Il y a toute une série d'aspects de la collecte de données qui y sont mentionnés. Je pense qu'il serait clairement bénéfique, pour la protection de la vie privée des Canadiens, d'y ajouter des critères de nécessité, selon le type de collecte. Est-ce qu'ils devraient être les mêmes pour toutes les formes de collecte de données? Nous serions portés à croire que les critères pourraient varier selon le contexte, mais qu'ils auraient tout à fait leur place.

Cela dit, votre question sur la conservation est très intéressante, elle nous ramène à la multiplicité des autorisations accordées et à la faiblesse des exigences qui les entourent. C'est ce que nous voulons dire quand nous affirmons que cela vient s'ajouter à l'erreur de départ quand le seuil n'est pas assez élevé et qu'on détermine qu'on peut conserver telle donnée parce qu'elle « pourrait être utile ». Cela vient aggraver le problème, plutôt que de le régler, et c'est la base de notre argumentaire concernant la conservation.

Mme Pam Damoff: Merci.

J'aimerais aussi vous parler des rapports. Je me demande si vous considérez pertinent d'obliger le commissaire au renseignement à produire un rapport annuel sur ses activités et les organismes qu'il surveille et si vous estimeriez bénéfique que le SCRS publie un rapport annuel.

● (1230)

Mme Micheal Vonn: Tout à fait, puisque nous trouvons les rapports annuels produits par le SCRS et le commissaire du CST, par exemple, extrêmement utiles. Si nous devions faire une recommandation, nous pencherions clairement plus pour trop de rapports plutôt que pas assez pour assurer l'imputabilité et maintenir la confiance.

Mme Pam Damoff: Merci.

Il me reste environ une minute, et monsieur Boisvert, je ne voudrais pas vous laisser de côté, donc je vous poserai une question assez brève.

D'après les témoignages que nous avons entendus un peu plus tôt sur le projet de loi C-51, la nouvelle infraction visant le fait de préconiser ou de fomenter la perpétration d'infractions de terrorisme de façon générale était si générale qu'il était impossible d'intenter des poursuites sur cette base. Quand le ministre a comparu ici, il a parlé des modifications à apporter pour qu'on puisse porter des accusations. J'aimerais savoir si vous pouvez nous en parler brièvement, en une trentaine de secondes, probablement.

M. Raymond Boisvert: Quand je travaillais pour le SCRS, bien que cela fasse déjà longtemps puisque je l'ai quitté il y a presque six ans, j'étais responsable de l'équipe des activités contre-terroristes, et certaines accusations étaient très difficiles à porter compte tenu de la valse complexe qui se joue entre le renseignement et la preuve. Autrement dit, nous prenions des mesures contre des cibles qui respectaient le seuil du SCRS, parce que nous avions des raisons de croire à des malversations, mais un problème se posait lorsque venait le temps de transmettre l'information tout en protégeant nos sources. Bien sûr, le projet de loi C-59 propose de nouveaux outils pour faciliter cela.

Cependant, nous laissions passer beaucoup d'occasions d'agir, d'abord parce qu'il était très difficile de convertir en preuve utilisable l'information recueillie au titre du renseignement et ensuite, parce que bien souvent, je trouvais l'attitude des procureurs de la Couronne excessivement prudente. À titre de Canadien, je trouve que c'est très important, parce qu'il doit y avoir des mécanismes de poids et de contrepoids, qu'il faut définir les choses pour que notre système judiciaire laisse très peu de place à des poursuites qui ne pourraient pas être menées à bien. Plus souvent qu'autrement, les affaires soumises étaient jugées inadmissibles, même si ailleurs, au sud de notre frontière, par exemple, on n'aurait pas hésité à intenter des poursuites.

Le président: Merci, madame Damoff.

[*Français*]

Monsieur Paul-Hus, vous avez sept minutes.

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

Bonjour, monsieur Boisvert et madame Vonn.

Monsieur Boisvert, je vais commencer par vous.

Je vais parler un peu du groupe État islamique. On sait maintenant que ce groupe a perdu beaucoup de terrain en Syrie et en Irak, mais il a commencé à mener des opérations de cyberattaques. Le rapport public de 2017 sur la menace terroriste pour le Canada confirmait que Daech avait utilisé des moyens de cyberexploitation afin de dresser des listes de personnes à abattre. Ces listes renfermaient le nom et les renseignements personnels de personnes choisies au hasard et on incitait les sympathisants de Daech à les attaquer.

En ce qui concerne la menace que représente le groupe État islamique, pensez-vous qu'on devrait se concentrer principalement sur les cyberattaques de ce genre et les contrôles?

M. Raymond Boisvert: Je dirais que non. Mes inquiétudes portent davantage sur les attaques cybernétiques. Comme je l'ai expliqué dans mes commentaires initiaux, ces attaques représentent beaucoup plus un danger direct pour la société ainsi que pour notre prospérité actuelle et future.

Compte tenu de la nature du terrorisme, de telles attaques ont des effets amplifiés par comparaison avec les autres menaces à la sécurité nationale. Par contre, ce n'est pas encore la fin de Daech. Ce groupe a encore une capacité opérationnelle suffisante pour attaquer des Canadiens ou des intérêts canadiens ici ou à l'étranger.

M. Pierre Paul-Hus: Parlons justement d'intérêts économiques. Il y a quelques jours, le journal *Le Monde* nous apprenait que le siège de l'Union africaine, situé à Addis-Abeba, était espionné par Pékin. Ce bâtiment a été construit en 2012 par les Chinois, qui en ont profité pour installer des systèmes leur permettant de transférer toute l'information du siège de l'Union africaine à Shanghai.

Ce genre de choses vous surprend-il?

Le gouvernement essaie de tisser des liens économiques avec la Chine, mais plusieurs pays considèrent la Chine et la Russie comme des acteurs majeurs en matière de cyberattaques et de collecte de renseignements. Êtes-vous d'accord là-dessus?

● (1235)

M. Raymond Boisvert: Oui.

Si vous me le permettez, je vais faire quelques commentaires en anglais, étant donné que je travaille plutôt en anglais présentement.

[*Traduction*]

Il ne fait aucun doute que la Russie peut présenter une menace. On l'a vu par son ingérence dans les processus démocratiques en Europe de l'Ouest comme aux États-Unis, et dans un nombre grandissant d'États américains. L'intention malicieuse de la Russie par son appui au régime autocratique de la Syrie et d'ailleurs est claire. Ce sont là des activités beaucoup plus prévisibles et se rapprochant beaucoup plus du modèle classique des activités quasi militaires. Dans le cas des menaces de guerre hybride que nous voyons émerger de la Russie, elle utilise des mandataires pour mener ses cyberattaques, et nous l'avons vue lancer diverses attaques en collaboration avec les groupes criminels organisés russes, qui ont eu des effets néfastes graves sur d'autres pays, dont le Canada.

Le cas de la Chine est beaucoup plus complexe, et je comprends les difficultés que présente un pays comme le nôtre. Les entreprises d'État et le capitalisme autoritaire semblent créer beaucoup d'occasions d'affaires qui peuvent influencer les décisions, mais elles présentent parfois des complexités dont je ne suis pas certain que nous ayons examiné toutes les ramifications au Canada.

Il y a aussi le fait que la Chine admet désormais elle-même jouir d'un « pouvoir acéré », qu'elle exerce presque sans réserve. Elle ne cherche même plus à cacher ses intentions. Elle adopte une stratégie très offensive en matière de ressources et de propriété intellectuelle, comme elle est très claire dans ses rapports avec les dissidents et les universitaires. Elle en arrête certains, elle en punit d'autres, y compris des institutions universitaires nord-américaines, comme bon lui semble, donc je crois que les Canadiens doivent réfléchir aux valeurs associées aux débouchés économiques qui se présentent. La guerre froide est révolue, mais il y en a une nouvelle forme qui se pointe rapidement, et je pense que notre obsession du contre-terrorisme ne nous sert pas toujours.

[*Français*]

M. Pierre Paul-Hus: On parlait justement de guerre. Je ne me souviens plus si c'était ici ou à la séance du Comité permanent de la défense nationale. Je crois que c'est Mme Damoff qui a abordé le sujet. Il a été question des actes malveillants de la Chine et de la Russie envers le Canada.

Plus tôt, vous avez dit que l'attaque constituait la meilleure façon de se défendre. Croyez-vous que le Canada est en mesure de mener des actions offensives susceptibles de le protéger, ou ce processus est-il trop complexe?

Je sais que c'est complexe, mais je me demande quel type d'actions le Canada pourrait mener pour se protéger.

M. Raymond Boisvert: Dans un monde hyper compétitif, il faudrait en effet opter pour l'offensive. Nous faisons face à des nations étrangères qui ne sont aucunement assujetties aux mêmes règlements ou à des organismes du genre de celui que représente Mme Vonn et qui font que le gouvernement doit rendre des comptes.

J'ai parlé plus tôt d'une éventuelle attaque cybernétique contre l'une de nos organisations. Il est difficile de déterminer si, de façon évidente, cette attaque proviendrait d'un pays en particulier ou de ses représentants. Quoi qu'il en soit, je crois qu'il nous est de plus en plus possible de déterminer précisément quels ordinateurs et centres de fonctionnement nous pourrions viser, attaquer et retirer du réseau international de communications.

M. Pierre Paul-Hus: Le gouvernement actuel critiquait un peu le projet de loi C-51. On a donc proposé le projet de loi C-59 pour modifier certaines choses. On rappelle souvent que les droits et libertés des Canadiens ne doivent pas être brimés; on s'entend là-dessus. Cependant, lorsqu'on est dans un contexte défensif, on doit disposer de mesures de protection.

Selon vous, le projet de loi C-59 va-il atténuer de façon excessive les mesures de protection du gouvernement?

[*Traduction*]

M. Raymond Boisvert: Non, je pense... J'apprécie beaucoup le travail de Mme Vonn et de ses collègues d'autres organisations au Canada ou ailleurs, dans les démocraties occidentales. C'est un élément important de la discussion, mais bien souvent, je crains un peu qu'on passe trop de temps à scruter des organisations respectueuses du droit, à mes yeux. Elles sont soumises à toutes sortes d'examens, dont ceux du vérificateur général et du commissaire à la protection de la vie privée. Nous avons maintenant un certain nombre d'autres organismes que j'accueille favorablement, comme je l'ai déjà dit. Je pense qu'en cette ère de transparence et de responsabilité, les organismes qui exercent ces pouvoirs spéciaux doivent y avoir accès, mais qu'on oublie parfois, en mettant autant l'accent sur la collecte fortuite de renseignements sur certains Canadiens, que quoiqu'on en dise, ce n'est pas si répandu. Je sais qu'à l'époque où j'étais là, c'était un phénomène très marginal et fortuit. Cela arrive, en raison de la convergence de l'infrastructure mondiale de l'information et des communications. Ce genre de chose arrive, mais les Canadiens ne semblent pas s'inquiéter autant de tous les courtiers en information, qui détiennent pourtant des centaines, voire des milliers d'identificateurs uniques à leur sujet.

Parfois, j'aimerais que l'organisation de Mme Vonn et les autres s'y attardent un peu plus. Il serait bon de prendre conscience du fait que les Canadiens doivent surveiller leurs données et leurs renseignements personnels, mais cesser de s'inquiéter autant des agences de sécurité, parce qu'elles sont soumises à des règles d'engagement et à de nombreuses vérifications. Il faudrait plutôt tourner le regard vers ceux qui échappent à cette surveillance.

● (1240)

Le président: Merci, monsieur Paul-Hus et monsieur Boisvert.

Allez-y, monsieur Dubé.

M. Matthew Dubé: Merci, monsieur le président.

Je vous remercie tous deux d'être ici. C'est intéressant, compte tenu des observations qui viennent d'être faites sur l'information recueillie fortuitement, parce qu'il y en a, il y a de l'information accessible au public, et il y aurait clairement intention, avec ce projet de loi, d'élargir les pouvoirs ouvrant la porte à cette nouvelle menace, que vous décrivez. Or, quand on demande au directeur du CST de nous expliquer pourquoi ces pouvoirs seraient utilisés, il ne peut nous en donner aucun exemple.

Cette question s'adresse à vous, madame Vonn. J'aimerais comprendre, parce qu'il y a un lien, là. L'une des réponses que ces fonctionnaires m'ont donnée quand ils ont comparu devant le comité, était « ne vous inquiétez pas; si vous prenez la partie 3 du projet de loi, à l'article proposé 25, vous verrez qu'il faut veiller à ce que des mesures soient en place pour protéger la vie privée des Canadiens », mais c'est une exigence très vague, et on précise ensuite « en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation », puis on décrit l'information visée.

Le choix du mot « divulgation » est particulièrement troublant, parce que c'est le nouveau terme utilisé pour désigner la communication d'information, tel qu'il en était question dans l'ancien projet de loi C-51. Faut-il s'inquiéter de la communication de cette information? Elle serait apparemment recueillie par le CST à des fins de recherche ou à d'autres fins légitimes, mais elle pourrait tout de même être communiquée, et je me demande s'il y a lieu de craindre les conséquences à cela, particulièrement si l'information en question est communiquée à nos alliés du Groupe des cinq, comme on en a vu des exemples dans un article de *La Presse* la fin de la semaine dernière, qui faisait état du fait que la GRC acquiert de l'information sur des Canadiens de la DEA sans la surveillance judiciaire qui s'appliquerait normalement au Canada.

Compte tenu du portrait très vaste que je viens de brosser, j'aimerais comprendre comment le fait de préserver les dispositions sur la communication d'information qu'on trouvait dans le projet de loi C-51, même si la forme en est modifiée, jouera sur l'effet de ces nouveaux pouvoirs du CST, parce que je pense que beaucoup de personnes ne le comprennent pas.

Mme Micheal Vonn: Merci.

Il est absolument essentiel pour les défenseurs des libertés civiles que le public comprenne que la collecte de renseignements personnels par les agences de sécurité nationale, qu'elle soit fortuite ou non, n'est pas inoffensive. En partie parce que nous avons des alliances, la communication d'information peut parfois avoir des conséquences problématiques pour les personnes visées, même si l'idée est que nous n'exploiterons peut-être pas ces renseignements, que nous ne les utilisons peut-être pas.

On essaiera de nous rassurer, mais on ne sait pas quelles données seront utilisées ou exploitées. Nous savons que cela peut aller de la cartographie des réseaux au profilage, qui constitue un énorme problème. Les Canadiens comprennent bien que c'est une menace à leur propre sécurité personnelle. Il est absolument primordial de comprendre les risques qui viennent avec la collecte, l'utilisation, la conservation et l'exploitation des données. Il faut en comprendre les ramifications et veiller à ce que les mécanismes mis en place ne soient pas que théoriques si l'on nous dit que des mesures sont prises. Quelles sont ces mesures? Comment pouvons-nous savoir où elles interviennent? Nous prémunissent-elles contre tous les risques?

Il y a des choses qui se passent en coulisses, en matière de sécurité nationale, que la plupart des Canadiens ne peuvent pas voir. Nous en sommes arrivés à avoir des raisons d'être méfiants, parce que l'on ne nous donne même pas de définitions simples de ce qui nous permettrait d'avoir l'information requise pour assurer une bonne responsabilité démocratique.

Quand on voit les failles que comportent les définitions du projet de loi C-59 sur l'information accessible au public, entre autres, pour reprendre ce que disait mon collègue, et quand on sait qu'un organisme de sécurité nationale peut acquérir des données grâce à un courtier en données à l'aide des techniques qu'on vient de nous décrire, pour les intégrer à un système tel que l'information peut être communiquée à nos alliés étrangers, on voit que ces façons de faire peuvent avoir des effets amplifiés sur la sécurité des personnes — je ne parle pas de la sécurité nationale, mais bien de la sécurité personnelle.

Les gens ne sont pas aussi alertes qu'on le voudrait à l'égard de ces menaces, mais ils prennent de plus en plus la mesure de ces problèmes, comme vous l'illustrez bien.

● (1245)

M. Matthew Dubé: J'aimerais vous entendre tous les deux à ce sujet.

On entend à répétition les mots « infrastructure de l'information ». Il y en a une définition. Nous pouvons en débattre, mais les définitions applicables à l'attaque d'une entité étrangère ou à l'information recueillie par le CST n'étaient pas les mêmes que lorsque la Loi sur le CST a été adoptée. Ces structures d'information... Je pense en particulier aux questions posées par Mme Damoff aux deux derniers groupes de témoins sur...

Même quand on regarde les services de télécommunications dans ce pays, on se met des oeillères si l'on croit que la technologie LTE et les autres choses du genre ne sont pas interreliées. Il y a de toute évidence des efforts internationaux qui se déploient pour rendre ces réseaux plus efficaces et plus robustes, mais pendant ce temps, les définitions juridiques... Elles ne semblent plus vraiment d'actualité, pour ce qui est de ce qu'on considère étranger ou non. Dès qu'on accorde à un ministre le pouvoir de cibler l'infrastructure d'information, il ouvrira inévitablement un filet bien plus grand que jamais auparavant. Je me demande ce que vous en pensez.

Nous pourrions peut-être commencer par M. Boisvert, avant de revenir à Mme Vonn.

Le président: C'est une question très importante. Malheureusement, M. Dubé ne vous a laissé qu'une minute pour y répondre, donc pouvez-vous y répondre très brièvement?

M. Raymond Boisvert: Ce sera très difficile. C'est un monde très complexe, qui se complexifie de plus en plus. Les données se multiplient de façon exponentielle.

Il y a deux côtés à la médaille. D'une part, la technologie nous permet de faire toutes sortes de choses. D'autre part, bien sûr, elle prête le flanc à des attaques pouvant venir de partout, puisqu'on peut voler les renseignements personnels identifiables dans ces réseaux, comme on dit qu'une agence de sécurité pourrait le faire, dans le cadre d'un mandat et de manière légitime, aux fins d'une enquête tout à fait fondée.

Nous avons un grave problème pour ce qui est des données, de la protection de la vie privée et de l'invasion ou de la perte de sécurité de la personne. Je pense qu'il faut beaucoup plus nous inquiéter des menaces venant des acteurs malveillants que des agences de sécurité.

Mme Micheal Vonn: On peut sentir la tension qui s'installe quand on donne au CST de vastes cyberpouvoirs qui exploitent activement les vulnérabilités du système, contre lesquelles les Canadiens doivent évidemment se protéger. Allons-nous les divulguer ou les exploiter? C'est l'un des problèmes inhérents à ces nouveaux pouvoirs.

M. Matthew Dubé: Si vous me permettez d'intervenir très rapidement, en une vingtaine de secondes...

Le président: Vous avez 20 secondes.

M. Matthew Dubé: Quand je me suis prêté à l'exercice auquel s'est prêtée CBC/Radio-Canada concernant les téléphones cellulaires, j'ai remarqué que le CST n'a pas osé se prononcer sur l'incidence de tout cela sur la confiance du public. Est-ce que ce pourrait être parce que ces échappatoires mêmes sont exploitées et qu'inévitablement, il y a là un risque?

Le président: Vous devrez trouver le moyen de répondre à cette question ultérieurement. Je suis désolé.

Allez-y, monsieur Fragiskatos, vous avez sept minutes, s'il vous plaît.

M. Peter Fragiskatos (London-Centre-Nord, Lib.): Merci infiniment, monsieur le président. Je remercie nos deux témoins ici présents.

Monsieur Boisvert, j'aimerais d'abord parler un peu de cybersécurité et d'offensive. Dans votre exposé, vous avez parlé d'une communauté de nations aux vues similaires qui prennent la cybersécurité très au sérieux pour diverses raisons, non seulement du point de vue de la sécurité publique ou de la sécurité nationale dans son sens classique, mais également du point de vue de la défense des principes démocratiques fondamentaux.

J'aimerais que vous nous situiez un peu, ou je devrais plutôt dire que vous situiez le CST, en ce qui concerne ses propositions et ses cybercapacités offensives. Comme se compare-t-il à ses pendants des autres puissances moyennes? Je ne parlerai pas des États-Unis, mais on peut prendre l'exemple de l'Australian Signals Directorate, qui est l'équivalent du CST et qui a des cybercapacités offensives. En Nouvelle-Zélande, le Government Communications Security Bureau est l'équivalent du CST. Il ne participe pas directement à l'élaboration d'une stratégie offensive de cybersécurité, puisqu'elle relève plutôt de la force militaire. C'est ainsi que les responsabilités sont partagées là-bas.

Où nous situons-nous par rapport à nos alliés du Groupe des cinq? Regardons un peu ce qu'ils font et les comparaisons qui s'en dégagent.

M. Raymond Boisvert: Je pense qu'à l'heure actuelle, nous sommes en queue de peloton pour ce qui est de nos investissements et des pouvoirs consentis à nos organismes de sécurité pour réagir.

Je pense que cela pourrait changer. La nouvelle cyberstratégie gouvernementale qui s'en vient pourrait nous propulser à un autre niveau atmosphérique, mais pour l'instant, je pense que le Canada semble traîner de la patte par rapport à ses principaux alliés, comme le Royaume-Uni, l'Australie et la Nouvelle-Zélande, entre autres. Pour moi, c'est très problématique, parce que si ma responsabilité de conseiller provincial en matière de sécurité consiste à contribuer à la réalisation d'objectifs stratégiques afin d'assurer notre prospérité, cela revient surtout à protéger l'infrastructure critique et à assurer la cybersécurité.

Ainsi, comme je l'ai dit, nous ne pouvons pas tout faire seuls ou ils ne peuvent pas tout faire seuls, et j'entends par « ils » ceux qui possèdent cette infrastructure critique. Je parle des grands organismes indépendants du gouvernement de l'Ontario, notamment dans les secteurs de la santé, de l'éducation et des transports. Nous devons renforcer nos capacités pour les arrimer à celles de pays comme l'Australie.

● (1250)

M. Peter Fragiskatos: Je suis content que vous mentionniez l'infrastructure essentielle, parce que j'aimerais que vous nous expliquiez comment la cyberoffensive peut nous permettre de protéger notre infrastructure essentielle. Vous avez exprimé très publiquement vos inquiétudes concernant les centrales hydroélectriques et nucléaires, de même que les systèmes de santé et les attaques destinées à nous extirper des renseignements personnels et privés sur les Canadiens ou sur notre R-D. Quelle est l'importance de notre stratégie offensive, de notre cyberoffensive, pour assurer notre cybersécurité et protéger tout cela?

M. Raymond Boisvert: Permettez-moi d'affirmer premièrement, à mon tour, qu'il faut vraiment comprendre que le secteur de la santé en général est désormais le secteur gouvernemental le plus ciblé au monde. En ce moment même, avec les adresses de domaine .mail et . gov, la plupart des organismes de santé sont la cible d'attaques. Pourquoi? Parce que les données sont le nouvel or noir. C'est la ressource la plus coûteuse et la plus recherchée au monde et les acteurs malveillants de toutes sortes s'y intéressent de plus en plus. On peut aussi dire que c'est probablement le secteur le moins protégé dans notre société, par opposition à d'autres grands secteurs gouvernementaux, dont le militaire.

Je pense que nous devons nous organiser rapidement afin d'apprendre à utiliser les outils cyberoffensifs. Par exemple, il faudrait constamment aller fouiller le Web invisible à la recherche d'indicateurs précoces de compromission et des mentions par les acteurs malveillants de notre existence, de nos domaines, de nos stratégies, pour y réagir précocement.

Il y aurait aussi possibilité d'intervenir de manière offensive. Dans l'éventualité d'une vaste attaque par saturation, comme il y en a eu contre *Spamhaus*, *The New York Times* et d'autres organisations, des attaques qui prennent de plus en plus d'ampleur, il faut comprendre que sans l'aide de nos grandes agences de sécurité, ces piliers de nos sociétés démocratiques risquent de s'effondrer. Il faut être proactif, cibler ces serveurs — le tout, bien sûr, en consultation avec la ministre des Affaires mondiales et avec l'approbation du ministre de la Défense nationale —, dans l'espoir d'avoir un effet cinétique sur ces serveurs et de les éliminer.

M. Peter Fragiskatos: Je comprends cela.

Vous avez indiqué très clairement à quel point il est important de sécuriser les infrastructures essentielles. Mon collègue d'en face a déjà posé des questions à ce sujet.

Dans le cas de la menace que fait peser Daech, par exemple, le pendule oscille et a oscillé au fil des ans. Après les événements du 11 septembre, en particulier, on mettait l'accent sur l'islam radical, si je peux m'exprimer ainsi, de même que sur la lutte contre cette menace. Toutefois, pouvez-vous passer en revue ce que vous avez dit à propos de l'importance de sécuriser nos infrastructures essentielles?

Si nous dressons la liste des menaces et que nous les classons en fonction du danger qu'elles représentent pour notre sécurité nationale, pensez-vous qu'il est plus important maintenant de se concentrer sur les infrastructures essentielles que sur les autres éléments que nous examinions dans le passé, après les événements du 11 septembre?

M. Raymond Boisvert: Oui. Comme je l'ai dit plus tôt, le terrorisme est efficace parce qu'ils terrorisent les gens. Il a un effet disproportionné. Le nombre de Canadiens touchés par un acte terroriste est très faible.

Inversement, les infrastructures sont tous les éléments qui nous permettent de rester en vie. Il s'agit du chauffage, de l'éclairage, des aliments dans les épiceries et de l'essence dans les stations-service. Tous ces éléments fondamentaux qui nous permettent d'exister reposent de plus en plus souvent maintenant sur des systèmes automatisés — sur des machines, sur l'apprentissage automatique. Toutes ces connexions sont interdépendantes. C'est la raison pour laquelle elles courent des risques. Elles courent des risques principalement à l'ère de la guerre du cinquième domaine. Nous sommes passés de la terre à la mer, puis de l'air à l'espace. Maintenant, tout est lié à la cybernétique. Nous n'assisterons probablement plus à un autre débat sur les F-35 parce que, dans la plupart des administrations, la majeure partie des fonds sont dirigés vers la guerre de l'information.

Ils feront ce que la Russie a fait en Moldavie, en Ukraine et en Géorgie, c'est-à-dire s'attaquer à quelque chose et le signaler. Vous éliminerez peut-être simplement un petit élément, puis un élément plus important, puis un élément qui risque d'avoir un effet cataclysmique. Je crois que c'est vraiment là que se trouve la grande menace.

Les terroristes utilisent-ils des outils cybernétiques? Pas tellement jusqu'à maintenant. Est-ce que Daech passera de la domination des médias sociaux au perfectionnement de leurs compétences en matière d'attaque? Je pense que c'est très possible.

Le président: Merci, monsieur Fragiskatos.

M. Paul-Hus et M. Eglinski interviendront pendant cinq minutes.

Si mes collègues n'y voient pas d'inconvénient, je vais me prévaloir de l'immense pouvoir que confère mon poste et permettre à M. Spengemann d'intervenir pendant les cinq dernières minutes de la séance, même si nous aurons dépassé le temps qui nous était imparti.

Vous disposez tous deux de cinq minutes.

● (1255)

[*Français*]

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

Ma question s'adresse à M. Boisvert.

Le Canada adopte une approche de laisser-faire à l'égard des investissements chinois dans les entreprises canadiennes, en particulier dans le secteur de la technologie. Cela vous préoccupe-t-il, d'autant plus qu'un des plus proches alliés du Canada lui reproche de vendre une entreprise de haute technologie qui vend des systèmes de communications par satellite aux Chinois?

M. Raymond Boisvert: J'avoue que c'est un domaine très complexe, comme je l'ai souligné auparavant. De nouvelles occasions se présentent. Le Canada doit composer avec une nouvelle réalité économique, alors que des négociations sont en cours avec ses partenaires en Amérique du Nord.

La Chine représente une réelle occasion, mais il faut garder les yeux ouverts. En ce qui concerne les investissements dans certains secteurs, particulièrement dans le secteur technologique, j'ai effectivement plusieurs préoccupations.

M. Pierre Paul-Hus: D'accord.

Je cède la parole à mon collègue.

[*Traduction*]

M. Jim Eglinski (Yellowhead, PCC): Le Comité a entendu dire que le Groupe des cinq était indispensable à la communauté canadienne du renseignement. Si la nouvelle obligation de rendre des comptes et la nouvelle réglementation réduisent notre capacité de consulter ce groupe, quelles en seront les conséquences?

M. Raymond Boisvert: Du moins pendant la période où j'ai travaillé au SCRS et au sein de la communauté du renseignement, le Canada était toujours un contributeur net très puissant et respecté au sein du groupe. Cependant, cela pourrait avoir changé avec le temps.

En fin de compte, je suis enclin à croire que nous sommes entrés dans une nouvelle ère. Comme les choses changent constamment, la législation doit changer. Nous devons améliorer notre capacité de réaction aux nouvelles avancées technologiques. Toutefois, nous sommes aussi encore en partie à l'ère de ce que j'appelle « l'après-Ed Snowden ». Une fois que nous aurons traversé cette période, la société aura néanmoins été transformée. Il a été un personnage lourd de conséquences. Je le reconnais, et je respecte son rôle.

Par conséquent, nous sommes dans une ère de responsabilisation et de transparence. Je pense que la présence de paliers supplémentaires ne pose pas de problème, tant qu'un mécanisme comme les pouvoirs d'urgence existe, comme ceux dont jouit le chef du CST. Je ne voudrais pas répondre à des commentaires alarmistes selon lesquels nous serons maintenant coincés et incapables d'intervenir efficacement. Je crois que, dans l'ensemble, un bon équilibre a été établi.

M. Jim Eglinski: Pensez-vous que cela pourrait mettre les Canadiens en péril?

M. Raymond Boisvert: Voulez-vous dire si le projet de loi C-59 est adopté dans sa forme actuelle, ou s'il y a un plus grand nombre de paliers?

M. Jim Eglinski: Oui, par rapport aux premières parties de ma question.

M. Raymond Boisvert: Je le répète, je pense que le projet de loi C-59 établit un bon équilibre. Je crois que les Canadiens seront mieux servis par cette mesure législative et que nous aurons une occasion aussi bonne que dans le passé de nous attaquer aux menaces naissantes.

M. Jim Eglinski: D'accord.

L'accroissement du nombre de comptes à rendre est-il problématique du point de vue des opérations si plus d'argent est consacré à l'administration? Voyez-vous un quelconque...?

M. Raymond Boisvert: Il ne fait aucun doute que la reddition de comptes a un coût, et ce coût pourrait être lié à l'agilité. Je dois toujours mesurer ces coûts. Je pense à une époque où j'étais responsable du secteur du contre-terrorisme, ou du principal secteur. Plus de 30 % des membres de mon équipe de gestion participaient aux audiences du Comité de surveillance des activités de renseignements de sécurité et aux audiences relatives aux certificats de sécurité, et, à ce moment-là, plus de 87 % de nos employés avaient moins de 2 années de service.

Ce milieu était lié à la gestion de risques élevés. Nous gérions un certain nombre d'enlèvements, dont ceux de Robert Fowler, Louis Guay et Amanda Lindhout. Probablement qu'une demi-douzaine de cas d'enlèvement se déroulaient simultanément partout dans le monde.

C'est une situation difficile à gérer. Si vous ajoutez des paliers, vous devriez probablement réfléchir à la question des ressources et vous efforcer de garantir que ces paliers ne nuisent pas à la capacité opérationnelle.

M. Jim Eglinski: Merci.

Le 20 novembre, j'ai pris la parole à la Chambre des communes pour aborder la question du projet de loi C-59, et j'ai parlé de la partie 5 qui modifie la Loi sur la communication d'information ayant trait à la sécurité du Canada. Nous avons entendu dire et lu à maintes reprises que, pour protéger les Canadiens, il était essentiel d'échanger des renseignements et d'éliminer le cloisonnement de l'information. Pensez-vous que le projet de loi C-59 accroît ou réduit notre capacité d'échanger des renseignements?

M. Raymond Boisvert: Disons simplement que nous sommes passés d'une capacité pratiquement nulle à une capacité considérable et que nous retournons peut-être à une situation imparfaite. Je suppose que, du point de vue d'un expert en sécurité et non de quelqu'un bien sûr... J'emprunterais les arguments de Mme Vonn à cet égard. Il faut vraiment faire attention à ce sujet.

Je vais vous relater une brève anecdote. Au début des années 2000, j'étais affecté à un poste au Moyen-Orient. Tout à coup, l'un des employés de l'ambassade est venu me voir — parce qu'il y avait de nombreux détenteurs de passeports qui perdaient leur document à répétition — et m'a dit, « Vous savez, il semble, selon les rapports que nous obtenons, qu'un passeport canadien soit apparu dans cinq différents pays au cours des six derniers mois, bien que son détenteur soit censé vivre encore dans le pays. » Je lui ai dit, « D'accord, puis-je connaître son nom? » Il m'a répondu, « Non, désolé, je ne peux pas vous le communiquer. »

De toute façon, nous avons fini par avoir un long débat. La question a été renvoyée à l'ambassadeur, ainsi qu'aux Affaires étrangères et au SCRS, et j'ignore si elle a été résolue finalement. À mon avis, c'était le pire exemple de la façon dont les choses se déroulaient dans le passé. Nous ne devons jamais nous retrouver de nouveau dans cette situation, parce que cela mettrait en péril la vie des Canadiens.

● (1300)

Le président: Merci, monsieur Eglinski.

Monsieur Spengemann, la parole est à vous pendant les cinq dernières minutes de la séance.

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

Je vous remercie de votre présence.

Madame Vonn, vous vous joignez à nous pendant la semaine qui marque le premier anniversaire de la fusillade qui a eu lieu à la mosquée de Sainte-Foy, au Québec. Le pays cherche encore à faire face à cette incroyable tragédie. Je me demande si, d'une façon très générale, vous pourriez nous dire ce que vous pensez de la situation actuelle du Canada en ce qui concerne l'équilibre entre les libertés civiles et une sécurité satisfaisante. D'un point de vue organisationnel, vous disposez peut-être de données étayant l'opinion des Canadiens, mais, à votre avis, où se situent les Canadiens par rapport à leur état d'esprit préalable au 1er janvier de l'année dernière?

Mme Micheal Vonn: Je vous remercie de votre question. J'espère que vous comprenez que l'Association des libertés civiles de la Colombie-Britannique prend la sécurité très au sérieux. L'importance de concilier correctement les droits et libertés des Canadiens avec la capacité du gouvernement d'assurer la sécurité nationale occupe une grande partie de notre temps.

Comme vous le savez peut-être, le Canada accusait — pour employer certains des termes qui ont déjà été mentionnés — un peu de retard dans un certain nombre de domaines, y compris le fait de disposer de mécanismes en matière de transparence et de responsabilisation qui sont la norme dans un grand nombre des pays de nos alliés. Nous accueillons favorablement la capacité d'inscrire dans la loi et de rendre plus transparente la responsabilisation qui est nécessaire pour que les Canadiens soient convaincus que la sécurité nationale est dans leur intérêt. Nous avons fait des progrès à cet égard.

Ce qui nous préoccupe à propos du projet de loi C-59, c'est le fait que les gens ont le sentiment que c'est le bon moment de régler les questions importantes. Lorsque nous vous présentons nos inquiétudes à propos des seuils de surveillance des données en vrac qui n'ont jamais été débattus d'une façon appropriée par le Parlement, nous vous disons que nous nous réjouissons de cette occasion qui nous est donnée de réfléchir ensemble à ces éléments importants. Toutefois, en partie en raison du fait que nous sommes saisis d'un projet de loi omnibus, certains de ces aspects ne reçoivent pas suffisamment d'attention.

M. Sven Spengemann: Je mentionne très brièvement que l'une des séries de dispositions qui importent énormément — elle se trouve près de la fin du projet de loi — est celle qui traite des jeunes, soit les articles 159 à 167. Ces articles font référence à la Loi sur le système de justice pénale pour les adolescents et rendent les jeunes vulnérables à de nombreux égards.

Pouvez-vous nous dire très brièvement si vous pensez que ces dispositions protègent adéquatement la vie privée et les intérêts personnels des jeunes Canadiens?

Mme Micheal Vonn: Pourrais-je fournir plus tard au Comité une réponse à ce sujet? Je vous le demande parce que j'ai l'impression de n'avoir pas prêté suffisamment attention à cet aspect particulier du projet de loi, étant donné que je me concentrais sur d'autres aspects. C'est avec plaisir que nous vous ferons part de nos opinions à cet égard.

M. Sven Spengemann: Je pense que ce serait utile.

Monsieur Boisvert, si vous nous permettez de tirer parti du poste que vous occupez, je sais que vous aurez de nombreuses observations à formuler à ce sujet. Les jeunes Canadiens sont vulnérables non seulement en raison de leur âge, mais aussi parce qu'ils sont les proies d'organisations terroristes comme le Groupe d'Abu Sayyaf, Al-Chabaab et l'État islamique.

Pourrions-nous connaître votre point de vue quant à la protection des jeunes contre les organisations terroristes qui s'attaquent à eux, en vertu des dispositions du projet de loi?

M. Raymond Boisvert: Je parlerai peut-être davantage à un niveau supérieur, ainsi qu'en ma qualité d'expert.

Je ne reproche pas à Internet de favoriser la radicalisation, mais c'est certainement une importante voie d'accès et une partie de l'écosystème qui permet à une personne de devenir la proie de messages négatifs.

Comme cela a été souligné de nouveau dernièrement aux États-Unis, dans le cadre d'une étude menée plus récemment, j'aimerais aussi faire ressortir le fait que la principale menace de radicalisation est l'extrême droite, et non l'extrémisme islamique. Je pense que c'est un point très important.

La radicalisation ou l'extrémisme sont du pareil au même. Ils véhiculent l'idée que nous vivons de plus en plus fréquemment dans un monde où nous sommes en mesure de propager la haine, de séduire les gens et de les motiver. La difficulté pour un organisme de sécurité, c'est que la personne sera souvent portée à son attention pour des raisons d'exploitation des données et d'affichage en ligne. Le cas d'Aaron Driver, qui est survenu en Ontario il y a près d'un an et demi de cela, en est un excellent exemple.

Internet est tout de même un important outil. Il reste à savoir comment on détermine le moment où quelqu'un passe de la radicalisation — le passage de la réflexion à l'indignation, puis à la formulation de commentaires relatifs à la mobilisation en vue d'une planification opérationnelle — à l'intention d'agir. Voilà le dilemme auquel font face les services de renseignement et les groupes d'application de la loi, comme la GRC, qui travaillent ensemble à la résolution de ces cas.

● (1305)

M. Sven Spengemann: Le temps qui me reste est très limité, mais, si vous me le permettez, j'ai une très brève question à vous poser.

Le président: Il vous reste 13 secondes.

M. Sven Spengemann: Vous êtes la personne la mieux placée pour répondre à cette question. Que pensez-vous d'un jeune Canadien qui a fait partie d'une organisation terroriste et qui revient au pays?

M. Raymond Boisvert: Je crois que le processus sera difficile et coûteux parce que, premièrement, ce conditionnement est difficile à comprendre. Une fois qu'une personne a été exposée à des degrés de violence extrême, qu'elle a été fortement radicalisée et formée à faire la guerre, on oserait espérer qu'elle en a eu assez, qu'elle en a vu assez et qu'elle a conscience d'avoir commis une terrible erreur. Je pense que la plupart de ces personnes sont exactement dans cet état d'esprit, mais comment le savoir?

Si je suis responsable d'assurer la sécurité des Canadiens ou de mettre en œuvre notre programme de contre-terrorisme, je dirais, « Eh bien, nous devons aller jusqu'au bout pour nous assurer que... rencontrons cette personne et parlons-lui aussi souvent que nous le pouvons afin d'avoir une meilleure idée de ce qui sous-tend ses motivations et de savoir si elle a tourné la page ». Ce qui est coûteux, c'est le fait que vous devez tout de même, je crois, assurer un certain niveau de surveillance au tout début du processus, mais que vous ne pouvez pas surveiller tout le monde. En 2012, le nombre de personnes préoccupantes dépassait de loin la capacité des services de sécurité, et je ne veux même pas penser aux chiffres d'aujourd'hui.

M. Sven Spengemann: Merci.

Le président: Merci, monsieur Spengemann. Je déteste mettre fin à cette conversation.

Au nom du Comité, je tiens à vous remercier de votre discernement.

Sur ce, la séance est levée.