CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la procédure et des affaires de la Chambre

PROC • NUMÉRO 028 • 1re SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 15 mars 2012

Président

M. Joe Preston

Comité permanent de la procédure et des affaires de la Chambre

Le jeudi 15 mars 2012

● (1115)

[*Traduction*]

Le président (M. Joe Preston (Elgin—Middlesex—London, PCC)): Nous allons ouvrir la séance.

Tout d'abord, j'aimerais remercier nos invités d'être venus ce matin. Je suis désolé pour le retard. Nous avons dû changer de salle afin que nos délibérations puissent être télévisées.

Nous entamons aujourd'hui notre étude sur la motion de privilège concernant le député de Provencher.

Je dois informer nos invités et les membres du comité que nous allons entreprendre nos travaux en séance publique et que nous ferons tout notre possible pour parler des atteintes au privilège et de tout ce qui s'y rapporte. Cependant, en tant que président, je considère qu'à un certain moment, nous devrons nous réunir à huis clos, pour des raisons de sécurité.

Je demanderais donc aux députés de tous les partis de nous en informer si c'est le cas. Nous essaierons de retarder le plus possible ce moment et d'attendre la fin de la séance pour discuter des questions délicates. Nous éviterons ainsi de siéger à huis clos, puis de reprendre nos travaux en public.

Par ailleurs, le Président nous a aujourd'hui remis une autre motion de privilège. Nous devrons trouver un moment pour en discuter. Je suis conscient qu'à l'heure actuelle, vous n'avez qu'entre minuit et six heures pour dormir, mais il se peut qu'on empiète sur ce temps.

Madame la greffière, nous sommes ravis de vous avoir avec nous aujourd'hui. Je vais donc tout de suite vous céder la parole et vous permettre de présenter les personnes qui vous accompagnent. Nous enchaînerons ensuite avec la période de questions.

Mme Audrey O'Brien (greffière de la Chambre des communes, Chambre des communes): Excellent.

Bonjour, monsieur le président. C'est un plaisir que d'être ici aujourd'hui.

[*Français*]

Ça me fait plaisir de me joindre à vous pour discuter de cette question très importante. Je suis accompagnée de deux de mes chefs de service. Louis Bard est dirigeant principal de l'information à la Chambre des communes.

[*Traduction*]

Il est responsable de la Direction des services d'information. Le sergent d'armes, Kevin Vickers, s'occupe, entre autres, des services de sécurité de la Chambre des communes. Il assure la sécurité de la Cité parlementaire et, bien entendu, des députés.

Je n'ai pas de déclaration liminaire comme tel, mais j'aimerais vous dire comment nous percevons la situation.

Je suis très heureuse que vous ayez choisi d'inviter le sergent d'armes et le dirigeant principal de l'information, parce que j'estime que ces services ont d'importants points en commun dans leur façon d'assurer la sécurité de la Cité parlementaire.

Premièrement, sachez que la sécurité ici à la Chambre des communes est fondée sur le renseignement. Il y a un parallèle à faire entre la sécurité assurée par le sergent d'armes et les services de sécurité de la Chambre des communes — et leurs partenaires — et la sécurité de la TI assurée par le dirigeant principal de l'information et l'équipe des services d'information de la Chambre des communes.

Si vous me le permettez, je vais prendre quelques instants pour vous donner un aperçu de notre travail. Évidemment, je ne suis pas une experte en matière de sécurité. Ce sont eux les experts sur qui je compte, et je suis convaincue que la Chambre et les députés sont entre bonnes mains.

Je vais tout d'abord vous parler du travail du sergent d'armes, que vous connaissez probablement plus et qui est moins difficile à comprendre. Le sergent et son directeur de la sécurité communiquent quotidiennement avec nos partenaires — la GRC, la police d'Ottawa, le SRSC, etc. — pour discuter du niveau de menace pour la journée, à l'égard de la Cité parlementaire et des députés. Ils sont en liaison constante.

Si, pour quelque raison que ce soit, le niveau de menace est élevé, soit à l'égard de la Cité parlementaire, en raison d'une manifestation contre un Sommet qui se tient quelque part dans le monde ou quelque chose du genre, soit à l'endroit d'un député ou d'un ministre, par exemple, nos partenaires de l'extérieur qui sont chargés de surveiller continuellement le niveau de menace vont nous faire part de leurs recommandations. Nous allons donc nous ajuster en conséquence pour être en mesure d'intervenir efficacement et de veiller à la protection de la Cité parlementaire et des députés.

Bien sûr, vous comprendrez que je ne peux révéler aucun détail sur ce type de mesures. Les consultations ne sont même pas discutées en public. Dans l'intérêt de la sécurité, il faut se taire et s'occuper de protéger la Cité parlementaire et les députés.

De façon très similaire, le dirigeant principal de l'information et son équipe sont en communication constante avec le Centre de la sécurité des télécommunications Canada, afin de surveiller les cybermenaces. L'internet, grâce à l'accès illimité qu'il offre, est une réalité à laquelle nous devons nous ajuster et que nous essayons de comprendre de diverses façons. Avec l'utilisation de plus en plus répandue des médias sociaux, il y a plein de choses qui se passent dans le cyberespace. Il faut se tenir au courant, mais en même temps, il faut accepter qu'on ne peut pas tout contrôler.

Auparavant, les manifestations pour ou contre un enjeu ou une position en particulier étaient assez directes. Les gens se réunissaient sur le gazon de la Colline parlementaire en brandissant des pancartes et en scandant des slogans. Ils écoutaient des gens, les applaudissaient, puis retournaient chez eux. Et c'était correct. Ces manifestations se déroulent encore et c'est correct aussi. Mais on assiste de plus en plus à des campagnes organisées sur l'internet et sur des médias sociaux dans lesquelles on défend des positions ou on proteste contre diverses mesures. Ces campagnes, tout comme le comportement humain, varient beaucoup. Elles peuvent être consciencieuses, sérieuses, anarchiques et même menaçantes, comme dans le cas du groupe Anonymous.

● (1120)

La difficulté dans ce cas, qui n'est peut-être pas celle à laquelle doivent faire face d'autres organisations — je pense aux entreprises notamment — c'est que lorsque nous créons un réseau parlementaire ici, le réseau de campus pour la technologie de l'information, il est construit pour correspondre à ce que nous croyons être un niveau de sécurité approprié et nous le surveillons constamment. Mais ce dont il faut se rappeler, c'est que de notre point de vue — et je pense également du point de vue des députés, étant donné que le réseau existe d'abord pour servir les députés — il doit être accessible aux personnes qui veulent vous joindre. La communication qui circule dans les deux sens, c'est-à-dire d'ici à l'extérieur et de l'extérieur vers notre réseau, c'est à la base de la conversation politique au Canada. Nous ne pouvons pas protéger un système de telle façon que l'accès en soit si compliqué et si difficile que cela devienne un irritant, ou encore pire, Dieu nous en protège, un obstacle à ce flux d'information et de communication libre.

Parallèlement, je pense que nous devons reconnaître que peu importe la façon dont on voudra créer un réseau, il est tout simplement impossible de le protéger complètement contre le piratage. Les fuites dans WikiLeaks qui ont fait les manchettes il y a quelques mois, en constituent un exemple parfait. En fait, il n'existe pas de réseau sans faille. Et lorsqu'on soutient qu'un réseau est parfait, c'est comme si on lançait un défit en quelque sorte et quelqu'un quelque part s'évertuera à le pirater tout simplement parce que c'est ainsi qu'il passe son temps. Je pense que c'est quelque chose qu'il faut accepter.

Ce que nous devons faire — et j'estime que c'est ce que nous faisons — c'est de songer très sérieusement à l'idée que nous avons besoin d'un réseau protégé, que nous avons besoin d'un réseau sécuritaire afin que les parlementaires puissent faire leur travail. Et c'est ce que nous faisons en surveillant de très près l'activité sur le réseau de façon constante afin de pouvoir déceler tout ce qui semble inusité ou qui ressort du lot. C'est ce que nous faisons de diverses façons grâce aux mesures de sécurité en place. Lorsque nous constatons une activité inusitée, nous prenons les mesures appropriées pour régler le problème, qu'il s'agisse d'isoler un ordinateur en particulier ou quoi que ce soit d'autre. Bien sûr, tout cela se fait avec nos partenaires du Centre de la sécurité des télécommunications et les intervenants qui s'y trouvent.

Nous disposons de diverses méthodes — et je n'entrerai pas dans les détails pour vous les expliquer, tout simplement parce que je pense que je ne pourrais pas le faire adéquatement — et de divers thèmes, je crois, auxquels correspondent nos opérations. Il y a, par exemple, le principe de protection. Nous disposons de pare-feux informatiques protégeant le réseau parlementaire. Nous avons des passerelles filtres. Nous avons des logiciels de chiffrement. Pour ce qui est de la détection d'activités inhabituelles, nous disposons de types de logiciels habituels, c'est-à-dire anti-pourriels et antivirus, qui sont constamment mis à jour et qui font l'objet de suivi au fur et à mesure que les systèmes et la technologie se développent.

Le contrôle de l'accès est certainement très important. Je me souviens avoir comparu devant le comité sur une autre question et j'avais dit qu'un réseau n'est aussi sécuritaire que la personne qui en constitue le maillon le plus faible. Donc, quiconque l'utilise,

[*Français*]

il est bien important de savoir qui a accès, qui a les mots de passe et tout cela. Il y a des protocoles bien importants qui régissent l'utilisation du réseau.

L'autre aspect est la sécurité physique des différentes pièces d'équipement qu'on a, naturellement.

[*Traduction*]

Voilà donc pour la sécurité physique, qu'il s'agisse d'ordinateurs portables ou autre.

Quant aux communications entre le réseau de la Colline et le réseau dans vos circonscriptions, cela est rendu possible grâce à la création de ce qui s'appelle un réseau privé virtuel ou un RPV. Les communications protégées sont ainsi permises dans l'environnement du réseau.

Du côté administratif, nous menons des campagnes de sensibilisation en matière de sécurité qui relèvent du sergent d'armes et du dirigeant principal de l'information. Nous adoptons des politiques appropriées, allant du port d'épinglettes à l'utilisation appropriée de la technologie.

Nous essayons de sensibiliser les gens aux dangers existants, sans toutefois réagir exagérément de manière à attirer l'attention plus qu'il ne faut aux divers fauteurs de troubles qui ne veulent rien de plus que d'avoir la chance de faire les manchettes.

Nous travaillons de très près avec le CST et le SCRS. J'ai ici un extrait, une déclaration du SCRS qui pourrait être utile. Elle se lit comme suit:

> La menace d'attaques contre les systèmes d'information critiques et les infrastructures qui dépendent de ces systèmes sera, dans un avenir assez rapproché, pratiquement impossible à éliminer entièrement, car les réseaux utilisés pour commettre les attaques et les systèmes de gestion des réseaux sont en constante évolution. Au fur et à mesure que de nouvelles stratégies verront le jour, de nouveaux outils d'attaques apparaîtront et le savoir-faire des personnes qui se servent de ces outils s'améliorera.

Je ne veux pas laisser l'impression que la situation dans laquelle s'est retrouvé le ministre de la Sécurité publique est quelque chose que nous tolérons. C'était tout à fait épouvantable. Mais, parallèlement, je pense qu'il faut placer le tout dans le contexte de ce qui se passe dans le monde aujourd'hui. Cela ne devrait pas générer d'anxiété non fondée sur l'exhaustivité des mesures de sécurité en place.

● (1125)

[*Français*]

C'est à peu près tout ce que j'avais à dire.

[*Traduction*]

Nous sommes là pour répondre à vos questions, et les deux experts qui m'accompagnent sont bien sûr également à votre disposition.

Le président: Merci, et merci d'être accompagnée d'experts.

La parole est à M. Lukiwski.

M. Tom Lukiwski (Regina—Lumsden—Lake Centre, PCC): Merci, monsieur le président.

Merci madame O'Brien, monsieur Bard et monsieur Vickers d'être là.

Ce sur quoi la plupart d'entre nous allons nous concentrer je crois, c'est l'information que vous pouvez nous donner sur les cybermenaces liées aux technologies de l'information. Nous allons parler avec certains organismes d'application de la loi au cours des prochaines séances pour évaluer la menace qu'Anonymous pourrait représenter au-delà de la Cité parlementaire. Par conséquent, la plupart de mes observations seront dirigées à M. Bard, même si je vous incite tous à me faire part de votre opinion.

Merci, madame O'Brien d'avoir répondu dans votre déclaration préliminaire à certaines des questions que j'allais poser.

D'abord, étant donné que personne ne peut mettre en place des dispositions ou des protocoles de sécurité qui mettraient un système complètement à l'abri des menaces, j'aimerais savoir tout de suite, selon votre avis éclairé, notre niveau de vulnérabilité? À quel point sommes-nous vulnérables à la possibilité d'un piratage de notre système par Anonymous? Deuxièmement, comptez-vous renforcer les mesures de sécurité au-delà de ce qui existe actuellement dans la Cité parlementaire? Et finalement, auriez-vous des recommandations à faire quant à nos systèmes installés à l'extérieur de la Cité parlementaire? Je pense plus particulièrement à nos bureaux de circonscription.

Un à la fois, je vous prie, veuillez donner votre évaluation de notre niveau actuel de vulnérabilité, et ensuite veuillez nous dire quelles mesures pourraient être mises en place.

Mme Audrey O'Brien: Avant de demander à M. Louis Bard, le dirigeant principal de l'information, de répondre à la question de M. Lukiwski, je veux signaler que les menaces lancées par le groupe Anonymous n'avaient en fait rien à voir avec le réseau. C'est quelque chose qui a été publié sur YouTube, par conséquent cela échappait à notre contrôle et ne touchait pas notre environnement.

Pour ce qui est de la situation de piratage et des mesures en place, Louis pourra vous en parler.

M. Louis Bard (dirigeant principal de l'information, Chambre des communes): Merci.

Il s'agit d'excellentes questions. Il ne fait aucun doute que la Chambre des communes, à titre de symbole du Parlement, est régulièrement recensée dans des menaces potentielles à la sécurité. Le Parlement peut figurer dans chaque menace que l'on cerne en raison de sa valeur de symbole.

Comme l'a dit Mme O'Brien, nous travaillons de très près avec divers partenaires comme le CST. Nous travaillons avec la GRC. Nous travaillons également avec l'industrie. Nous vous avons présenté un certain nombre de scénarios, de technologies et de couches superposées qui ont été mises en place pour protéger notre environnement, et nous nous fions à l'industrie également pour ce qui est d'amener une troisième dimension aux menaces, à savoir ce qui se passe et ce à quoi nous devrions nous préparer. Par conséquent, comme M. Vickers le fait relativement à la sécurité physique, nous évaluons quotidiennement ces menaces, de même que la situation.

Il y a environ trois ou quatre ans, le comité a approuvé la création d'une équipe de sécurité de la TI, que nous avons mise en place. Nous avons également déployé de nouvelles technologies et de nouveaux mécanismes pour protéger l'environnement.

Pour nous, lorsqu'un incident survient comme cela s'est produit il y a deux ou trois semaines, il ne fait aucun doute qu'à ce moment-là, nous renforçons nos activités de surveillance en fonction des menaces. Nous disposons de nombreuses alarmes. Nous faisons un suivi lorsque ces alarmes sont activées. Nous faisons un suivi des avis. Nous veillons à renforcer nos mesures de sécurité. Nous nous assurons d'apporter des ajustements à nos protocoles du jour. Citons comme exemple l'importante arnaque visant le Conseil du Trésor l'an dernier. Immédiatement, nous avions une longueur d'avance pour analyser la situation de sorte qu'en fait, aucun incident ne s'est produit sur la Colline du Parlement suite à cet événement.

Nous avons également ajusté nos stratégies de gestion de la continuité des opérations afin d'être en mesure de faire face aux menaces internationales, par exemple. Si nécessaire, je peux exporter mon site Web ailleurs pour protéger le campus. Il existe toutes sortes de stratégies de coulisses qu'il est possible d'activer et nous pouvons agir très rapidement. Il ne fait aucun doute que nous maintenons des liens très serrés avec les autres responsables, avec le CST et d'autres organismes, pour nous inspirer de toute situation possible afin de réduire l'impact au minimum.

Ce qui m'importe le plus, toutefois, c'est la façon dont nous prenons des décisions. Mon travail consiste à offrir un accès aux services à tous les parlementaires, à assurer la transparence, et à faire en sorte que j'élimine tous ces stress. Je dirais que nous rejetons 70 p. 100 de tous les courriels envoyés au Parlement avant qu'ils ne pénètrent dans le système de la Colline du Parlement. Et au-delà, nous offrons aux députés les outils requis pour recenser les pourriels afin de les filtrer et de mettre en place des règles. En fin de compte, je crois toujours que je dois accorder une certaine souplesse aux députés afin qu'ils puissent bien fonctionner.

Pour ce qui est des bureaux de circonscription, il ne fait aucun doute que l'environnement à Ottawa est protégé. Cet environnement est bien protégé. Nous offrons toutes sortes d'outils aux députés dans leurs circonscriptions. Toutefois, dans vos circonscriptions, c'est vous qui prenez les décisions. Vous établissez votre environnement et la façon dont vous voulez travailler. Par conséquent, je ne peux qu'offrir de l'aide, des conseils et des suggestions pour que vous utilisiez les outils protégés que nous vous fournissons. Je n'ai pas beaucoup de contrôle lorsque vous êtes dans votre circonscription, mais nous sommes toujours là pour vous aider en matière de sécurité.

Pour ce qui est des recommandations, il ne fait aucun doute que la politique d'utilisation acceptable vous donne un cadre de travail pour la façon dont vous fonctionnez. Il ne fait aucun doute qu'elle permet de mieux utiliser les ressources TI de la Colline parlementaire. Mais cela dépend également de votre personnel dans votre circonscription et de la façon dont vous vous comportez dans votre circonscription. Les lignes directrices sont adéquates. Mais parallèlement, comme nous l'avons toujours dit, il est primordial de faire la distinction entre votre travail en tant que députés et votre vie privée. Bien souvent, nous essayons de faire en sorte que ce soit bien distinct — la façon dont vous établissez vos outils informatiques à la maison, avec votre famille, et la façon dont vous décidez de créer d'autres accès Internet, qui rendent vos courriels privés accessibles, à l'extérieur de l'environnement de la Chambre des communes. C'est ce que nous recommandons fermement. C'est exactement ce que je fais moi-même.

● (1130)

Toutefois, la sécurité change quotidiennement. Chaque jour nous devons faire... C'est comme si on épluchait un oignon. Il y a toujours quelque chose de nouveau à découvrir. Notre force, c'est que nous avons la capacité de réagir. Je pense que nous l'avons prouvé à plusieurs reprises. Et la régie interne ainsi que le comité nous ont appuyés pour tous les investissements que nous avons faits dans la technologie de la sécurité au cours des dix dernières années.

● (1135)

Le président: Merci. Vous avez largement dépassé votre temps.

Madame Charlton, pour sept minutes.

Mme Chris Charlton (Hamilton Mountain, NPD): Merci beaucoup monsieur le président.

Merci beaucoup pour votre exposé ce matin.

J'aimerais commencer à un niveau plus général. Comme vous le savez, lorsque le Président établit à première vue qu'il s'agit d'une atteinte au privilège, c'est ce qui est renvoyé au comité. Nous avons trois responsabilités à cet égard. La première, bien sûr, consiste à confirmer si en fait il y a atteinte au privilège. Ensuite, il nous incombe d'identifier le coupable. Et troisièmement, notre tâche consiste à explorer les recours possibles.

J'ai besoin d'orientation. Il me semble, même si je ne veux pas préjuger du travail du comité, que nous étions tous d'avis que nous devons tous être à l'abri de menaces de toutes sortes ou de tentatives d'intimidation dans l'exécution de notre travail en tant que parlementaires. Je pense qu'il est fort probable que nous nous mettrons tous d'accord là-dessus assez rapidement.

Je ne comprends toujours pas ce que nous allons faire pour déterminer qui est le coupable dans ce cas-ci. Je reconnais que cela n'est pas habituel, et qu'à maintes reprises lors de questions de privilège nous n'avons pas été en mesure de trouver les coupables. Je me demande si vous pouviez nous donner des conseils sur la façon dont nous pourrions mener notre enquête en tant que membres du comité afin de pouvoir assumer sérieusement nos responsabilités relativement au deuxième et au troisième point et de la façon dont nous pourrions travailler efficacement tant pour cerner le coupable que pour établir un recours.

Mme Audrey O'Brien: Merci.

La question que vous posez touche vraiment la nature même du travail du comité sur cette question. Ce n'est certainement pas une tâche facile, en partie parce que, comme l'a dit Mme Charlton, c'est une situation sans précédent étant donné que les attaques en question proviennent d'une entité inconnue. Elle porte le nom Anonymous, mais si je comprends bien, ce titre particulier ou cette marque d'identification existe dans le cyberespace; les divers regroupements de personnes à géométrie variable qui fonctionnent sous ce nom encouragent les personnes qui veulent manifester de diverses façons à le faire en utilisant ce titre.

Je serai très franche si vous le permettez, je ne pense pas qu'il y ait beaucoup d'avantages à essayer d'identifier le coupable en tant que tel. Je pense que cet exercice — et dans ce sens je suis très heureuse que nous ne soyons pas en séance à huis clos ce qui nous permet de parler librement — est très utile puisqu'il donne à chacun la possibilité de se rendre compte que pour tous les avantages et tout ce qui a d'extraordinaire... Je me souviens avoir lu quelque part quelqu'un qui disait que Internet c'était comme avoir la bibliothèque d'Alexandrie à sa disposition.

C'est très bien en soi, mais il y a également l'envers de la médaille, c'est-à-dire que les gens qui veulent commettre des méfaits ou s'adonner à certaines activités, comme ceux faisant partie du groupe Anonymous qui profèrent des menaces... Internet leur donne également la possibilité.

Le sergent d'armes et moi discutions de cette question ce matin lorsque nous nous sommes réunis les trois avant de comparaître devant vous, et il me rappelait que menacer un fonctionnaire est un acte criminel. Je suppose que le ministre de la Sécurité publique a parlé à qui de droit pour ce qui est d'une enquête appropriée menée par les services policiers.

Quant au comité, honnêtement je ne suis pas certaine que le fait de vouloir trouver un coupable ne serait pas une immense perte de temps parce que je pense que ces attaques — d'après ce que j'en comprends suite à mes lectures — sont extrêmement fluides. Ce n'est pas comme si, par exemple dans la situation de Wikileaks, il y avait un Julian Assange qui est la tête dirigeante de cette organisation et assume la responsabilité de cette approche à l'information... Il s'agit ici d'un groupe de personnes qui, en guise de manifestation je suppose, cherchent essentiellement à causer des problèmes à diverses institutions. Il y a tout un côté anarchique très sombre à cette affaire.

Parallèlement, je pense qu'il est important pour le comité de reconnaître et de féliciter les citoyens informés qui utilisent Internet de nombreuses façons ainsi que les médias sociaux pour discuter de questions politiques et pour prendre position ou faire valoir leur point de vue dans un sens ou dans l'autre. L'engagement — il s'agit d'un engagement au-delà de l'espace et du temps — que permet Internet est quelque chose qu'il faut louer. Nous ne devrions pas permettre aux gens qui veulent s'en servir pour faire le mal, faute d'une meilleure expression, d'emporter la bataille. Ça c'est une chose.

Pour ce qui est des recours, je pense que la sensibilisation est l'élément le plus important, à savoir que si vous utilisez WiFi dans un café et que vous naviguez sur Internet, vous êtes plus susceptible d'être vulnérable à des attaques que si vous ne faites que visiter de nouveaux sites.

Je ne sais pas si cela répond complètement à votre question, mais voilà ce que j'en pense.

● (1140)

Mme Chris Charlton: Sauf votre respect, pour ce qui est des recours, dans ce cas-ci le ministre n'a pas utilisé le WiFi d'une façon inappropriée. Une vidéo YouTube a été téléchargée, et elle aurait pu l'être de toute façon sans WiFi.

Mme Audrey O'Brien: Oui tout à fait. Je pense que je faisais un lien à la conversation antérieure sur le piratage.

Mme Chris Charlton: Comme je l'ai dit, j'ai une opinion bien arrêtée sur le fait que je devrais pouvoir faire mon travail sans faire l'objet de menaces ou d'intimidation, mais je crois tout aussi fermement à la liberté d'expression. Comme vous l'avez dit, cela peut faire l'objet d'une conversation très dynamique.

Donc, pour ce qui est des recours, je ne pense pas qu'il s'agisse de dire « n'allez pas dans des cafés Internet. » Je pense que si des recours existent, ils prendraient une forme tout à fait différente.

Je pense que mon temps est écoulé et je le regrette. Peut-être pourrons-nous continuer cette...

Mme Audrey O'Brien: Veuillez m'excuser. Je pense que j'ai parlé un peu trop longtemps, comme j'ai tendance à le faire.

Vous avez absolument raison, et je ne voulais pas banaliser ces questions en disant qu'il suffisait d'éviter le Wi-Fi. Mais dès qu'on songe à limiter ce qui passe sur YouTube, on aborde la question de la liberté d'expression que je vous laisse le soin de régler.

Le président: Merci.

Merci, madame Charlton.

Monsieur Garneau, vous avez sept minutes.

[*Français*]

M. Marc Garneau (Westmount—Ville-Marie, Lib.): Merci, monsieur le président.

Je remercie également les invités qui sont parmi nous aujourd'hui.

En résumé, le Président a reconnu qu'il y avait, de prime abord, matière à question de privilège. Je ne remets certainement pas en cause la décision qui a été prise. Ça a donné lieu à la motion suivante:

> Que la question des menaces, des entraves et de la tentative d'intimidation à l'endroit de l'honorable député de Provencher soit renvoyée au Comité permanent de la procédure et des affaires de la Chambre.

Franchement, je me gratte la tête depuis le 6 mars dernier, soit depuis cette décision. Je la respecte, assurément. Lors de mon intervention, j'ai dit qu'il était important que la GRC s'implique immédiatement parce qu'il y avait clairement eu une menace. Nous reconnaissons tous qu'il s'agit là d'un geste criminel et méprisable. Or je me suis demandé ce qu'on pouvait faire de plus.

Vous avez peut-être très bien résumé la chose en disant que le fait d'être menacé de temps en temps était inhérent à notre profession. Le premier ministre, par exemple, est continuellement entouré physiquement à des fins de protection.

[*Traduction*]

Nous savons également qu'à certaines occasions, des ministres ont dû être protégés en raison d'un projet de loi particulier. Cela fait partie de notre travail, et je pense que c'est ce que j'ai essayé de mentionner lorsque je suis intervenu avant que la décision n'ait été prise. Cela fait partie de notre travail d'une certaine façon, et c'est quelque chose que nous, et en particulier les ministres du Cabinet qui déposent des projets de loi, devons savoir et accepter.

Alors, que peut-on faire dans ces circonstances? Vous avez parlé de sensibilisation à ce qui peut nous arriver et de la protection de l'accès à notre documentation sur Internet et ainsi de suite.

Soit dit en passant, hier quelqu'un a piraté mon compte Twitter. Je devais être fatigué, mais je pense être tombé dans un très vieux piège avant de me rendre compte que des gens s'adonnent à ce genre d'activité. Nous devrions être mieux au courant de ce genre de chose, cela ne fait aucun doute.

Il me semble que vous dites également que nous pouvons réagir dans des cas particuliers et voir ce qui peut être fait et quelles pourraient être les mesures appropriées. Entre-temps, cela fait, dans une certaine mesure, partie du travail; même si nous voulons protéger les parlementaires le plus possible, il n'y a pas de solution miracle.

Si Anonymous, pour quelque raison prodigieuse — et je doute que cela ne soit le cas — était appréhendé et démantelé, d'autres prendraient sa place. Il y a les groupes OpenMedias et Leadnows qui font état de leur désaccord avec les décisions du gouvernement, mais ils le font démocratiquement; et puis il y a ces autres groupes comme Anonymous. Mais ils sont nombreux, et c'est le reflet du XXI^{e} siècle.

Alors, que pouvons-nous faire — je pose la même question qui a été posée par les autres — à part se renseigner et être très prudents?

● (1145)

[*Français*]

Mme Audrey O'Brien: Monsieur le président, la description que M. Garneau fait de la situation est, à mon avis, très appropriée.

[*Traduction*]

Vous avez dit que votre compte Twitter a fait l'objet de piratage. Ce qui est important de savoir, c'est que lorsque vous êtes sur Twitter, vous n'êtes plus sur un réseau protégé, n'importe quoi peut donc arriver. Voilà le volet plus sombre des médias sociaux.

[*Français*]

Pour ce qui est de la question de privilège soumise au comité, selon ce que je comprends des interventions, tout le monde, peu importe le parti politique, est d'accord pour dire qu'en émettant ces menaces, le groupe Anonymous a franchi certaines limites. Il s'agit ici de dire qu'en tant que députés, vous menez une vie publique, et que dans ces conditions, vous êtes prêts à assumer le fait qu'on attaque vos positions politiques, etc., mais que les menaces proférées à l'endroit d'une personne ne sont pas acceptables. Je sais que cette déclaration peut sembler ne mener à rien, mais il est important, selon moi, que tout le monde s'unisse pour dire que

[*Traduction*]

Il y a des limites à ne pas franchir.

Le président: Monsieur Hawn, vous avez quatre minutes.

L'hon. Laurie Hawn (Edmonton-Centre, PCC): Merci, monsieur le président.

Merci à vous d'être là.

Monsieur Bard, j'aurais besoin d'explications. Vous avez dit que 70 p. 100 des courriels adressés à la Chambre des communes n'arrivent jamais à nos ordinateurs. Eh bien, d'abord je vous en remercie. Nous vous en sommes reconnaissants.

Des voix: Oh, oh!

L'hon. Laurie Hawn: C'est un pourcentage très élevé. S'agit-il uniquement de pourriels? En quoi consistent ces messages?

M. Louis Bard: Cela pourrait être du pourriel. Il existe de nombreux règlements. Le courriel doit d'abord être valide, il doit être bien adressé et avoir un véritable destinateur. On ne peut pas envoyer un courriel en l'adressant seulement au « Parlement »; il doit être adressé à un parlementaire. Également, on ne peut pas remplacer le nom de l'expéditeur. Le message ne peut pas faire l'objet d'un envoi collectif.

Nous avons établi toute une série de règlements au fil des ans, en fonction des pratiques exemplaires de l'industrie, et nous les avons appliquées pour faire en sorte de ne pas corrompre ni remplir vos boîtes postales de courriels non voulus qui n'ont aucun sens.

L'hon. Laurie Hawn: C'est excellent.

Nous pourrions tous poser la même question pour faire valoir notre point de vue. Tout le monde est en faveur de la libre expression. Même si je ne suis pas d'accord avec quelqu'un, je reconnais le courage de cette personne qui est prête à s'exprimer sur telle ou telle question, tout en s'identifiant. Je pense que l'on peut dire sans équivoque qu'Anonymous est un couard. Je n'ai que du mépris pour quiconque ou quelconque organisation qui exploite la liberté d'expression de cette façon.

Manifestement, l'extorsion est un crime, j'espère que la GRC ou quiconque.... Comme Marc l'a dit, ils sont comme les talibans: il y en aura toujours et ils seront toujours là. Mais, je pense que nous devrions faire tout ce qui est possible pour en retracer un et en faire un exemple, et j'espère que c'est ce qui se produira.

Monsieur Bard, nous avons parlé de la façon dont les choses étaient établies dans les circonscriptions, et vous avez des conseils à cet égard. Serait-il utile de profiter de votre bonne volonté et de demander à ce que quelqu'un vienne dans nos bureaux de circonscription voir ce qui en est en matière de protection? Je sais que nous sommes 308 et que cela pourrait être coûteux, mais est-ce que ce serait une solution envisageable?

● (1150)

M. Louis Bard: Oui. Nous offrons ce service — on n'envoie pas quelqu'un dans votre bureau local, mais quelqu'un peut offrir des conseils et travailler avec votre personnel du bureau pour donner les conseils appropriés.

L'hon. Laurie Hawn: Au risque de déformer vos propos, est-ce que les 308 députés devraient procéder ainsi, s'ils ne l'ont pas déjà fait?

M. Louis Bard: Eh bien, c'est vraiment au député de le demander. Je dirai que si vous n'avez pas élaboré pour votre bureau ce type de plan, des stratégies de gestion de la continuité des opérations, comment protégez-vous votre environnement? Comment donnez-vous accès à votre réseau à vos bénévoles? Comment savez-vous que c'est la bonne personne que vous appelez lors d'un appel conférence? Il y a tant de choses à contrôler.

Je dis toujours que mes meilleurs clients sont les députés et mes plus grands risques sont les députés, leur personnel et les employés de la Chambre.

L'hon. Laurie Hawn: Oui, certainement.

Voici une question technique, pour revenir à Anonymous et YouTube. YouTube peut techniquement identifier qui a téléchargé les vidéos sur le site. Est-ce vrai ou pas?

M. Louis Bard: Je pense qu'il s'agit là de la difficulté, parce que ceux qui agissent au nom de « Anonymous » sont très créatifs. Vous pouvez recevoir quelque chose de Chine qui provient d'ici à Ottawa. Ils se spécialisent dans le balayage de l'environnement pour identifier les faiblesses et les vulnérabilités des technologies; voilà ce qu'ils font. Très souvent, ils font faire leur sale boulot par d'autres. Ils fourniront la porte ouverte, la possibilité d'afficher quelque chose pour activer un script.

C'est une situation très complexe. Nous avons vu des cas aux États-Unis où cela a pris plus de deux ans pour finalement en identifier cinq. Mais il a fallu deux ans pour les trouver, et ce groupe est en mutation constante. Chaque jour, c'est une tâche difficile. Le problème dépasse les frontières du Canada; il est à l'échelon mondial.

L'hon. Laurie Hawn: Oui, et sans entrer dans les méthodologies, est-ce que des organisations comme le CSTC ont la capacité de remonter ces liens, que cela vienne de la Chine ou d'ailleurs? Ont-ils la capacité technique de le faire?

M. Louis Bard: Oui.

Le président: Je suis désolé, mais votre temps est écoulé.

Monsieur Comartin.

M. Joe Comartin (Windsor—Tecumseh, NPD): Merci, monsieur le président.

Je remercie les témoins d'être ici.

Je veux poursuivre au sujet de l'identification du coupable dans le cadre de ce que notre personnel... C'est peut-être une question qui s'adresse à M. Vickers, ou peut-être M. Bard, mais je pense qu'elle s'adresse plutôt à M. Vickers. Il y a eu quelques réussites au cours des deux dernières années, en Angleterre et aux États-Unis, nous en avons eu un exemple aussi récemment qu'il y a une semaine aux États-Unis, pour identifier et poursuivre Anonymous ou d'autres personnes — je ne pense pas qu'on peut dire qu'ils sont un groupe — qui se cachent derrière ce masque. Je ne sais pas s'il y aura des condamnations, mais il y a une série d'incidents pour lesquels on a déposé des accusations au cours de la dernière année ou deux.

Avons-nous — est-ce que la Chambre a — des liens avec les forces policières? Dans une situation comme celle où se trouve le député de Provencher, où un tel lien serait nécessaire, existe-t-il un protocole par lequel on active ces liens pour s'assurer que nos forces policières fassent enquête sur l'incident? De plus, étant donné le cas le plus récent d'identification par le FBI aux États-Unis, vérifions-nous si nos forces policières sont en contact avec eux pour voir s'ils peuvent nous fournir des ressources pour identifier le coupable afin de l'accuser?

Mme Audrey O'Brien: Monsieur le président, je vais donner la parole au sergent, qui en sait évidemment plus sur les discussions entre les forces policières. Je pense que nous avons une très bonne relation de travail avec les autorités et nous en profitons. Toutefois, je pense que la Chambre en tant qu'institution, que nous en tant qu'administration de la Chambre, ne demandons pas une enquête sur un cas particulier.

Kevin peut peut-être vous expliquer comment les policiers réagiraient et ce qui les feraient lancer une enquête.

● (1155)

M. Kevin Vickers (sergent d'armes, Chambre des communes): Habituellement, monsieur Comartin, nous avons des contacts quotidiens avec nos partenaires en matière de sécurité. Évidemment, à titre de sergent d'armes, je suis responsable de votre sécurité à tous, alors si quelque chose est portée à mon attention, quelle qu'elle soit, nous faisons toujours ce qui est approprié afin que le suivi adéquat soit effectué. C'est également vrai dans ce cas.

M. Joe Comartin: Alors au sujet de la situation concernant le ministre de la Sécurité publique, y a-t-il eu une plainte officielle déposée, que cela soit auprès de la GRC ou d'un autre service de police? Est-ce que cela s'est fait?

Mme Audrey O'Brien: Monsieur le président, le sergent préférerait ne pas entrer dans les détails d'un cas spécifique publiquement. Je pense que l'on peut dire, cependant, que l'administration de la Chambre ne serait pas en position de déposer ce type de plainte — je voulais simplement le clarifier.

M. Joe Comartin: Bien.

De façon plus générale, monsieur Vickers, vous dites que vous êtes en contact régulier avec les autres forces policières. Peut-être que M. Bard est aussi au courant. Au sujet de ces incidents pour lesquels on a déposé des accusations, en Angleterre et aux États-Unis, est-ce que notre personnel suit le développement de ces accusations pour voir quel a été le résultat?

M. Kevin Vickers: Si je savais qu'un député a été menacé, je m'assure que le suivi adéquat est fait auprès de ce député. Mon personnel et moi nous nous tiendrons au courant de l'affaire jusqu'à ce que la situation soit résolue d'une façon ou d'une autre.

Mme Audrey O'Brien: Si vous me le permettez, monsieur le président, je pense qu'il serait exagéré de dire que nous surveillons le résultat des enquêtes menées aux États-Unis ou au Royaume-Uni. Mais nous nous garderons certainement informés des développements.

M. Joe Comartin: Pour la population en général, pourrions-nous nous attendre à ce qu'ils surveillent le plus récent cas aux États-Unis, qui, je crois, représente une percée assez importante quant à la capacité de suivre Anonymous en particulier?

Je suis désolé, je devrais peut-être expliquer ce que je recherche. L'une de nos responsabilités est d'essayer d'identifier le coupable. Je cherche des sources qui pourraient aider notre comité dans cette quête, en tenant compte de ce que vous avez dit, madame O'Brien.

Le comité n'a pas du tout la capacité d'identifier le coupable. Cela devra être fait par quelqu'un d'autre. Alors j'essaie de voir si cette aide pourrait provenir directement de nos forces policières ou de leurs liens avec les services policiers d'autres pays.

Mme Audrey O'Brien: Je pense que le sergent peut probablement vous répondre.

M. Kevin Vickers: Monsieur le président, je peux vous assurer que nous, la Chambre, demeurons en contact dans le cadre de nos pratiques et nos procédures générales. Dans le cas précis d'Anonymous, je suis au courant des succès récents que vous avez mentionnés.

Je sais également que la Gendarmerie royale du Canada est considérée comme ayant des compétences de classe mondiale pour ce genre d'enquête. Elle collabore étroitement avec d'autres partenaires en matière de sécurité partout dans le monde pour de telles enquêtes. Il pourrait être utile au comité d'inviter à un moment donné ces experts de la GRC afin qu'ils vous donnent des renseignements pertinents.

Autant que je sache, ces compétences existent. Comme vous l'avez souligné, des exemples récents montrent que, suite à des enquêtes criminelles, les responsables ont pu être identifiés.

Le président: Merci.

Merci, monsieur Comartin. Je vous ai donné beaucoup de temps parce que le président était très intéressé aux réponses également.

Monsieur Albrecht, veuillez être aussi intéressant, s'il vous plaît.

M. Harold Albrecht (Kitchener—Conestoga, PCC): Oh, monsieur le président, je ne peux pas vous le garantir, ayant travaillé avec M. Comartin.

Merci, monsieur le président, et merci à nos témoins d'être ici.

Alors que j'examine ce cas pour essayer de le comprendre, il me semble qu'il y a trois niveaux de préoccupation. L'un concerne la Cité parlementaire.

Monsieur Bard, merci de nous assurer que beaucoup de courriels qui nous sont destinés n'arrivent pas, puisqu'ils poseraient problème.

Le deuxième niveau, c'est le bureau de circonscription. Je me souviens que, lorsque nous avons mis en place notre bureau de circonscription, nous avons reçu une très bonne trousse de matériel, avec des bons renseignements et de bonnes instructions. En fait, je pense qu'il y avait des pratiques clairement interdites que l'on ne devait pas utiliser. Je pense que c'est une bonne chose.

J'ai maintenant une préoccupation, après vous avoir entendu aujourd'hui: est-ce que cela est surveillé de façon régulière, ou devrais-je être proactif, en tant que député, pour demander de l'aide dans mon bureau de circonscription afin que cela se fasse de façon régulière et qu'il soit aussi sécuritaire qu'au départ?

Ma troisième question — je vais toutes les poser et vous pourrez peut-être répondre brièvement à chacune — concerne une autre préoccupation que nous partageons probablement tous. Qu'en est-il de nos ordinateurs personnels? Qu'en est-il des ordinateurs de nos familles? Qu'en est-il des ordinateurs personnels de nos collaborateurs? Y a-t-il des mesures préventives que nous devrions connaître et mettre en oeuvre individuellement? Et si c'est le cas, êtes-vous disponible pour nous aviser sur ces questions également?

Des voix: Oh, oh!

M. Harold Albrecht: Je suis maintenant allé trop loin.

● (1200)

M. Louis Bard: C'est une question qui coûte très, très cher.

Des voix: Oh, oh!

M. Louis Bard: Non, non, il n'y a aucun doute que nous travaillons toujours très fort sur nos campagnes de sensibilisation pour les députés, en vous fournissant des trousses de renseignements, des documents, pour faire votre inventaire et évaluer vos ordinateurs. Nous avons des cliniques pour les portables. Lorsque vous revenez de l'intersession de l'été, nous surveillons les chambres afin d'être certain que vous ne nous ramenez pas de surprises de vos circonscriptions sur vos portables. Nous essayons de prendre de l'avance et d'être en mesure de vous aider autant que possible.

Cependant, vous êtes la personne qui dirige le bureau de circonscription, alors vous devez avoir ces pratiques exemplaires pour refaire votre évaluation de risque, revoir régulièrement la trousse afin d'être certain de comprendre les risques et les problèmes s'il y a des menaces ou autres choses du genre. Et oui, nous pouvons toujours vous aider avec cela.

Le même type d'exercice peut s'utiliser avec votre famille. Vous pouvez utiliser le même matériel afin de mettre en place des mesures de sécurité dans votre maison, parce que les mêmes questions s'y appliquent. Est-ce que vous avez une bonne protection? Mettez-vous à jour votre antivirus? Il y a toutes sortes de choses que vous pouvez faire. Comment faites-vous vos transactions bancaires, et qui y a accès?

M. Harold Albrecht: Je vous remercie pour l'aide que votre direction nous offre, chaque fois que nous revenons de nos circonscriptions, afin d'examiner nos portables. J'en ai toujours profité, et je crois que c'est très utile.

Y a-t-il un processus semblable qui encouragerait le personnel de nos bureaux de circonscription à effectuer un processus d'examen semblable régulièrement afin d'être certain que...? Ou est-ce que les députés doivent être proactifs eux-mêmes?

M. Louis Bard: Si les députés le veulent, je peux vous donner une trousse que vous pouvez utiliser pour évaluer votre situation. Nous pouvons trouver des façons de réévaluer la situation régulièrement afin qu'on vous rappelle de le faire.

M. Harold Albrecht: Je ne sais pas à quelle fréquence cela se ferait, mais si « régulièrement », nous recevions des mises à jour et des recommandations de votre bureau et peut-être une offre d'examiner à distance ce que nous faisons ou ne faisons pas, je trouverais cela utile.

Merci, monsieur le président.

Le président: Merci beaucoup.

Monsieur Lukiwski.

M. Tom Lukiwski: Merci.

Je veux revenir un instant à la question de la vulnérabilité. Je vous remercie pour tout ce que vous faites et continuez de faire lorsque nous sommes dans la Cité parlementaire, mais que se passe-t-il lorsque nous en sortons? Évidemment, les ministres voyagent beaucoup à l'étranger, et les députés également. Nous avons des associations parlementaires qui sont toujours à l'étranger. À quel point les députés sont-ils vulnérables à l'extérieur de la cité? Nous devons demeurer en contact. Dans le cas des ministres, il y a beaucoup de travail parlementaire qui se fait, qu'ils soient à Ottawa, en Chine ou ailleurs. À quel point les députés qui voyagent à l'étranger sont-ils vulnérables?

M. Louis Bard: Je pense qu'il y a un niveau élevé de vulnérabilité, surtout si vous voyagez à l'étranger, parce qu'ils savent que vous venez et qu'ils arriveront à vous surveiller ou observer qui sera là et vous suivre pendant votre visite. C'est pourquoi le choix des technologies que vous utilisez lors de voyages est si important. Par exemple, si vous apportez des documents confidentiels, des documents secrets, sur votre portable, vous êtes très vulnérable si vous le perdez, si vous n'avez pas protégé les documents, chiffré les documents, codé les documents, imperméabilisé les documents: il y a tant de choses que l'on peut faire pour protéger un document. Moi, je n'emporte pas de documents secrets lorsque je voyage. Je trouve d'autres façons de transférer les documents.

● (1205)

M. Tom Lukiwski: Y a-t-il des protocoles spécifiques que vous suggéreriez pour les députés qui voyagent à l'étranger ou bien seront-ils vulnérables quoi qu'ils fassent? Beaucoup de mesures relèvent du gros bon sens, nous le savons. Mais y a-t-il des protocoles ou des dispositions particulières que vous nous suggéreriez ou que vous étudiez puisqu'on est peut-être maintenant la cible d'Anonymous ou d'autres groupes?

M. Louis Bard: Je dirai exactement ce que j'ai dit l'an dernier lorsque nous examinions l'élaboration des rapports du comité. Souvent, l'un des problèmes de sécurité, c'est que les gens n'évaluent pas ce qu'ils prévoient faire pendant leur voyage. Vous devez vraiment évaluer les risques avant de partir, et alors vous pouvez mettre en place les mesures nécessaires qui vous aideront, grâce à des trousses spéciales, des outils spéciaux, ou des téléphones spéciaux ou des BlackBerry. On peut faire toutes sortes de choses pour éviter les risques: ne pas utiliser de téléphone cellulaire, utiliser une ligne terrestre... Comme mesure préventive, avant votre départ, nous devons comprendre le but de votre voyage et ce que vous prévoyez faire, et ainsi, selon les risques, nous pouvons vraiment trouver des solutions.

Le président: Il vous reste une minute.

M. Tom Lukiwski: Merci beaucoup.

Est-ce que des systèmes informatiques des députés ont déjà été piratés? Si oui, que faites-vous dans une telle situation?

M. Louis Bard: Nous faisons la même chose que dans le cadre des politiques des TI sur l'utilisation acceptable de façon régulière.

C'est déjà arrivé pour un caucus, pour le serveur Web de votre caucus. Nous avons aidé nombre d'entre vous avec vos serveurs de caucus lorsqu'il y a eu une infiltration, une corruption, des pourriels, et d'autres choses semblables. C'est arrivé à cause de portables de députés qui avaient été infectés par des virus.

Lorsque nous détectons quelque chose, nous commençons par informer le député, ensuite nous demandons la permission de retirer l'ordinateur personnel ou le portable afin de corriger la situation très rapidement. Nous le faisons sur une base personnelle et privée avec chaque député. Si nous remarquons un problème, nous essayons de trouver un compromis et d'identifier les menaces. S'il n'est pas possible de trouver une solution avec le député, je contacterai le whip. Voilà le protocole.

J'ai vu beaucoup d'exemples au cours des 19 dernières années, mais je dois dire qu'à chaque fois nous avons pu corriger la situation à la satisfaction du député. Jamais au cours des 19 dernières années n'avons-nous perdu l'accès à notre réseau, été paralysés pendant des jours ou été obligés de fermer le réseau. Touchons du bois — nous n'avons jamais procédé à une interruption du service.

Le président: Merci.

Passons maintenant à Mme Charlton. Et je crois que vous allez partager votre temps de parole avec Mme Latendresse.

[*Français*]

Mme Alexandrine Latendresse (Louis-Saint-Laurent, NPD): Merci, monsieur le président.

Tout d'abord, je vous remercie de vos informations très utiles.

J'ai une question qui s'adresse spécifiquement à Mme O'Brien au sujet des atteintes au privilège, comme cela a été le cas ici.

J'ai lu dans votre excellent ouvrage que dans le cas où — et c'est déjà arrivé par le passé — on reconnaît qu'il y a eu atteinte au privilège, mais qu'aucun moyen ne permet d'identifier qui en est à la source, rien de plus ne peut être fait. On reconnaît qu'il y a eu atteinte au privilège, et c'est tout.

Dans le cas présent, c'est assez clair qu'il y a eu atteinte au privilège, étant donné que le ministre a reçu des menaces spécifiquement liées à son travail. En effet, on lui demandait de retirer le projet de loi. Cela étant dit, je pense qu'Anonymous, comme on l'a dit précédemment, est quelque chose d'intangible. On ne peut même pas dire que c'est une organisation, parce que n'importe qui peut prétendre être Anonymous et apposer cette étiquette sur ses actions. Ce n'est pas un groupe organisé qui a des actions concertées ou des choses comme cela.

Dans le cas présent, ne sommes-nous pas dans cette situation où, puisque nous ne pourrons pas trouver qui est à l'origine de cela, il sera impossible d'y donner suite?

● (1210)

Mme Audrey O'Brien: Monsieur le président, je pense que Mme Latendresse a entièrement raison. Je vois mal comment vous pourriez identifier la personne ou les personnes qui sont responsables des menaces qui ont été proférées contre le ministre.

Comme vous le dites si bien, parce que ce n'est même pas un groupe organisé, n'importe qui peut utiliser le nom d'Anonymous, ce qui est même encouragé par les gens qui font le marketing de cette entité. À mon avis, on ne peut pas faire grand-chose à cet égard.

Par contre, je suis une personne dévouée à l'institution du Parlement. Si je me fie à la discussion de ce matin, tout le monde semble d'avis, comme je le disais plus tôt à M. Garneau, qu'une limite a été franchie par Anonymous. On passe aux menaces, ce qui est inacceptable.

Une des choses que j'ai apprises ce matin est que le groupe, apparemment, parraine certains sites Web malicieux. Si vous vous opposez à tel ou tel projet de loi, on vous donne des instructions pour faire part de votre opposition. En fait, on ne vous aide pas vraiment à envoyer un courriel au ministre pour lui signifier votre désaccord, mais on vous fait envoyer quelque chose qui, soudainement, déclenche un processus malicieux. Certaines personnes opposées à un projet de loi, qui sont peut-être de bonne foi et qui voudraient faire connaître leur opposition, risquent malheureusement de se faire prendre par de tels sites.

Je le répète, il faut faire de l'éducation. Il serait important qu'un rapport du comité puisse indiquer aux citoyens qu'on veut qu'ils soient engagés et qu'ils participent au débat politique, mais qu'il ne faut pas se laisser prendre par des choses qu'ils ne comprennent peut-être pas. Il faut faire attention. Signer des pétitions et envoyer des courriels, ça va. Cependant, cela n'est pas toujours aussi simple.

J'aimerais clarifier le point suivant. M. Bard dit que 70 p. 100 des courriels ne sont pas acheminés vers les parlementaires. Il est important de préciser ce qu'est une campagne de courriels, qui se fait à l'échelle de certains comtés ou de certaines régions et qui est tout à fait légitime. Je parle de courriels qui comportent une adresse: cela est acceptable. Cependant, quand une adresse n'est pas identifiable, on a un cas qui fait partie des 70 p. 100. Je ne voudrais pas qu'on croie que plusieurs courriels sur un sujet quelconque ne se rendront pas parce qu'on décide de faire le ménage.

Mme Alexandrine Latendresse: En effet, tous les députés reçoivent beaucoup de ces courriels, qui sont légitimes.

● (1215)

Mme Audrey O'Brien: C'est exact.

Mme Alexandrine Latendresse: Merci.

[*Traduction*]

Le président: Merci.

Monsieur Zimmer.

M. Bob Zimmer (Prince George—Peace River, PCC): Merci monsieur le président.

Merci d'être venus aujourd'hui. Je suis content que vous soyez ici.

Pour le bénéfice de la population, je pense qu'il y a vraiment deux enjeux ici. L'Intimidation en ligne, comme je l'appelle, et la sécurité.

Je parlerai plus précisément de l'intimidation en ligne. Je pense que la population a une certaine perception de nous, les politiciens, comme étant inaccessibles. J'ai un compte Twitter. J'ai un compte Facebook. Je pense qu'il y a une certaine perception, surtout de la part d'Anonymous — et je n'ai jamais discuté avec Anonymous auparavant — qu'il semble y avoir une escalade. J'invite la population à dialoguer avec nous. Nous sommes accessibles. Lancez la discussion, plutôt que de passer à des activités plus extrêmes immédiatement. Je les inviterais à faire cela.

J'ai cependant une question sur la sécurité. Nous sommes Canadiens et nous avons de bons systèmes de sécurité, mais est-ce que nous consultons d'autres organisations — la CIA, le FBI et Scotland Yard — pour savoir ce qu'ils font? Avons-nous ce type de discussion?

Mme Audrey O'Brien: Je vais donner la parole au DPI dans un instant, mais je vais d'abord vous dire que je suis complètement d'accord avec vous. L'idée d'avoir une discussion et un dialogue avec nos représentants politiques, que ce soit pour appuyer ou décrier une mesure, est totalement louable.

Je pense que M. Hawn a très bien décrit les gens qui font ce type de menaces, comme Anonymous: c'est quelque chose de lâche.

M. Bob Zimmer: Exact.

Mme Audrey O'Brien: Ça n'a rien à voir avec une réelle participation politique.

Quant à l'intimidation en ligne et la sécurité, j'ai dit plus tôt que la sécurité, le Centre de sécurité des télécommunications, est l'organisation au Canada qui a comme tâche d'examiner plus précisément les cybermenaces. Il fait évidemment partie d'un réseau international avec les Américains et le Royaume-Uni.

Grâce à nos contacts directs avec le CST, nous sommes au courant des pratiques exemplaires qui sont élaborées, partout dans le monde, car je crois que chaque parlement essaie de trouver l'équilibre entre l'accessibilité et l'ouverture, et ce type de mauvaises situations posées par des groupes comme Anonymous.

Louis, peut-être voulez-vous ajouter quelque chose.

M. Louis Bard: Comme Mme O'Brien l'a indiqué, il est clair que le CST est l'organisation principale avec laquelle nous travaillons, à cause de son rôle. Le CST nous a beaucoup aidés pour choisir nos technologies, pour la surveillance, et d'autres choses, et il nous informe également de ce qui se passe. Il y a aussi la GRC, et d'autres organisations du gouvernement fédéral, comme la DGSIT et tous les services partagés ainsi que d'autres éléments, qui sont utiles.

En même temps, je me concentre plutôt sur les outils et les moyens, et nous discutons avec toutes sortes d'entreprises partout dans le monde pour comprendre ce qui se passe. De plus, nous avons visité d'autres parlements et d'autres institutions. Je suis même allé avec M. Vickers visiter certaines organisations de sécurité aux États-Unis pour comprendre leurs activités. Nous faisons tout ce que nous pouvons. Chaque jour, nous examinons chaque renseignement et chaque document que nous pouvons trouver.

M. Bob Zimmer: Merci.

J'ai une dernière question qui provient d'un collègue. Nous aimerions savoir s'il est possible pour des pirates d'insérer quelque chose sur un ordinateur. Est-ce possible? Cela pourrait être de faux renseignements, un faux document, ou quelque chose comme ça. J'imagine que cela serait un peu comme un virus. Est-ce possible de faire une telle chose?

M. Louis Bard: Il est certain que tout est possible, par des pièces jointes ou d'autres façons. Nous avons constaté des structures d'infection très complexes. Par exemple, les pirates se connecteront à votre ordinateur personnel et essaieront d'établir d'autres connexions, ou d'importer d'autre matériel, ou copier ce qu'il y a sur votre bureau. On a vu toutes sortes de choses. À chaque fois, nous avons été les premiers à déceler ces incidents sur la Colline du Parlement et avons pu informer nos pairs.

Je fais attention à ne pas partir en croisade contre d'autres partenaires; ce n'est pas mon travail. Mais oui, il y a toutes sortes de possibilités. Je peux vous garantir que nous effectuons une surveillance très complète. Lorsque nous constatons des anomalies, nous contactons très rapidement les députés. Je dirais que les députés ont collaboré pleinement dans tous les cas. Les députés, les bureaux des ministres, les bureaux des whips, les caucus et les bureaux de recherche des caucus — tout le monde collabore très, très bien.

Le président: Merci.

M. Bob Zimmer: Me reste-t-il du temps?

Le président: Non, il ne vous en reste pas.

M. Bob Zimmer: Merci.

● (1220)

Le président: Merci.

Monsieur Kerr.

M. Greg Kerr (Nova-Ouest, PCC): Merci, monsieur le président.

Merci beaucoup d'être ici. C'est tout un apprentissage ce matin.

Nous avons couvert beaucoup de choses, et vos explications sont très bonnes. Il nous reste évidemment des questions ainsi que des orientations. À part ce que vous avez mentionné, y a-t-il d'autres choses que notre comité devrait faire avant de terminer son étude?

Lorsque j'entends parler de ce qui peut arriver, je me demande s'il serait à notre avantage de convoquer les représentants du secteur privé qui développent ces technologies et appareils merveilleux afin de pouvoir discuter avec eux de ce qui se fait ou pourrait se faire. Cela dépasse l'enjeu de la sécurité, mais ce sont eux qui développent l'expertise qu'on utilise. Devrions-nous songer à une telle chose?

Mme Audrey O'Brien: Je dirais, monsieur le président, à vous et à monsieur Kerr, que c'est au comité de décider ce qu'il veut faire au sujet de cette enquête, même si ce n'est que pour en apprendre plus.

Louis a dit clairement que notre rôle est d'établir des contacts avec les diverses organisations et l'industrie privée afin d'être constamment informés des développements de la technologie ainsi que de l'autre côté de la médaille, les développements des malfaiteurs. Alors même qu'un certain type d'antivirus est trouvé, des pirates essaient de le contourner, etc. Je ne sais pas si vous trouveriez ces conversations utiles.

Je peux vous donner l'assurance que notre participation à divers réseaux nous tient au courant des pratiques exemplaires et des renseignements les plus récents sur le sujet, que nous utilisons afin d'améliorer notre sécurité et d'offrir une meilleure sécurité aux députés et à la Chambre des communes.

M. Greg Kerr: Je le comprends, mais vous n'avez pas tout à fait répondu comme je l'espérais. Notre tâche est de représenter la population des diverses parties du pays d'où nous venons. C'est évidemment important pour la population, tout comme ce qui se passe au-delà de notre système de sécurité et de notre portée. C'est pourquoi je me demandais si vous croyez qu'il serait bon d'entendre les gens du domaine de la sécurité, peut-être ceux qui font affaire avec les policiers, par exemple, de même que des experts de l'industrie qui développent ces choses et si cela pourrait élargir la portée de notre étude.

Je sais que vous avez déjà répondu. Je me demandais si cela serait une bonne chose à faire avant de terminer notre étude?

Mme Audrey O'Brien: Comme je l'ai dit, je pense que c'est à vous de décider. En ce qui me concerne personnellement, vous avez ici les deux experts de la Chambre des communes dont vous avez besoin.

En ce qui a trait aux autres autorités qui existent, vous pourriez juger utile de poursuivre la séance à huis clos concernant certaines situations que vous avez connues, etc. Je ne suis pas certaine de l'orientation que le comité veut donner à son étude.

M. Greg Kerr: Nous non plus.

Merci.

Mme Audrey O'Brien: Merci, monsieur Kerr.

Le président: Merci, monsieur Kerr.

Monsieur Comartin, vous avez la parole.

M. Joe Comartin: Merci, monsieur le président.

Monsieur Bard, j'examine en ce moment les courriels qui ont été envoyés à M. Toews par Anonymous. Une adresse Web y figure. Je m'interroge au sujet de ce cas précis. Si, à titre de député, je m'adressais à vous afin de vous demander de retracer la source de ce courriel, seriez-vous en mesure de le faire, et est-ce un service que vous fourniriez à des députés?

M. Louis Bard: En ce qui a trait à toute demande émanant des députés concernant des courriels qu'ils reçoivent, si ces courriels sont reçus sur le système de courrier électronique de la Chambre des communes, nous maintenons un journal des courriels ainsi que des accès à Internet. Ces journaux sont conservés pendant un certain temps, ce qui nous permet de faire certaines enquêtes.

Par exemple, en ce qui a trait à toutes ces vidéos sur YouTube auxquelles vous avez fait référence, il ne fait aucun doute que nous avons exercé la diligence voulue afin d'examiner les environnements informatiques, et je peux vous affirmer qu'aucune de ces vidéos n'a été affichée à partir d'un ordinateur de la Chambre des communes. C'est très clair.

C'est la portée de ce que l'on peut faire. Si l'on sort des limites de la Chambre des communes et que l'on va à l'extérieur, je n'ai pas accès à ces outils.

● (1225)

M. Joe Comartin: Avons-nous un protocole à la Chambre des communes avec le CSTC pour leur demander de le faire?

Laissez-moi simplement vous dire que je sais, d'après mon expérience au sein du ministère de la Sécurité publique, et à la lumière des travaux que nous avons effectués concernant les sites de pornographie juvénile afin d'en retracer la source, qu'au moins une partie de cette technologie est disponible. En toute franchise, le CSTC est l'une des meilleures agences dans le monde pour retracer les sources. Donc, avons-nous un protocole avec eux qui nous permet, si vous n'êtes pas en mesure de retracer la source, de leur demander de le faire?

M. Louis Bard: Je peux certainement répondre à la première partie de votre question.

Le CSTC n'a pas vraiment d'autorité sur la Colline parlementaire. Cependant, il coopérera, sur demande, afin de m'aider à gérer mon environnement. Si cela va au-delà de la surveillance ou de la gestion de l'enceinte parlementaire, si cela relève du domaine criminel, cela dépasse mon champ de compétence, et je m'en remettrais à Kevin pour ce qui est de ces questions.

M. Joe Comartin: Monsieur Vickers, avons-nous un protocole avec le CSTC dans les cas où nous soupçonnons qu'il y ait eu une activité criminelle et que nous souhaitons retracer l'origine d'un courriel?

M. Kevin Vickers: Tout d'abord, monsieur Comartin, le mandat du CSTC est très, très précis. Cette agence doit se conformer à des dispositions législatives très contraignantes... qui définissent ce qu'elle peut faire et ne peut pas faire, plus particulièrement si cela touche des citoyens canadiens.

La GRC, par exemple, serait une autorité compétente et aurait des liens internationaux. Dans le cas que vous venez de mentionner, par exemple, à savoir, la pornographie juvénile, la GRC pourrait essayer d'enquêter, si elle a une adresse IP, afin de déterminer la source qui distribue ces pornographies juvéniles, tout comme ce serait le cas pour des vidéos distribuées sur YouTube.

Donc, cela existe. Comme vous l'avez dit plus tôt, certains cas ont été des réussites. Le greffier l'a mentionné, le monde dans lequel ces individus exercent leurs activités est très compliqué et sophistiqué, et les choses deviennent de plus en plus difficiles, mais comme vous l'avez indiqué, il y a un certain nombre d'exemples de réussite.

Mme Audrey O'Brien: Peut-être que...

M. Joe Comartin: Désolé, madame O'Brien; mon temps va bientôt être écoulé et j'aimerais déterminer clairement qui est responsable.

Si je pense avoir été victime d'un acte criminel, dois-je m'adresser en personne à la GRC à titre de député, ou avons-nous un protocole selon lequel vous, monsieur Vickers, ou quelqu'un d'autre de la Colline, devez le faire? Qui a la responsabilité d'entrer en contact avec la GRC pour effectuer...

M. Kevin Vickers: Il serait de votre responsabilité, à titre de plaignant, de déposer une plainte officielle auprès de la GRC.

M. Joe Comartin: Merci.

Mme Audrey O'Brien: Pour faire suite à ce que vous avez dit, lorsque M. Bard disait que si vous recevez, par exemple, un courriel sur votre compte de la Colline, et que pour quelque raison que ce soit vous souhaitez en connaître l'origine, nous pouvons vous donner ce renseignement. Ensuite, pour ce qui est de ce que vous décidez de faire de ce renseignement, si vous avez le sentiment que cela viole vos droits et que vous souhaitez déposer une plainte auprès de la GRC, comme Kevin l'a dit, c'est à vous de le décider. Nous n'intervenons pas en tant qu'institution, en tant qu'intermédiaire, pour prendre ces décisions.

Le président: D'accord.

Voilà qui complète ma liste d'intervenants. Je serais ravi de laisser les membres qui le souhaitent poser une question.

Monsieur Lukiwski, vous avez une question à poser? Certainement.

M. Tom Lukiwski: Une question rapide — et veuillez m'excuser car je suis un peu en retard en matière de technologie.

Monsieur Bard, vous avez indiqué que 70 p. 100 des courriels entrants étaient bloqués. Est-ce que cela concerne l'adresse parlementaire principale? Nous avons tous des adresses de courriel personnelles. Il y a mon adresse de courriel au bureau, où la plupart de mon courrier électronique arrive, mais nous avons tous, en plus des adresses courriel personnelles.

Si quelqu'un arrivait à mettre la main sur l'adresse de courriel personnelle d'un député, y a-t-il quelque moyen que ce soit à votre disposition pour vous permettre de détecter quelque chose ou de bloquer toute communication dans ce cas?

● (1230)

M. Louis Bard: S'il s'agit d'une adresse personnelle située à l'extérieur de l'environnement, si c'est...

M. Tom Lukiwski: Non, je parlais de celles que l'on nous donne ici.

M. Louis Bard: Il peut s'agir de tout courriel envoyé au site parl.gc.ca. Tout ce qui nous est envoyé est filtré et analysé afin de d'assurer qu'il s'agit d'un courriel valide.

Lorsque je parle de courriel « rejeté », cela signifie que ce n'est pas un bon courriel; ce n'est pas un courriel valide. Il s'agit d'une tentative de corrompre des services et d'en bloquer l'accès, de courriels qui n'ont pas de valeur légitime.

Si nous avons quelque doute que ce soit concernant ce courriel, mais qu'il ne contient pas de virus ou quoi que ce soit d'autre, il vous sera envoyé, et nous déterminons ensuite à quel point il s'agit de pourriel. Si nous sommes d'avis qu'il pourrait s'agir d'un pourriel, c'est au député de décider ce qu'il veut faire de ce courriel.

C'est la procédure suivie.

Le président: D'accord. J'ai quelques autres intervenants qui souhaitent poser des questions.

Monsieur Zimmer, puis monsieur Garneau.

M. Bob Zimmer: C'est davantage une observation que ce que j'ai dit auparavant.

C'est un défi pour le grand public, je pense, avant de jouer le jeu en suivant Anonymous, ou en l'appuyant de quelque façon que ce soit. Je dirais que le défi pour le grand public... Je vois les choses dans un contexte plus large. Je ne vois pas cela simplement comme un défi qui nous concerne, à titre de parlementaires. Je vois cette problématique comme Canadien, que je considère relevée de l'intimidation, en général. L'une des observations faite dans la lettre était ce qui suit:

> Comment réagissez-vous au fait de voir des renseignements personnels concernant votre famille tombés entre les mains de gens que vous ne connaissez pas, sans avoir aucun contrôle sur la personne qui diffuse ces renseignements ou sur la manière dont ils seront utilisés?

Je vois cela comme une menace contre la population canadienne en général, pas seulement contre les parlementaires. Avant d'adhérer à cette approche du tout ou rien, je mettrais ces gens au défi d'ouvrir leur propre compte Twitter et de poser ces questions directement, et de voir leur nom figurer dans une liste. Je serais ravi de répondre à toute question, comme c'est le cas de la plupart d'entre nous. Je pense que cela concerne tous les partis politiques. Je ne pense pas qu'il s'agisse d'une question partisane du tout. Je pense que le dialogue est possible; nous y sommes ouverts, alors dialoguons. D'accord.

Le président: Merci.

Monsieur Garneau, allez-y.

[*Français*]

M. Marc Garneau: Merci beaucoup.

[*Traduction*]

En posant ma question, j'admets mon ignorance. Réglemente-t-on d'une quelconque façon ce qui est diffusé sur YouTube? Peut-on afficher tout et n'importe quoi sans vérifier s'il y a violation de la loi? Est-il question, à l'échelle internationale, de créer des normes qui permettraient de déterminer ce qui peut être diffusé sur YouTube? Ou est-ce l'anarchie totale?

M. Louis Bard: Pour moi, dans le cadre de l'élaboration de l'environnement technologique dont je suis responsable, j'ai toujours gardé à l'esprit le concept du Parlement ouvert, du dialogue. Comme vous le savez, le Président a rendu il y a deux ou trois ans une décision relativement à l'assouplissement des permissions accordées aux députés, au téléchargement de données et à la réutilisation de notre contenu.

Je trouve que votre question est très pertinente, monsieur Zimmer. Les députés devront trouver des façons novatrices de communiquer avec leurs électeurs.

En même temps, il ne faut absolument pas que vous pensiez que j'ai l'intention d'analyser vos courriels, vos articles électroniques, etc. Je ne fais pas ce genre de chose. Ce sont les députés qui auront un rôle à jouer, parce que nous n'exerçons aucune surveillance de ce genre.

M. Marc Garneau: Je ne posais pas la question par rapport au Parlement à proprement parler. Je parlais de façon générale. Je voulais savoir s'il existait des processus de vérification. Je ne parlais pas spécifiquement de ce qui se fait au Parlement. Peut-on tout simplement diffuser tout et n'importe quoi sans contrainte?

Le président: Vous parlez de YouTube précisément?

M. Marc Garneau: Oui, de YouTube.

M. Louis Bard: Je pense bien que oui.

Le président: Oui.

Monsieur Kerr et monsieur Comartin, allez-y.

M. Greg Kerr: Merci beaucoup.

Je vais peut-être répéter quelque chose qui a déjà été dit, mais je voudrais que ce soit clair. Les BlackBerry sont quelque peu différents des ordinateurs. Y a-t-il des choses auxquelles on devrait faire particulièrement attention quand on se sert de son BlackBerry?

M. Louis Bard: À l'heure actuelle, les BlackBerry sont les téléphones intelligents qui offrent l'environnement le plus sécurisé sur la Colline du Parlement. Il est clair que ces dispositifs sont hautement sécurisés et par conséquent ils constituent de bons outils. D'ailleurs, ils ont été élaborés de façon à s'intégrer à nos infrastructures et sont donc parfaitement adaptés à l'environnement présent de la Chambre des communes.

D'autre part, nous permettons l'utilisation d'un petit nombre d'applications tierces, également très sécurisées. Par contre, il y a certaines fonctions du BlackBerry, comme le téléphone portable ou la messagerie NIP à NIP dont on se sert en marge de nos environnements, ce qui augmente les risques. Par conséquent, je répète qu'il est important de se rappeler la raison pour laquelle on utilise l'appareil. C'est toujours important. Cela dit, il s'agit d'un bon outil, hautement sécurisé à l'heure actuelle.

● (1235)

M. Greg Kerr: D'accord. Une petite précision. Vous disiez que la messagerie NIP est moins sécurisée que le courriel normal?

M. Louis Bard: Oui.

M. Greg Kerr: Merci.

M. Louis Bard: Tout à fait, parce que quand on se sert de la messagerie NIP à NIP il n'y a pas de réseau; c'est une technologie qui permet à deux personnes de communiquer. Il s'agit de fréquences radios, et le seul élément de sécurité qui entre en ligne de compte, c'est que nous deux nous parlons, par exemple, nous parlons rien que nous deux, et c'est là le seul élément de sécurité.

Le président: Merci.

Monsieur Comartin, le mot de la fin est à vous.

M. Joe Comartin: Je vais changer de sujet, madame O'Brien. À l'heure actuelle, on parle beaucoup, en raison de l'affaire que nous connaissons tous, des limites ou des interdictions qu'on devrait imposer dans le cas de documents juridiques traitant d'informations matrimoniales. Si j'ai bien compris, les juristes estiment que c'est une responsabilité provinciale parce que la justice, c'est quelque chose qui relève des provinces.

Par contre, il y a un aspect qui relève du gouvernement fédéral dans la mesure où on voudrait, par exemple, modifier la Loi sur le divorce ou la Loi sur la preuve au Canada afin d'interdire l'accès public à ce genre de dossiers. Soit dit en passant, ce n'est pas quelque chose que je préconise. À votre connaissance, a-t-on demandé aux juristes parlementaires de formuler une opinion à cet égard?

Mme Audrey O'Brien: À ma connaissance, on n'a pas demandé au juriste de formuler une opinion à cet égard.

M. Joe Comartin: Merci.

Le président: Merci.

M. Albrecht désire poser une petite dernière question. Allez-y.

M. Harold Albrecht: Merci, monsieur le président.

Merci, monsieur Bard, d'avoir souligné la sûreté du système BlackBerry. Vous avez précisé que la messagerie NIP est moins sécurisée. Est-ce également le cas du BlackBerry Messenger?

M. Louis Bard: Tout à fait.

M. Harold Albrecht: D'accord. En résumé, ces deux systèmes de messagerie sont moins sécurisés que l'envoi de courriels à partir de nos comptes personnels.

M. Louis Bard: Oui.

M. Harold Albrecht: Très bien. Merci beaucoup.

Le président: Très bien.

Merci à tous. Je voudrais vous remercier du respect que vous avez démontré lorsque vous avez posé vos questions et vous dire que je suis heureux que nous n'ayons pas abordé de questions qui ne devraient pas être débattues en public.

Merci beaucoup. Notre étude a bien démarré. Je vous remercie de nous avoir accompagnés au tout début de notre mission. Comme vous le savez peut-être, nous ne savons pas encore quelles seront les prochaines étapes, mais c'est vrai que nous comptons inviter d'autres témoins, et nous allons commencer par ça.

Mme Audrey O'Brien: Monsieur le président, le sergent d'armes, qui ne cesse de suivre les nouveaux développements, m'informe d'un message affiché dans Twitter qui dit que je me débrouille pas mal en ce moment, mais qu'il est possible que je méprenne « Anonymous » pour un groupe qui s'appelle « LulzSec ».

Je n'essaie même pas de prononcer ce mot parce que...

Mme Chris Charlton: En quel honneur ont-ils le droit de poser des questions?

Mme Audrey O'Brien: Je ne sais pas si je devrais présenter des excuses à ces personnes, ou s'il s'agit plutôt de gens qui ne méritent même pas de réaction.

Ça rejoint ce que disait M. Zimmer par rapport au fait que nous avons tous la responsabilité de ne pas nous faire berner par des sites Web qui se servent de nous, à notre insu, pour disséminer des pourriels et des maliciels.

Je dirais à la personne de Twitter que j'ai déçue que j'essaierai de faire mieux.

Merci beaucoup.

Le président: Moi, je vous ai trouvée extraordinaire un point c'est tout.

Mme Audrey O'Brien: Merci, monsieur Preston. Il m'est toujours agréable de vous revoir.

Le président: Merci.

Y a-t-il autre chose de pertinent?

Oui, allez-y, monsieur Lukiwski.

M. Tom Lukiwski: Étant donné qu'il y a une nouvelle question de privilège qui nous a été renvoyée, je me demandais s'il ne serait pas judicieux de parler pendant quelques minutes des travaux futurs. En plus, j'ai cru comprendre que M. Ménard allait dire formellement qu'il avait l'intention de comparaître devant notre comité.

Le président: Poursuivons la séance à huis clos, nous parlerons des travaux du comité, si les membres du comité sont d'accord.

Je suspends les travaux pendant une minute.

[*La séance se poursuit à huis clos*]