CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la procédure et des affaires de la Chambre

PROC • NUMÉRO 031 • 1re SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le mardi 3 avril 2012

Président

M. Joe Preston

Comité permanent de la procédure et des affaires de la Chambre

Le mardi 3 avril 2012

● (1105)

[*Traduction*]

Le président (M. Joe Preston (Elgin—Middlesex—London, PCC)): Ouvrons la séance d'aujourd'hui. Il s'agit de la 31e séance, tenue conformément à l'ordre de renvoi du jeudi 6 mars sur la question de privilège relative aux menaces portées contre le député de Provencher.

Nous avons plusieurs invités aujourd'hui, et notre séance se divisera en deux volets. Commençons. Je crois comprendre que vous ferez une déclaration préliminaire. Veuillez vous présenter, puis poursuivre avec cette déclaration. Les membres vous poseront ensuite leurs questions.

Mme Toni Moffa (chef adjointe, sécurité des TI, Centre de la sécurité des télécommunications Canada): Merci, monsieur le président.

[*Français*]

Cela me fait plaisir de comparaître devant ce comité, aujourd'hui. Je m'appelle Toni Moffa et je suis chef adjointe ou sous-ministre adjointe du Programme de la sécurité des technologies de l'information au Centre de la sécurité des télécommunications Canada, ou le CSTC. M. Scott Jones, le directeur général de la section de la cyberdéfense, m'accompagne aujourd'hui.

Je vais commencer par quelques mots qui résumeront le mandat et les activités du CSTC. Le CSTC a pour mission, depuis un peu plus de 65 ans, de fournir du renseignement et de protéger l'information importante pour le gouvernement du Canada.

[*Traduction*]

Comme vous le savez peut-être, le CSTC mise sur ses technologies de pointe, sur son expertise et sur ses partenariats nationaux et internationaux pour offrir au gouvernement du Canada trois services clés. En premier lieu, nous fournissons du renseignement électromagnétique étranger conformément aux priorités du gouvernement fédéral en matière de renseignement établies tous les ans par le Cabinet.

En deuxième lieu, nous fournissons des conseils et des services pour aider à protéger les renseignements électroniques et les systèmes d'information importants pour le gouvernement du Canada dans le cadre du Programme de la sécurité des technologies de l'information (TI). C'est le programme dont je suis responsable et que je représente aujourd'hui.

En troisième lieu, bien que nous ne soyons ni un organisme chargé de l'application de la loi, ni un organisme d'enquête, ni un organisme de réglementation, nous travaillons avec nos partenaires fédéraux de la collectivité de la sécurité, du renseignement et de l'application de la loi en leur fournissant une assistance opérationnelle et technique qui leur permet, à leur demande, d'utiliser l'expertise et les capacités uniques du CSTC dans l'exercice des fonctions que la loi leur confère.

Toutes nos activités légiférées s'inscrivent dans de nombreuses responsabilités et font l'objet de nombreux examens internes et externes, y compris d'un examen indépendant du commissaire du Centre de la sécurité des télécommunications qui assure le respect rigoureux des lois qui régissent nos activités et le respect de la vie privée des Canadiens.

Aujourd'hui, je parais devant vous à titre de sous-ministre adjointe responsable de la gestion du Programme de la sécurité des TI. Dans le cadre de ce programme, nous fournissons des produits et des services qui aident à prévenir, à détecter et à contrer les menaces de sécurité des TI et les vulnérabilités des TI. À ce titre, nous avons une responsabilité partagée avec d'autres ministères et organismes fédéraux. Nous collaborons avec la Direction du dirigeant principal de l'information du Secrétariat du Conseil du Trésor, avec Travaux publics et Services gouvernementaux Canada et avec le nouveau ministère Services partagés Canada pour colmater les vulnérabilités et atténuer les menaces de sécurité qui visent les systèmes TI fédéraux.

Aux fins de prévention, nous publions des normes et des conseils techniques qui, une fois mis en oeuvre par les ministères et organismes fédéraux, aident à renforcer la sécurité et la résilience des systèmes TI. Pour détecter et contrer les menaces de sécurité des TI, nous travaillons étroitement avec le Secrétariat du Conseil du Trésor et Services partagés Canada. Avec la coopération du Service canadien du renseignement de sécurité (SCRS), de la Gendarmerie royale du Canada (GRC) et de Sécurité publique Canada, nous faisons le suivi des activités et des méthodes des menaces de sécurité des TI qui cherchent à voler des renseignements électroniques ou à endommager les systèmes d'information qui sont importants pour le gouvernement fédéral.

Le CSTC contribue à ces efforts communs en utilisant son expertise et ses capacités techniques uniques ainsi que ses renseignements classifiés pour compléter les technologies de sécurité commerciales qui sont à la portée des praticiens de la sécurité des TI au gouvernement ou celles qu'ils utilisent déjà. Les technologies de sécurité commerciales dont sont dotés les systèmes fédéraux, semblables à celles qu'utilisent les citoyens chez eux, aident à recenser des millions de menaces bien connues du public et à contrer les cyberactivités desquelles pourrait découler le vol d'information sensible, classifiée ou personnelle ou des activités criminelles en ligne.

Par ailleurs, le CSTC a développé ses propres méthodes et opérations pour surveiller les connexions du gouvernement fédéral à l'Internet et pour détecter et contrer les menaces de sécurité des TI qui ne relèvent pas du domaine public. Pour les systèmes piratés dans le cadre de ces activités, le CSTC offre une assistance d'intervention rapide et ciblée qui permet d'atténuer l'incident de sécurité des TI et de l'empêcher de se reproduire. L'information technique sur les incidents de sécurité des TI qui ont lieu dans un secteur ou ministère est communiquée à tous les ministères de TI du gouvernement, y compris à la cité parlementaire, pour éviter la propagation de menaces de sécurité des TI semblables.

Pour assurer la sécurité des TI à l'échelle du pays, cette information est aussi diffusée à Sécurité publique Canada, qui la transmet à ses partenaires en dehors du gouvernement fédéral.

L'Internet est devenu un outil utile et indispensable pour les activités du gouvernement, les transactions opérationnelles et financières, le réseautage social et la transmission d'information aux citoyens. Toutefois, avec plus de deux milliards d'utilisateurs, c'est aussi un environnement attrayant pour les malfaiteurs qui veulent exploiter les vulnérabilités de l'Internet à des fins criminelles et néfastes. Au moyen de son Programme de la sécurité des TI, le CSTC offre des produits et des services qui tentent de prévenir ces catastrophes dans les réseaux fédéraux ou d'aider à recouvrer l'information perdue lorsqu'ils deviennent victimes de graves menaces de sécurité des TI.

Vous avez là un aperçu du CSTC et de son Programme de la sécurité des TI. C'est avec plaisir que je répondrai à vos questions.

Le président: Je vous remercie de votre déclaration préliminaire. Elle a suscité chez moi plus de questions que de réponses, mais je suis convaincu que les membres sauront combler mes lacunes.

Monsieur Albrecht, vous êtes premier. Vous disposez de sept minutes.

M. Harold Albrecht (Kitchener—Conestoga, PCC): Merci, monsieur le président.

Je remercie nos témoins de leur présence.

Quand je suis entré dans la salle, j'ai assuré les témoins que nous chercherions aujourd'hui à en apprendre davantage sur la question. M. Bard a comparu devant nous précédemment aux fins de notre étude. J'estime qu'il a su convaincre l'ensemble du comité que les systèmes de sécurité de la Colline sont aussi sûrs que possible et que les activités foisonnent au chapitre de la sécurité.

Toute votre présentation, ce matin, portait sur la sécurité des TI. Comme vous le savez, nous traitons aujourd'hui d'une question connexe, qui englobe par ailleurs le groupe Anonymous. Pouvez-vous m'expliquer en quelques mots ce que vous savez à propos d'Anonymous, de son fonctionnement et du type de menace que le groupe représente sur le plan du piratage des systèmes de TI de la Colline?

● (1110)

Mme Toni Moffa: Ce que nous savons d'Anonymous provient essentiellement de sources accessibles à tous.

De toute évidence, ce qui nous intéresse lorsque nous étudions des groupes et des personnes de cet ordre, ce sont les techniques employées ou susceptibles de l'être afin d'ouvrir une brèche de sécurité dans les systèmes à leurs propres fins.

Nous tentons notamment de nous protéger contre des techniques et des méthodes comme l'attaque par saturation ou le harponnage, c'est-à-dire l'attaque d'un système par leurre, et de mettre en place des mesures qui resserrent la sécurité globale du système.

Nous envisageons ce que les propriétaires de réseau peuvent faire sur le périmètre du réseau — assurer une surveillance afin de détecter les signes d'alerte, y réagir promptement et atténuer les dommages éventuels — ainsi qu'à l'intérieur du système. Nous formulons ensuite des conseils sur les meilleurs moyens de les protéger et de protéger leurs données.

Voilà le genre de choses que nous examinerions lorsqu'il est question de ce type de groupes ou de personnes.

M. Harold Albrecht: Merci.

La question en cause aujourd'hui et tout au long de l'étude est celle de l'intimidation d'un parlementaire pour l'empêcher de remplir ses fonctions de législateur et de présenter une loi, la menace de faire tout en son pouvoir pour empêcher à tout prix l'adoption de ce projet de loi. Je crois qu'il s'agit d'une menace sérieuse.

L'une de nos difficultés actuelles consiste à déterminer qui a proféré cette menace, notamment en accédant aux adresses IP et tout ça. De toute évidence, nous sommes conscients de l'existence d'obstacles à l'échelle locale.

Existe-t-il des mécanismes ou des ententes internationales qui nous permettraient, si quelqu'un affichait une vidéo menaçante sur YouTube, de nous en faire révéler la source et d'identifier l'auteur de la menace qui, selon moi, porte concrètement atteinte au processus démocratique dans son ensemble?

Mme Toni Moffa: Je présume que la menace à laquelle vous faites allusion concerne...

M. Harold Albrecht: M. Toews.

Mme Toni Moffa: ... l'affichage des vidéos.

Pour notre part, il ne s'agit pas d'une brèche de sécurité des TI; ce n'est pas de notre ressort.

M. Harold Albrecht: Non, précisément.

Mme Toni Moffa: C'est un organisme d'enquête qui serait le plus apte à mener ce type d'enquête en s'appuyant sur ses partenariats.

M. Harold Albrecht: Entretenez-vous des relations de travail avec des organismes d'enquête, comme le FBI ou Scotland Yard, qui permettraient à nos autorités d'enquêter pour découvrir qui a proféré une menace donnée?

Mme Toni Moffa: Nos partenariats avec l'étranger visent surtout des organismes qui mènent des activités semblables aux nôtres et non des organismes d'enquête.

M. Harold Albrecht: D'accord.

Je reviens à ce que vous avez dit au début, à savoir que votre responsabilité première, c'est la sécurité des TI. C'est quelque chose que je respecte et que je comprends. Avez-vous des conseils pour le comité sur la façon de composer avec ce groupe très obscur qu'est Anonymous?

Ce que je veux dire, c'est que nous ne savons même pas qui le compose. De toute évidence, personne ne le sait. Quels conseils formuleriez-vous à un comité qui cherche à prévenir le type de menace au processus démocratique selon moi ici en cause, qui concerne M. Toews et un projet de loi proposé et qui vise à court-circuiter notre travail?

Mme Toni Moffa: Malheureusement, je ne peux vous conseiller efficacement que sur la sécurité des TI, la manière dont on peut faire une brèche dans les systèmes et les moyens de prévenir ces brèches.

Par contre, je ne suis pas vraiment qualifiée par rapport aux autres éléments dont il est ici question.

M. Harold Albrecht: Merci, et merci à vous, monsieur le président.

Le président: Monsieur Toone, vous disposez de sept minutes.

● (1115)

M. Philip Toone (Gaspésie—Îles-de-la-Madeleine, NPD): Merci, monsieur le président, et merci de votre présentation fort instructive.

Je dois reconnaître que le Centre de la sécurité est probablement le moins connu de tous nos services de sécurité. Ce n'est qu'au cours de mes études universitaires que j'en ai entendu parler pour la première fois, lorsque l'un de vos collègues m'a expliqué qu'il travaillait pour vous. Ce qu'il avait à dire m'intéressait beaucoup.

Selon ce que je comprends, le Centre de la sécurité est entravé par le fait que son mandat consiste à trouver les brèches de sécurité potentielles hors des confins du Canada. Vous êtes une sorte de pare-feu contre les menaces qui pourraient s'immiscer dans notre pays. Ai-je bien compris?

Mme Toni Moffa: Pour ce qui est de protéger les systèmes fédéraux, oui: nous surveillons les connexions à Internet et les activités menées en ligne afin de déceler tout signe d'une menace susceptible de porter atteinte à nos réseaux fédéraux.

M. Philip Toone: Je reconnais tout à fait — vous le comprenez également — que c'est tout un travail. Internet est un réseau que l'armée a créé il y a bien des années justement pour qu'on puisse y accéder d'à peu près n'importe où. On l'a pourvu de redondances en cas de défaillance ou d'attaques à certains endroits. Il est très difficile d'y créer une brèche. C'est la beauté d'Internet. J'estime qu'il s'agit d'une structure hautement démocratique. Selon moi, il faut féliciter l'armée d'avoir créé une structure démocratique, mais les organismes de sécurité auront toutes les difficultés du monde à y déceler les menaces et à chercher à les contrer.

Dans le contexte de la menace ici en cause, le ministre Toews nous a demandé — en passant, nous lui souhaitons tous un prompt rétablissement. J'ai cru comprendre qu'il est toujours hospitalisé, et c'est quelque chose que je ne souhaite à personne. Nous sommes ici parce qu'il a été menacé personnellement par l'entremise d'une vidéo affichée sur YouTube, à l'extérieur du Canada selon ce que j'ai compris. Il y avait donc une vidéo YouTube enregistrée sur un serveur à l'étranger. La structure même d'Internet fait qu'il est très difficile de définir où le fichier est hébergé. Il y a des serveurs partout. Comme je l'ai dit, les redondances du système IP permettent très difficilement de déterminer où se trouvent les failles et d'où provient la menace.

Je veux simplement mieux comprendre. Si votre mandat consiste à nous protéger du renseignement électromagnétique étranger et à protéger le gouvernement canadien et les Canadiens en général des menaces de sécurité des TI — des menaces qui cherchent à porter atteinte aux systèmes d'information fédéraux ou à y voler des données —, où cela s'inscrit-il dans notre mandat actuel?

Tout a commencé par une vidéo affichée sur YouTube, alors en quoi consiste précisément la menace posée par la vidéo? Cliquer sur l'hyperlien de cette vidéo de YouTube pourrait-il permettre à un pirate d'entrer automatiquement au pays et, peut-être, de compromettre votre sécurité ici? Est-ce un motif juste et raisonnable de s'inquiéter au sujet de cette vidéo YouTube en particulier?

Mme Toni Moffa: Selon notre expertise technique, quelqu'un a utilisé un outil accessible au grand public pour afficher de l'information — dans ce cas-ci, une vidéo — sur Internet. Compte tenu des renseignements dont nous disposons, il ne s'agit donc pas d'une brèche de sécurité des TI, vous comprenez? Il ne s'agit pas d'une menace technique.

M. Philip Toone: Vous a-t-on demandé d'enquêter sur ce dossier? A-t-on demandé au Centre de la sécurité de se pencher sur cette soi-disant menace en particulier?

Mme Toni Moffa: Je sais qu'une enquête est en cours, mais il ne convient pas que je commente la question.

M. Philip Toone: Si je saisis bien votre mandat, ce dossier ne relèverait pas de vos compétences, n'est-ce pas?

Mme Toni Moffa: Notre mandat consiste entre autres à offrir de l'aide aux ministères fédéraux qui le demandent, à l'appui de leur propre mandat. Ils peuvent donc demander de se prévaloir de notre expertise technique.

M. Philip Toone: Alors pouvez-vous expliquer la menace? Selon vous, quelle est-elle?

Mme Toni Moffa: Dans ce dossier précis ou en général?

M. Philip Toone: Aux termes du mandat du Centre de la sécurité. Pourquoi ferait-on appel au Centre de la sécurité?

Mme Toni Moffa: Je vois, oui. Nous examinons les menaces qui ne sont pas de notoriété publique. Les technologies commerciales s'occupent très bien des activités malveillantes bien connues et menées par l'entremise de logiciels malveillants. Vos antivirus, vos pare-feu disposent donc de moyens et de techniques efficaces pour vous protéger.

Nous, nous nous intéressons aux menaces qu'eux ignorent et qui sont extrapolées d'information classifiée. Nous cherchons donc à déceler ces types d'activités et à protéger les systèmes du gouvernement contre eux, en complémentarité avec les technologies commerciales.

● (1120)

M. Philip Toone: Il me reste encore deux minutes. Selon ce que j'ai compris, la vidéo a été affichée sur YouTube en réaction aux déclarations de M. Toews à la Chambre relativement au projet de loi C-30. Il semblait sous-entendre que beaucoup de Canadiens s'adonnaient à des activités criminelles parce qu'ils se servaient d'Internet.

Beaucoup de gens ont très mal accueilli ces propos. Les réactions ont été nombreuses, et certaines ont peut-être dépassé les bornes. Je crois que c'était le cas pour cette vidéo YouTube.

Par contre, je me demande quelle est la menace pour les systèmes informatiques. En quoi réside la menace pour la sécurité?

Mme Toni Moffa: En ce qui concerne cette vidéo, sur le plan de la sécurité des TI, je ne vois aucune menace.

M. Philip Toone: D'accord. Y a-t-il un autre service de sécurité au pays qui serait mieux à même d'examiner la question? Qui aurait le mandat de traiter cette menace, et de quelle menace s'agit-il exactement?

Mme Toni Moffa: À mon avis, c'est du ressort des organismes d'enquête qui sont à la disposition du gouvernement.

M. Philip Toone: Peut-être ne s'agit-il pas d'une menace relative à la technologie de l'information autant que d'une contravention au Code criminel, par exemple.

Mme Toni Moffa: Je suis désolée, je n'ai pas entendu la fin de la phrase.

M. Philip Toone: S'agit-il même d'une menace relative à la technologie de l'information?

Mme Toni Moffa: À notre avis, non.

M. Philip Toone: Il s'agit peut-être davantage d'une contravention aux codes civil ou criminel?

Mme Toni Moffa: Je ne suis pas spécialiste de ces questions, mais oui.

M. Philip Toone: D'accord. Merci.

C'est tout pour moi, monsieur le président.

Le président: Merci, monsieur Toone.

Monsieur Easter, nous sommes enchantés de votre présence au comité aujourd'hui. Vous disposez de sept minutes.

L'hon. Wayne Easter (Malpeque, Lib.): Merci. C'est un plaisir d'être parmi vous, monsieur le président.

Je remercie les témoins.

Selon ce que vous avez expliqué, l'incident ne constitue pas ce que vous considéreriez être une brèche de sécurité.

Mme Toni Moffa: Une brèche de sécurité des TI...

L'hon. Wayne Easter: Vous affirmez qu'il s'agit plutôt d'une menace visant une personne. Du point de vue du CST, alors, vous n'avez pas vraiment de rôle à jouer dans cette enquête, qui devrait plutôt relever de la GRC ou des organismes policiers étrangers. Lorsqu'il est question d'Internet, il ne s'agit sans doute pas d'un problème qui vise strictement le Canada.

Est-ce exact?

Mme Toni Moffa: Je suis d'accord, oui.

L'hon. Wayne Easter: La vidéo YouTube et Vikileaks — une série d'incidents associés au ministre — visent notamment le projet de loi sur la surveillance légale qui a été proposé et qui, selon ce que j'ai compris, a été mis en veilleuse.

La population — vous pourrez éventuellement nous aider sur ce plan — est très préoccupée par Big Brother. La protection de la vie privée est presque une chose du passé. On craint beaucoup que l'État tentaculaire — que Big Brother, pour ainsi dire — découvre beaucoup d'information personnelle grâce à Internet ou par d'autres moyens.

Selon vous, comment peut-on atteindre un équilibre à ce sujet? D'une part, je sais très bien que votre travail est nécessaire pour assurer à distance la sécurité de nos systèmes de TI et qu'il faut également veiller à la sécurité et à la protection de l'information du pays, mais d'autre part, les gens veulent protéger leur vie privée et leurs renseignements personnels.

Comment trouvez-vous le juste milieu dans cette nouvelle ère?

Mme Toni Moffa: Le projet de loi que vous avez mentionné n'a aucune répercussion sur l'autorité et le mandat du CST. Notre propre mesure législative comporte évidemment des dispositifs relatifs au respect de toutes les lois applicables, y compris celles qui protègent la vie privée et les renseignements personnels des Canadiens. Nous sommes dotés d'un ensemble strict de politiques et de procédures internes qu'approuve et que revoit le ministère de la Justice. Le commissaire du CST procède annuellement à un examen de nos activités, qu'il a toujours trouvées conformes à la loi.

Ce sont là les poids et contrepoids dont nous disposons. Nous avons une culture organisationnelle fort rigoureuse. Tout le monde connaît ses responsabilités respectives et les mesures à prendre. Voilà comment nous réagissons.

● (1125)

L'hon. Wayne Easter: Par contre, les gens craignent toujours de se faire espionner. Il y a évidemment l'incident mettant en cause le ministre et ce qui semble être une menace. Mais à mon avis — et je pense que beaucoup de membres ici présents doivent le partager —, à l'ère d'Internet, lorsqu'un article est publié dans le journal, beaucoup des répliques qui paraissent dans la section des commentaires pourraient presque être considérées comme du courrier haineux.

Je pense que ça devient un problème grave. J'ignore, monsieur le président, comment nous réussirons un jour à le contrer, car les gens sont autorisés à afficher des messages sur Internet, dans les sections des commentaires, en les signant d'un pseudonyme. Selon moi, devoir signer un article de son propre nom rend moins enclin à tenir des propos outranciers contre une personne ou un enjeu politique.

Je sais que ce n'est pas votre domaine, mais voyez-vous des problèmes à ce sujet? Comment peut-on commencer à endiguer ce qui me paraît se rapprocher de plus en plus de la haine? Ce sont des dossiers donnés qui peuvent donner lieu à cette haine, sauf que des gens se font attaquer à un point tel que je ne lis presque plus les sections des commentaires. C'est un problème qui s'intensifie.

Constatez-vous la même chose?

Mme Toni Moffa: Eh bien, Internet est devenu une infrastructure vaste et complexe. On compte aujourd'hui deux milliards d'internautes, un nombre qui continue de croître. Il y a des centaines de millions de sites Web, et des billions de courriels sont transmis chaque jour. Il s'agit d'un milieu difficile à contrôler, si tant est qu'il soit possible de le faire.

L'hon. Wayne Easter: Je comprends, et il ne fait aucun doute qu'Internet est gigantesque et qu'il évolue. Mais alors qu'à une certaine époque, les gens devaient signer de leur propre nom... je sais qu'ils entrent leur nom quelque part pour ensuite utiliser leur pseudonyme.

Si je soulève cette question, c'est par rapport à la menace à laquelle nous sommes confrontés — Anonymous, dont nous ignorons même l'identité —, nous tous, qui ne sommes pas ministres, mais qui adoptons des positions politiques parce que cela fait partie intégrante de notre travail. Nous sommes de plus en plus aux prises avec du courrier haineux, car les gens qui écrivent ces lettres n'ont pas à signer leur nom.

Selon votre expérience, existe-t-il des pays ou des lois ailleurs dans le monde qui cherchent à régler ce problème? À mon avis, la situation se détériore, ce qui mène à des déclarations outrancières et à des attaques outrancières contre des personnes. Dans le cas présent, il s'agit d'une attaque outrancière d'Anonymous contre le ministre, mais il ne s'agit pas d'un cas unique. Je pense que nous tous ici... Quelqu'un n'aime pas des propos que nous avons tenus, puis part en guerre contre nous; dans la section des commentaires, on ne connaît plus de borne — c'est presque de la haine.

Le président: Je permets une réponse succincte.

Mme Toni Moffa: Je suis ici à titre d'experte technique. Il ne convient pas du tout que je formule des commentaires ou des suggestions à ce sujet.

Le président: Merci beaucoup.

Nous ferons un tour de cinq minutes.

À vous l'honneur, monsieur Zimmer.

M. Bob Zimmer (Prince George—Peace River, PCC): Merci d'être ici aujourd'hui.

J'ai posé cette question au cours de la dernière réunion. Nous cherchons à obtenir de l'information et des conseils sur la manière dont vous pouvez nous aider, nous, les parlementaires, mais je considère qu'il s'agit d'un problème d'ensemble pour les Canadiens en général. Les Canadiens nous ont élus et nous les représentons, alors nous attaquer, c'est les attaquer. Eux aussi peuvent être victimes d'attaques ou d'intimidation, et tout ça, au quotidien.

Ce que je vous demande — c'est vous l'experte —, c'est comment nous pouvons nous protéger le plus efficacement contre ces menaces technologiques au travail et à la maison.

Mme Toni Moffa: Certaines des choses que le DPI, Louis Bard, a mentionnées sont de bonnes pratiques en TI. Beaucoup découlent de nos conseils du point de vue de la sécurité des TI et permettraient de prévenir quantité d'activités malveillantes sur nos réseaux ou nos ordinateurs. Ce sont des normes et des conseils qui pourraient rendre la tâche très difficile à ceux qui cherchent à causer du tort.

Elles rendent par ailleurs nos systèmes moins vulnérables. De toute évidence, Internet est un endroit vulnérable qui suppose de multiples risques. Dès qu'on s'y connecte, il y a des risques. On peut prendre des mesures pour atténuer ces risques, mais ils ne seront jamais complètement éliminés.

● (1130)

M. Bob Zimmer: D'accord.

J'ai une autre question. Vous vous êtes sans doute intéressés au groupe Anonymous. Je ne devrais pas le présumer, mais j'aimerais savoir à combien vous estimez le nombre de membres d'Anonymous. Je pense qu'il y en a de toutes sortes. Il y a ceux qui ont des intentions malveillantes, puis il y a les autres, qui veulent seulement être associés au mouvement.

Selon vous, quelle est la proportion de membres qui ont de véritables intentions criminelles par opposition à ceux qui ne cherchent qu'à s'associer au groupe?

Mme Toni Moffa: Malheureusement, je ne suis pas qualifiée pour commenter leurs intentions. Ce qui nous intéresse, ce sont les techniques qu'emploient les groupes de cet ordre et les conseils que nous pouvons formuler pour empêcher que ce genre de choses ne réussisse à porter atteinte à nos propres systèmes.

Je ne suis donc pas en mesure de commenter ce point.

M. Bob Zimmer: D'accord.

J'ai une dernière question, s'il me reste du temps.

Je désire savoir comment coopère votre organisme. Comment coopère-t-on avec d'autres organismes outre-mer? Comment cela fonctionne-t-il, sur le plan des relations?

Mme Toni Moffa: Nous avons conclu avec nos homologues directs des partenariats internationaux par lesquels nous partageons nos renseignements et nos capacités techniques, car nous avons des objectifs en commun. Ce sont essentiellement nos homologues directs aux États-Unis, au Royaume-Uni, en Australie et en Nouvelle-Zélande — ce sont ceux avec qui nous collaborons le plus. De manière plus générale, il y a des groupes internationaux au sein desquels nous pouvons collaborer, comme l'OTAN.

M. Bob Zimmer: Nous entretenons donc actuellement des relations actives.

Mme Toni Moffa: Il y a des façons de coopérer de manière plus générale.

M. Bob Zimmer: Merci.

Le président: Merci, monsieur Zimmer.

Madame Latendresse, vous avez la parole pendant quatre minutes.

[*Français*]

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

Merci beaucoup, madame Moffa, de votre témoignage.

On vient de parler d'Anonymous, encore une fois. Anonymous n'est pas un groupe fermé. Il est presque certain que la personne qui a téléchargé en amont la vidéo sur YouTube et qui a fait des menaces au ministre n'a probablement aucun lien avec les pirates informatiques aux États-Unis, en Australie ou n'importe où. Des gens se disent que n'importe qui peut faire quelque chose au nom d'Anonymous. Il me semble donc extrêmement difficile de dire qu'Anonymous fait ceci ou qu'Anonymous a ces intentions-là. N'importe qui peut décider de mettre cette étiquette sur ses actions. Je trouve parfois difficile de cerner où on en est à cet égard parce que, pour l'instant, on se penche, comme on le précisait plus tôt, sur le cas de quelqu'un quelque part qui a mis une vidéo en ligne sur YouTube.

Oui, certaines personnes qui se disent d'Anonymous ont, par exemple, piraté les systèmes fédéraux américains, mais ce n'est pas ce qu'on étudie présentement.

Quand il y a des bris de sécurité et que des pirates informatiques entrent dans le système fédéral américain, est-ce que vous avez des contacts avec eux pour savoir ce qui s'est passé et comment vous pouvez mettre à jour vos outils pour prévenir ce genre de menace? Avez-vous des liens avec eux pour ça?

Mme Toni Moffa: De qui parlez-vous, exactement?

Mme Alexandrine Latendresse: Je pense, par exemple, à l'équivalent américain de votre agence.

Mme Toni Moffa: Oui, oui.

Mme Alexandrine Latendresse: Quand il y a des bris de sécurité aux États-Unis, vous pouvez échanger sur la façon d'améliorer le système.

Mme Toni Moffa: Nous partageons nos expériences. Nous pouvons ainsi nous entraider afin de prévenir ou d'aborder les problèmes quand ils arrivent dans nos systèmes.

● (1135)

Mme Alexandrine Latendresse: Certains sont arrivés récemment, je crois, il y a quelques mois, il n'y a pas très longtemps. Savez-vous si cela a été fait depuis? Y a-t-il eu des échanges, afin de rendre les systèmes plus efficaces et plus sécuritaires?

Mme Toni Moffa: Je ne peux pas faire de commentaires là-dessus, encore moins sur l'expérience des autres. Cela tombe dans le lot des renseignements classifiés.

Mme Alexandrine Latendresse: Pour revenir à Anonymous, si je comprends bien ce que vous nous dites, rien n'a été fait jusqu'à maintenant par quelqu'un qui relève de vous pour l'instant.

Mme Toni Moffa: C'est cela.

Mme Alexandrine Latendresse: Vous êtes donc ici surtout pour nous informer de ce que vous pouvez faire si, éventuellement, quelque chose se passe, si un pirate informatique essaie de...

Mme Toni Moffa: On s'informe des méthodes qu'ils utilisent pour essayer de prévenir leurs agissements à l'avenir.

[*Traduction*]

Le président: Merci.

Monsieur Hawn.

L'hon. Laurie Hawn (Edmonton-Centre, PCC): Merci, monsieur le président, et merci à nos témoins d'être venus.

M. Zimmer a posé une question à propos des bonnes pratiques en TI et tout ça. Vous avez dit que vous les faisiez connaître. Pouvez-vous nous fournir des exemples précis de bonnes pratiques en TI qui pourraient être utiles à des particuliers?

Mme Toni Moffa: Le site Web public du Centre de la sécurité des télécommunications, que tous peuvent consulter, donne de nombreux conseils à ce sujet.

En général, il faut protéger adéquatement le périmètre du réseau et être à l'affût de ce qui pourrait se produire afin de pouvoir y réagir rapidement. De telles pratiques permettent d'atténuer les dommages possibles ou de réduire le coût d'un éventuel nettoyage. Il est très important d'être vigilants.

Il faut aussi considérer la façon dont on protège les banques d'information dans les réseaux informatiques. Les renseignements n'ont pas tous la même valeur. Certains doivent donc être mieux protégés que d'autres. Pour ce faire, il existe des technologies.

L'un des principaux moyens de protection, c'est la sensibilisation des utilisateurs. Il ne faut pas seulement informer les professionnels de la sécurité des TI et les spécialistes, mais aussi l'ensemble des utilisateurs d'Internet et des réseaux informatiques. Il faut les prévenir des risques et des dangers et leur expliquer en quoi ils peuvent être vulnérables. La gestion des mots de passe est un bon exemple. Il faut notamment inciter les utilisateurs à changer souvent leurs mots de passe et leur montrer ce qu'est un bon mot de passe.

Beaucoup de choses peuvent être faites. L'une des mesures les plus importantes, c'est de veiller à ce que les logiciels utilisés dans les réseaux soient constamment à jour et d'installer les mises à jour de sécurité. Les fournisseurs sont très compétents: lorsque des failles sont décelées, ils proposent des programmes de correction qui permettent de mettre à jour leurs produits afin d'éviter que quelqu'un en exploite les vulnérabilités. L'un des très bons moyens de prévenir les dangers et les risques liés à l'utilisation des systèmes et des réseaux informatiques, c'est donc de les mettre à jour sans tarder.

L'hon. Laurie Hawn: Par contre, ce n'est pas quelque chose que l'utilisateur moyen peut faire.

Mme Toni Moffa: Les utilisateurs constateront que toutes les mises à jour sont intégrées dans l'antivirus ou le logiciel de sécurité de leur ordinateur.

L'hon. Laurie Hawn: Tout nous porte à croire que les chances de mettre la main sur Anonymous, quel que soit cet individu, sont très minces. Je suppose que cela dépend des cas, mais considérez-vous que les gens qui font de telles choses sont des professionnels ou plutôt des amateurs enthousiastes?

Mme Toni Moffa: On n'a pas besoin d'une grande compétence technique pour mettre en ligne une vidéo.

L'hon. Laurie Hawn: Il s'agit donc, probablement, d'amateurs enthousiastes.

Vous avez dit tout à l'heure que la détection des menaces informatiques et les mesures de défense ne relèvent pas du domaine public. Pourrait-on dire, sans entrer dans les détails, que le phénomène des menaces informatiques, tant dans le domaine public que privé, prend de l'ampleur? Pouvons-nous garder une longueur d'avance par rapport à ces menaces? À quel point cela pose-t-il problème?

Mme Toni Moffa: Non, je ne crois pas que nous ayons une longueur d'avance. Nous tentons d'en détecter le plus possible, mais le nombre de cas augmente de façon exponentielle. Étant donné le nombre de menaces, il est très difficile de soutenir le rythme.

L'hon. Laurie Hawn: Je vais m'arrêter ici.

Pour la gouverne des technophobes, dont je suis, pourriez-vous nous dire ce qu'est l'hameçonnage ciblé?

Mme Toni Moffa: L'hameçonnage ciblé est une technique. L'une des façons d'entrer dans le réseau informatique des gens et d'avoir accès aux données que contiennent leurs ordinateurs, c'est en leur envoyant un courriel semblable à un courriel ordinaire qui contient une pièce jointe très attirante pour eux. En cliquant sur le lien, l'utilisateur ouvre le fichier joint. Pour lui, rien n'a changé, mais l'ouverture du fichier a permis l'installation de programmes qui pourront être utilisés plus tard pour tirer des renseignements du réseau informatique.

L'hon. Laurie Hawn: Je ne voudrais pas avoir l'air trop paranoïaque, mais nous avons déjà parlé des petites clés USB. N'est-il pas inquiétant qu'on ne sache pas ce qui se trouve dans ces clés?

● (1140)

Mme Toni Moffa: Tout à fait. Plus on rattache de choses aux réseaux, plus ceux-ci sont vulnérables. Les clés USB et les dispositifs mobiles rendent les réseaux informatiques plus vulnérables parce qu'ils augmentent le nombre de voies d'accès.

L'hon. Laurie Hawn: Par conséquent, ne serait-il pas facile — non pas pour un amateur, mais pour un professionnel — de donner à quelqu'un une clé USB dans laquelle se trouve un programme qui s'activera lorsque la clé sera insérée dans un ordinateur?

Mme Toni Moffa: C'est possible.

L'hon. Laurie Hawn: Je vous remercie.

Le président: J'ai donné la parole à tous les gens qui voulaient poser des questions. S'il n'y a plus de questions pour les témoins, nous ferons une pause.

Je remercie les témoins de s'être déplacés.

J'invite le deuxième groupe de témoins à prendre place.

Nous prendrons une pause d'une minute ou deux le temps qu'ils s'installent.

Je vous remercie beaucoup de votre aide, aujourd'hui. Nous sommes heureux d'avoir pu entendre votre témoignage.

● (1140)

(Pause)

● (1140)

Le président: Nous passons maintenant à la deuxième partie de la séance.

Nous sommes en compagnie de Robert Gordon, du Centre canadien de réponse aux incidents cybernétiques, de James Malizia, du Service divisionnaire de la police de protection, et de Tony Pickett, de la Sous-direction de la criminalité technologique.

M. Gordon, avez-vous des observations préliminaires à présenter? D'accord.

Nous écouterons les observations préliminaires de la GRC, puis nous passerons aux questions.

Allez-y. Vous avez la parole.

M. Robert Gordon (conseiller sprécial, cybersécurité, Centre canadien de réponse aux incidents cybernétiques, ministère de la Sécurité publique et de la Protection civile): Monsieur le président, honorables membres du comité, je vous remercie de m'offrir l'occasion de vous adresser la parole aujourd'hui.

J'ai une petite correction à apporter. Je suis à la Direction générale de la cybersécurité nationale, qui relève du Secteur de la gestion des urgences et de la sécurité nationale, à Sécurité publique Canada. J'ai pris connaissance des délibérations du comité jusqu'à ce jour, et je pense qu'il pourrait être utile de vous donner d'abord un bref aperçu de la démarche gouvernementale dans le domaine de la cybersécurité. Puis j'exposerai le rôle du Centre canadien de réponse aux incidents cybernétiques (CCRIC), qui relève de la Direction générale de la cybersécurité nationale (DGCN), à Sécurité publique Canada.

Permettez-moi de vous parler d'abord de la Stratégie de cybersécurité du Canada, énoncée en octobre 2010 par l'honorable Vic Toews, ministre de la Sécurité publique. Cette stratégie renferme l'engagement du gouvernement à renforcer la sécurité et la résilience des systèmes essentiels du pays ainsi qu'une démarche pour y parvenir. Cette démarche se fonde sur l'idée que la sécurisation du cyberespace est une responsabilité partagée à l'égard de laquelle nous avons tous un rôle à jouer. En mettant en oeuvre cette stratégie, Sécurité publique Canada cherche donc à préciser les rôles et les responsabilités au sein du gouvernement du Canada, tout autant qu'à mettre en place les partenariats dont nous avons besoin avec d'autres ordres de gouvernement, le secteur privé, le monde universitaire et des alliés étrangers.

Permettez-moi de vous brosser un portrait général des ministères et des organismes qui tiennent un rôle opérationnel en cybersécurité, pour ainsi remettre en contexte le rôle respectif de Sécurité publique Canada et du Centre canadien de réponse aux incidents cybernétiques. Afin de contribuer à la mission de Sécurité publique Canada, qui consiste à bâtir un Canada sécuritaire et résilient, la Direction générale de la cybersécurité nationale dirige et coordonne l'élaboration et l'exécution de politiques et de programmes qui accroissent la résilience et la sécurité des systèmes vitaux, ainsi que de leurs informations, qui soutiennent la sécurité nationale, la sécurité publique et la prospérité économique du Canada. Au sein de la Direction générale de la cybersécurité nationale, le CCRIC est chargé d'aider à atténuer les incidents qui touchent des systèmes essentiels étrangers au gouvernement fédéral, à intervenir lorsque de tels incidents surviennent et à rétablir les activités normales. Vu que d'autres ordres de gouvernement et le secteur privé sont propriétaires de ces systèmes ou les exploitent, des partenariats sont indispensables pour en renforcer la sécurité. Par ailleurs, pour remplir son mandat, le CCRIC collabore étroitement avec des organismes fédéraux de renseignement et d'application de la loi ainsi qu'avec des alliés étrangers. En cas d'incident cybernétique national, le CCRIC assure également un rôle de coordination.

Le Centre de la sécurité des télécommunications Canada, qui a fait une présentation plus tôt aujourd'hui, Services partages Canada ainsi que les ministères et les organismes individuels (y compris Le Parlement) ont tous un rôle à jouer dans la prévention et la gestion des incidents cybernétiques qui peuvent se produire dans les systèmes du gouvernement fédéral. Deux autres organismes, à savoir Le Service canadien du renseignement de sécurité (SCRS) et la Gendarmerie royale du Canada (GRC), dont des représentants m'accompagnent aussi aujourd'hui, effectuent des enquêtes relatives à des systèmes tant à l'intérieur qu'à l'extérieur du gouvernement fédéral. Le SCRS fait enquête sur des activités cybernétiques qui soulèvent des préoccupations à l'égard de la sécurité nationale ou qui semblent reliées à des menaces contre la sécurité du Canada. Ses enquêtes visent à évaluer ces menaces et à renseigner Le gouvernement. Les organismes d'application de la loi, qu'il s'agisse de la GRC ou d'une force policière provinciale ou municipale, font enquête sur des incidents cybernétiques qu'on soupçonne être d'origine criminelle et qui proviennent du Canada ou de l'étranger. La GRC mène également des enquêtes criminelles qui relèvent de la sécurité nationale, puisque le SCRS n'a pas un mandat d'application de la loi. Les enquêtes relatives à l'application de la loi servent à amener des criminels devant les tribunaux.

Ces rôles et ces responsabilités doivent être clairs, non seulement pour des raisons d'efficacité et d'efficience, mais aussi pour qu'on intervienne rapidement lors d'incidents et qu'on y consacre tous les efforts possibles. À titre d'exemple, lorsqu'une enquête est lancée, on doit préserver les éléments de preuve pendant qu'on s'efforce d'atténuer les conséquences d'un incident et de rétablir les systèmes touchés. Et vu qu'une cyberattaque détectée sur un système a souvent des répercussions sur d'autres systèmes, il est indispensable de communiquer rapidement l'information entre le CSTC, pour qu'il protège les systèmes gouvernementaux, et le CCRIC, pour qu'il communique l'information à ses partenaires.

Je vais maintenant vous exposer plus en détail la façon dont le CCRIC accomplit son mandat, qui consiste à contribuer à la sécurité et à la résilience des systèmes cybernétiques qui sont essentiels à la sécurité nationale, à la sécurité publique et à la prospérité économique du Canada. À titre d'équipe nationale chargée des mesures de sécurité informatique, le CCRIC a un double rôle: premièrement, surveiller les menaces cybernétiques et proposer des mesures pour les atténuer et, deuxièmement, coordonner l'intervention nationale lors d'incidents majeurs dans le domaine de la sécurité cybernétique. À ce chapitre, le CCRIC est Ie centre canadien de prévention, d'atténuation et d'intervention en ce qui concerne les incidents cybernétiques.

● (1145)

Pour jouer son rôle, le CCRIC fournit des conseils d'expert et coordonne la communication de l'information et l'intervention de tous les ordres de gouvernement, de leurs pendants internationaux, des exploitants d'infrastructures essentielles, du secteur privé et de fournisseurs en technologie de l'information. Ces activités visent principalement à assurer une assistance et une coordination afin de résoudre l'incident et de rétablir des activités normales.

Le CCRIC n'est pas un organisme enquêteur et il n'a pas de pouvoirs d'application de la loi ou de réglementation. Le CCRIC agit selon le principe que la prévention et la préparation sont les moyens les plus efficaces de renforcer la cybersécurité au Canada. Il est un agent d'information fiable en ce qui concerne les menaces, les vulnérabilités et les techniques d'atténuation. Le centre possède ses propres capacités techniques et investit des efforts considérables pour établir des relations de confiance susceptibles de mener à l'échange de renseignements détaillés et à des mesures de suivi. Vu que ces relations donnent souvent lieu à la divulgation d'information que nos partenaires considèrent comme exclusive ou susceptible d'être dommageable pour leur réputation publique, nous en assurons jalousement la confidentialité.

Le CCRIC recueille et analyse de l'information confidentielle de source gouvernementale et autre. Il énonce ensuite des conseils d'atténuation et des pratiques exemplaires que ses partenaires peuvent mettre en application pour préserver leurs infrastructures cybernétiques tout en protégeant ses sources. En diffusant divers renseignements et en produisant divers guides, mais aussi par des séances d'information dans des cadres fiables, Sécurité publique Canada sensibilise également les gens à la nécessité d'en faire davantage en matière de cybersécurité.

Bref, lors d'un incident, le CCRIC collabore avec l'organisation touchée pour l'aider à reprendre ses activités normales, veille à informer ses partenaires fédéraux afin que ceux-ci sachent utiliser l'information reçue pour remplir leur mandat, puis fournit des conseils d'atténuation permettant à d'autres organisations et secteurs de prendre les précautions nécessaires.

Il se produit souvent des incidents et des attaques cybernétiques dont la gravité diffère énormément. Souvent, ils ne constituent qu'une nuisance et la communauté cybernétique est en mesure de se défendre elle-même. Néanmoins, certaines menaces cybernétiques sont susceptibles de prendre de l'ampleur. C'est pourquoi le CCRIC consacre du temps et des ressources pour rester vigilant à l'égard d'éventuelles menaces cybernétiques et de leurs possibles répercussions. Détecter tôt une menace cybernétique peut aider à mieux la comprendre et, donc, à mieux y faire échec si elle prenait de l'ampleur.

Enfin, les ministères et les organismes fédéraux prenant part à la sécurité cybernétique sont toujours déterminés à protéger les réseaux canadiens. Nous avons tous un rôle à jouer, mais collectivement nous devons nous rendre compte que notre sécurité cybernétique est une affaire de solidarité: si le gouvernement est touché, il est fort probable que d'autres organismes le seront aussi, et vice versa. En collaboration avec nos partenaires nationaux et étrangers, nous continuerons à recenser et à atténuer les menaces au fur et à mesure qu'elles se présenteront de manière à renforcer la sécurité des infrastructures numériques du Canada.

Je vous remercie de votre attention. Je me ferai un plaisir de répondre à toutes vos questions.

● (1150)

Le président: Je vous remercie.

Je donne la parole au commissaire adjoint Malizia.

Commissaire adjoint James Malizia (commissaire adjoint à la police de protection, Service divisionnaire de la police de protection, Gendarmerie royale du Canada): Je vous remercie, monsieur le président.

Le président: Votre exposé est court. Allez-y, je vous en prie.

Comm. adj. James Malizia: Oui, je vous remercie, et je remercie le comité de donner l'occasion à un représentant de la GRC de comparaître devant vous aujourd'hui.

Je suis accompagné du surintendant Tony Pickett, le directeur responsable de la Direction générale de la criminalité technologique à la GRC.

[*Français*]

Je vais tout d'abord aborder la question des menaces pesant sur le député de Provencher.

Les ministres fédéraux peuvent bénéficier de la protection de la GRC au Canada et à l'étranger, au besoin, en vertu de l'article 17 du Règlement de la Gendarmerie royale du Canada. Si un ministre ou un membre du Parlement croit que sa sûreté et sa sécurité sont menacées, il doit le signaler à la GRC ou aux autorités policières locales.

En se basant sur une évaluation des informations fournies, la GRC évaluera le besoin d'instaurer des mesures de sécurité. Si la demande est justifiée, la GRC peut ouvrir une enquête. Nous examinons et surveillons constamment les mesures de sécurité mises en place pour nos clients. Si nécessaire, nous ajusterons notre programme de sécurité en conséquence. Les mesures de sécurité dans leur ensemble sont fournies au cas par cas, fondées sur le renseignement et en rapport avec l'évaluation des menaces et des risques.

[*Traduction*]

Je vais tout d'abord aborder la question des menaces qui touchent le député de Provencher.

Les ministres fédéraux peuvent bénéficier de la protection de la GRC au Canada et à l'étranger, au besoin, en vertu de l'article 17 du règlement de la GRC. Si un ministre ou un membre du Parlement croit que sa sécurité est menacée, il doit le signaler à la GRC ou au service de police régional. À partir des renseignements fournis, la GRC évaluera le besoin d'instaurer des mesures de sécurité. Si la demande est justifiée, la GRC peut ouvrir une enquête.

Nous examinons les mesures de sécurité mises en place pour nos clients et en assurerons constamment le suivi. Si nécessaire, nous ajusterons notre programme de sécurité en conséquence. Les mesures de sécurité sont mises en oeuvre selon la situation. Elles se fondent sur les renseignements recueillis et sont proportionnelles aux menaces et aux risques évalués.

Nous prenons très au sérieux toutes les menaces qui pèsent sur les ministres et les députés quelle que soit la forme qu'elles prennent, par exemple une lettre, des propos de vive voix ou des messages publiés dans un média électronique ou social.

Le réseau Internet a révolutionné la façon dont nous communiquons et a transformé notre société. Il continue d'influencer la société à un rythme exponentiel. Ces nouvelles technologies en évolution ont amené plusieurs avancées: les communications instantanées dans le monde entier, la possibilité de mettre en commun des connaissances et de collaborer afin de faire plus efficacement du commerce, et j'en passe.

Néanmoins, l'envers de la médaille est que la technologie est utilisée à des fins de « cybercriminalité ». La GRC définit la cybercriminalité comme tout crime commis à l'aide d'un réseau informatique ou d'un périphérique. Le réseau ou le périphérique peut être l'agent, le facilitateur ou la cible du crime.

Les progrès technologiques ont créé un milieu où les gens peuvent rester anonymes. Les criminels exploitent le milieu anonyme pour dissimuler leur identité et mener des activités criminelles graves.

● (1155)

[*Français*]

Les criminels se réinventent sur Internet pour mettre en oeuvre des actes criminels liés, par exemple, à la fraude, au trafic de drogue, à l'exploitation sexuelle des enfants et au blanchiment d'argent. Parallèlement, les cybercrimes ont émergé, notamment le piratage et le vol de données. Dans ce cas, l'ordinateur, le réseau ou les données deviennent le centre de l'activité criminelle.

Comme vous le savez, Internet et les divers médias sociaux sont utilisés comme des moyens de promouvoir le changement social. Les individus et les groupes peuvent y exercer leur liberté d'expression. Cela peut être positif lorsque c'est fait de manière légale. Ces campagnes peuvent être comparées à des versions en ligne de manifestations sur la Colline du Parlement, à des pétitions ou à l'organisation de manifestations pacifiques.

[*Traduction*]

Les criminels se réinventent sur Internet pour mettre en oeuvre des actes criminels liés, par exemple, à la fraude, au trafic de drogue, à l'exploitation sexuelle des enfants et au blanchiment d'argent. Parallèlement, de nouveaux « cybercrimes » ont fait leur apparition, notamment Ie piratage et Ie vol de données, qui se rapportent aux ordinateurs, aux réseaux informatiques et aux données.

Comme vous le savez, Internet et les divers médias sociaux sont utilisés pour promouvoir le changement social. De plus, les particuliers et les groupes peuvent exercer leur liberté d'expression, ce qui peut être positif lorsqu'on le fait de manière légale. Ces campagnes peuvent être comparées à des versions en ligne de manifestations sur la Colline du Parlement, à des pétitions et à l'organisation de manifestations pacifiques.

La grande majorité des utilisateurs de médias sociaux ont des intentions positives et respectent la loi. Par contre, d'autres ont de tout autres objectifs et cherchent à réaliser leurs buts de façons très différentes. Certains groupes voudraient nous faire croire qu'ils sont l'unique agent du changement social. Selon ce que nous savons actuellement, certains de ces « cybergroupes » peuvent être décrits comme un mouvement où l'adhésion n'est pas définie. Ils offrent une tribune aux individus ou aux groupes qui partagent la même idéologie. Peu de ces individus ou de ces groupes se présentent comme des organisations criminelles, mais leurs tactiques peuvent parfois violer des lois dans des pays où ils comptent agir.

[*Français*]

La cybercriminalité se développe à une rythme alarmant partout dans le monde. Enquêter sur les menaces cybernétiques ou la cybercriminalité est un domaine en évolution et rempli de défis. Cependant, la GRC demeure engagée à faire respecter les lois, à appréhender les criminels et à garder le Canada sécuritaire et sécurisé.

[*Traduction*]

La cybercriminalité se développe à un rythme alarmant dans le monde entier. Les enquêtes sur les menaces cybernétiques ou la cybercriminalité sont un domaine en évolution et rempli de défis. Cependant, la GRC est déterminée à faire respecter les lois, à arrêter les criminels et à assurer la sécurité au Canada.

Je vous remercie.

Le président: Merci beaucoup. Je vous remercie tous les deux de vos observations préliminaires.

Nous passons aux questions des députés.

Vous pouvez commencer, monsieur Albrecht. Vous disposez de sept minutes.

M. Harold Albrecht: Je vous remercie, monsieur le président.

Jusqu'à présent, l'un des éléments les plus encourageants de notre enquête — pour moi, du moins — c'est la remarquable volonté de mettre en commun les renseignements. Monsieur Gordon, vous avez très clairement dit, à plusieurs reprises, que les différents groupes qui sont chargés de divers aspects de la sécurité ont un bon réseau de communication.

Dans la déclaration de la GRC, monsieur Malizia, vous avez souligné que vous prenez très au sérieux les menaces qui sont faites aux ministres et aux députés, qu'elles prennent la forme de lettres, de propos tenus de vive voix ou de messages publiés dans un média électronique ou social.

Je tiens à lire un message de menaces qui a été mis en ligne dans YouTube par le groupe qui se fait appeler Anonymous:

> Nous exigeons que vous laissiez tomber l'ensemble du projet de loi et que vous démissionniez de vos fonctions de ministre de la Sécurité. Nous savons tout de vous, M. Toews. À moins que vous ne laissiez tomber le projet de loi, nous révélerons les renseignements que nous avons sur vous au cours de l'opération White North.

Leur message se poursuit ainsi: « Anonymous demande la démission immédiate de Vic Toews, l'abandon de l'ensemble des projets de loi C-30 et C-11 [...] »

Selon moi, il est clair que M. Toews n'est pas menacé physiquement, du moins pas dans ce message. Par contre, étant donné, comme je l'ai dit tout à l'heure, que les législateurs sont élus pour améliorer la sécurité des citoyens grâce à l'élaboration de mesures législatives, il me semble qu'il y ait une atteinte directe à la démocratie. Par conséquent, ce message constitue, selon moi, une véritable menace, que tous les députés, surtout les ministres, doivent prendre au sérieux.

Monsieur Gordon, à la page 5 de votre déclaration préliminaire, vous dites que le CCRIC n'est pas un organisme enquêteur et qu'il n'a pas de pouvoirs d'application de la loi, ni de pouvoirs réglementaires. Plus haut dans le texte, vous dites:

> Les organismes d'application de la loi, qu'il s'agisse de la GRC ou d'une force policière provinciale ou municipale, font enquête sur des incidents cybernétiques qu'on soupçonne être d'origine criminelle et qui proviennent du Canada ou de l'étranger. La GRC mène également des enquêtes criminelles qui relèvent de la sécurité nationale, puisque Ie SCRS n'a pas un mandat d'application de la loi. Les enquêtes relatives à l'application de la loi servent à amener des criminels devant les tribunaux.

Je reviens à ce que je disais, à savoir qu'il s'agit vraiment d'une atteinte à la démocratie. En effet, on y empêche les parlementaires, par intimidation, de faire leur travail. On pourrait peut-être même dire que c'est une menace qui risque de décourager les gens qui songent à faire une carrière publique. À quel degré de criminalité associez-vous la mise en ligne d'une vidéo par le groupe qui se fait appeler Anonymous? La tenue d'une enquête criminelle est-elle nécessaire? Quel genre d'enquête faudrait-il mener pour tenter d'identifier les gens qui ont mis en ligne un message de menaces de ce genre?

Ma question s'adresse à qui voudra bien y répondre.

● (1200)

Comm. adj. James Malizia: Je vous remercie, monsieur le président.

Même si je ne suis pas en mesure de parler des enquêtes en cours, je peux dire, selon ce que nous savons actuellement, que certains de ces « cybergroupes » peuvent être décrits comme un « mouvement » où l'adhésion est non définie. Ils offrent une tribune pour des individus ou des groupes qui partagent des idéologies semblables. Peu de ces individus ou de ces groupes se présentent comme des organisations criminelles, mais leurs tactiques peuvent parfois violer des lois dans des pays où ils comptent agir.

Il est déjà arrivé que des enquêtes portant sur des menaces adressées à un ministre ou à un député donnent lieu à des accusations criminelles. Tout ce que je peux dire, c'est que la GRC lancera une enquête criminelle dès qu'on lui aura soumis les renseignements nécessaires.

M. Harold Albrecht: D'accord.

Vous avez aussi parlé de la communication de renseignements entre des pays étrangers. De quels moyens disposez-vous pour trouver l'origine, par exemple, des adresses IP ou des vidéos mises en ligne dans YouTube?

Comm. adj. James Malizia: Nous travaillons en collaboration avec des partenaires des forces de l'ordre du monde entier. Dans le dossier de la « cybercriminalité », nous nous servons du réseau Interpol, du réseau des agents de liaison de la GRC et du réseau du G8, qui est en service en tout temps et qui compte environ 60 États membres. De plus, les services de police communiquent des renseignements entre eux. Nous avons conclu des ententes de communication de renseignements avec les pays membres. Comme je l'ai dit tout à l'heure, la coopération internationale et la mise en commun des pratiques exemplaires nous permettent de collaborer et d'obtenir des résultats positifs.

M. Harold Albrecht: Voici ma dernière question. Le comité ne sait pas exactement comment on doit s'y prendre pour faire face à ce problème. C'est la première fois qu'une telle chose se produit. Je crois que nous avons dit tout à l'heure qu'il y a déjà eu des lettres anonymes. Par contre, le cas d'une vidéo mise en ligne dans YouTube, qui peut être vue par des milliers, voire des millions de personnes, est assez différent d'une lettre anonyme.

Selon vous, comment le comité pourrait-il atténuer les menaces formulées dans les messages mis en ligne, notamment celles qui sont faites aux fonctionnaires et aux élus dont la tâche est d'assurer la sécurité de tous les citoyens?

Comm. adj. James Malizia: Je m'en remettrais à mon collègue de Sécurité publique. Comme vous le savez, la « cybersécurité » ne relève pas de la GRC.

M. Robert Gordon: Comme quelqu'un l'a déjà dit, je crois que la mise en ligne d'une vidéo dans YouTube n'est pas un cas traditionnel dans le domaine de la « cybersécurité ». Sécurité publique Canada ne conseille donc rien à ce sujet. Nous avons donné des conseils sur la protection des différents réseaux, mais il est très facile de mettre en ligne une vidéo. Hélas, nous ne sommes pas en mesure de donner un conseil à ce sujet.

● (1205)

M. Harold Albrecht: Je révèle encore une fois mes faibles compétences techniques en ce qui concerne Internet.

Il n'y a donc aucun moyen technique de trouver l'adresse IP de la personne qui a mis en ligne le message de menaces qui pourrait en fait compromettre le poste d'un député ou d'un ministre?

Comm. adj. James Malizia: Ce que je peux dire, monsieur le président, c'est que chaque enquête est différente. Dans certains cas, selon la complexité de l'affaire, nous pouvons identifier les individus qui prennent part aux actes criminels et, dans d'autres, nous ne le pouvons pas.

M. Harold Albrecht: Je vous remercie.

Le président: Je vous remercie.

Monsieur Comartin, vous disposez de sept minutes.

M. Joe Comartin (Windsor—Tecumseh, NPD): Monsieur le commissaire adjoint, je veux que les choses soient bien claires, surtout pour les gens qui suivent le débat. Si je comprends bien, nous ne pouvez pas nous dire si la GRC mène une enquête sur cette affaire?

Comm. adj. James Malizia: Je crois comprendre qu'on a fait savoir qu'une enquête est actuellement en cours.

M. Joe Comartin: C'était ma prochaine question.

Lorsque le ministre a comparu au comité, il a dit qu'il avait demandé à la GRC de mener une enquête. Pouvez-vous le confirmer?

Comm. adj. James Malizia: Oui, nous avons reçu de l'information.

M. Joe Comartin: Pouvez-vous confirmer qu'une enquête est en cours?

Comm. adj. James Malizia: Je peux dire qu'une enquête est en cours.

M. Joe Comartin: Je vous remercie.

Je sais que vous ne pouvez pas donner de détails, mais y a-t-il d'autres organismes que la GRC qui prennent part à l'enquête visant à identifier la personne qui a mis en ligne la vidéo dans YouTube?

Comm. adj. James Malizia: Je ne suis pas en mesure de donner des détails sur l'enquête en cours.

M. Joe Comartin: Très bien.

Monsieur Gordon, supposons un instant qu'il n'y ait pas d'enquête en cours. Qui a la compétence d'investiguer sur un site comme celui-là? La GRC, le CST ou un autre organisme?

Qui est plus compétent pour faire une enquête?

M. Robert Gordon: Je ne suis pas certain de bien comprendre la question.

M. Joe Comartin: Permettez-moi de la reformuler.

Qui est le plus en mesure d'identifier la personne qui a mis en ligne la vidéo dans YouTube?

M. Robert Gordon: Je ne peux connais pas la réponse à cette question, mais peut-être que M. Pickett la connaît.

Surintendant Tony Pickett (officier responsable, Sous-direction de la criminalité technologiques, Gendarmerie royale du Canada): Je peux probablement répondre à cette question. Des groupes de spécialistes de divers ministères collaborent assez souvent dans ce genre de dossier.

La complexité de ces dossiers suggère habituellement que la source n'est pas unique, c'est pourquoi les ministères, et même parfois des organismes internationaux, des organismes d'application de la loi ou des organismes de renseignement, mettent souvent des ressources en commun.

Par conséquent, je dirais que l'expertise ne se trouve pas en un seul endroit. Nous devons examiner chaque dossier au cas par cas et nous adresser à d'autres ministères ou organismes fédéraux pour obtenir de l'aide dans ce genre de dossier.

M. Joe Comartin: Est-ce que cela peut aller jusqu'à s'adresser à d'autres pays?

Surint. Tony Pickett: Absolument.

M. Joe Comartin: Nous savons que des accusations ont été portées en Grande-Bretagne et au Royaume-Uni contre des personnes qui affirmaient faire partie d'Anonymous. Est-ce que ce genre de collaboration pourrait toucher à des affaires en cours dans d'autres pays et mener à partager des renseignements avec ces autres pays?

Comm. adj. James Malizia: Bien que je ne puisse pas me prononcer sur les enquêtes qui ont été menées dans d'autres pays, nous échangeons et partageons régulièrement des renseignements avec des organismes du monde entier, qu'il s'agisse de pratiques exemplaires ou de collaboration dans le cadre d'enquêtes.

● (1210)

M. Joe Comartin: Très bien.

Monsieur le commissaire adjoint, en ce qui concerne les accusations qui nous intéressent, pouvez-vous répondre à quelque question que ce soit en ce qui concerne le type d'accusations qui seront portées? Je suis désolé, car il en a été question lors de la dernière réunion en ce qui concerne le problème de dédoublement, c'est-à-dire que nous recommandions, faute de terme plus approprié, des mesures punitives émanant de la Chambre de Communes et que des accusations criminelles émanent du système de justice pénale. C'est votre côté de la pièce de monnaie.

Des analyses ont-elles été faites au sujet du type d'accusations qui pourraient être portées dans de telles circonstances?

Comm. adj. James Malizia: Comme vous le savez, il existe différentes accusations en vertu du Code criminel. Cela peut aller de l'utilisation non autorisée d'ordinateur, en vertu de l'article 342, aux menaces, en passant par l'utilisation, la possession et le trafic de mots de passe, les méfaits concernant des données, l'extorsion et l'intimidation. Il y a différentes possibilités qui s'offrent à nous en vertu du Code criminel.

M. Joe Comartin: Nous tentons ici d'établir une certaine chronologie, mais je sais que vous ne pourrez pas répondre à cette question, alors je ne la poserai pas.

En ce qui concerne l'enquête qui est en cours, y est-il question de menaces physiques? Vise-t-elle seulement les vidéos publiées sur YouTube?

Comm. adj. James Malizia: Ma position ne me permet pas de vous donner quelque renseignement que ce soit.

Le président: Je me disais que nous obtiendrions cette réponse.

M. Joe Comartin: Je savais que nous obtiendrions cette réponse, monsieur le président.

Le président: Il vous reste une minute si vous voulez...

M. Joe Comartin: Je n'ai plus de questions. Cela ne va nulle part.

Le président: Monsieur Easter, vous disposez de sept minutes.

L'hon. Wayne Easter: Merci, monsieur le président, et merci aux témoins pour leur présence.

Dans le cadre de ses questions, monsieur Albrecht a lu quelques-unes des menaces proférées sur YouTube. Il a pratiquement sous-entendu dans sa question que le fait de demander la démission d'un ministre devait être considéré comme une menace. J'espère bien que non. Je pense avoir demandé la démission d'un certain nombre de ministres et je ne veux pas sortir d'ici les menottes aux poings.

Je ne considère en aucune façon que le fait de demander la démission d'un ministre constitue une menace. Je pense que nous avons demandé la démission de quelques-uns d'entre eux.

Par ailleurs, dans votre allocution, vous avez dit que le ministre avait demandé la tenue d'une enquête. Dans la déclaration que vous nous avez présentée, monsieur le commissaire adjoint, vous avez dit, et je cite:

> Si un ministre ou un membre du Parlement croit que sa sûreté et sa sécurité sont menacées, il ou elle doit le signaler à la GRC ou à la police de juridiction locale.

Le ministre Toews a-t-il demandé cette protection de la police?

Comm. adj. James Malizia: Dans le passé, nous avons offert des services de protection à des ministres qui avaient reçu des menaces, selon les menaces en question. Les mesures de sécurité offertes sont variées. Bien entendu, nous continuons de faire le point, au moyen de l'évaluation des menaces et des risques, des menaces qui nous sont transmises, puis nous déterminons si des services de protection seront fournis.

Comme vous le savez, je n'ai pas le droit de parler des services de protection que nous offrons.

L'hon. Wayne Easter: Par conséquent, nous ne pouvons pas savoir si le ministre Toews a fait cette demande.

Je sais très bien comment fonctionnait la protection des ministres dans le passé.

Vous ne pouvez donc pas nous répondre. Nous savons que le ministre Toews a fait une déclaration à la Chambre et c'est la raison pour laquelle le comité examine ce dossier, mais vous ne pouvez pas nous dire si le ministre Toews a demandé par la suite de faire assurer sa sécurité.

Comm. adj. James Malizia: Ce que je peux vous dire, c'est que c'est la GRC qui détermine si des mesures de sécurité seront fournies après avoir fait une évaluation des menaces et des risques.

L'hon. Wayne Easter: D'accord. Merci.

D'après les témoignages qui ont été présentés précédemment par vos deux groupes, il me semble les divers organismes soient plutôt en mesure de faire face aux menaces contre le système. Certes, la GRC est en mesure de faire face aux menaces contre des personnes et c'est à vous de juger.

Est-il juste de dire que, à l'ère d'Internet, les divers appareils de sécurité et les divers organismes, sont davantage en mesure de faire face aux menaces contre le système dans son ensemble qu'à celles proférées contre des personnes? Les circonstances dans lesquelles cette menace a été proférée est une réalité différente.

Monsieur Gordon.

● (1215)

M. Robert Gordon: Monsieur le président, il s'agit probablement d'une bonne façon de distinguer les responsabilités d'une manière générale. Nous nous occupons de l'intégrité des données et des systèmes. Nous nous occupons de la confidentialité des données et veillons à ce que tout ce qui se trouve sur les systèmes demeure confidentiel. Nous nous occupons de l'intégrité des données, afin que personne ne puisse s'infiltrer et changer le contenu, ainsi que de la disponibilité des données, c'est-à-dire que vous ayez accès à vos renseignements de diverses façons. En effet, c'est une bonne définition.

L'hon. Wayne Easter: Monsieur Gordon, à la page deux de votre déclaration, vous dites que le CCRIC est chargé d'aider à atténuer les incidents qui touchent les systèmes essentiels étrangers au gouvernement fédéral, à intervenir lorsque de tels incidents surviennent et à rétablir les activités normales, et vous avez souligné le mot « étrangers ». Qu'en est-il à l'intérieur du gouvernement fédéral? Que s'y passe-t-il? Pourquoi avez-vous souligné le mot « étrangers »?

M. Robert Gordon: C'était essentiellement pour établir une distinction entre les rôles et les responsabilités du Centre de la sécurité des télécommunications, qui offre une expertise et des conseils techniques pour les systèmes du gouvernement du Canada, et les responsabilités de la Sécurité publique, qui concentre ses activités à l'extérieur du gouvernement fédéral et offre les connaissances et les pratiques exemplaires du gouvernement fédéral à une gamme de clients et de consommateurs externes, des gouvernements provinciaux et territoriaux à certains secteurs infrastructurels essentiels.

L'hon. Wayne Easter: Vous avez ensuite parlé de votre intervention relativement à des incidents cybernétiques. Je vais manquer de temps, alors je vais poser deux questions en même temps, monsieur le président.

En termes simples, pouvez-vous nous décrire le processus d'intervention pour ces incidents cybernétiques, qu'il s'agisse d'attaque contre le système, de tentative d'explorer des données, de tentative de déformer des données, de désinformation ou quoi que ce soit d'autre?

Ma deuxième question s'adresse plutôt à la GRC. Si, dans le dossier qui nous intéresse, l'identité d'Anonymous était dévoilée et que l'individu se trouvait juste au sud de la frontière ou ailleurs à l'étranger, quel serait le processus suivi? Comment faites-vous alors pour attraper l'individu, l'accuser d'un crime et l'obliger à subir les conséquences du crime ici, lorsque le crime est commis sur Internet, à l'extérieur du pays?

Il s'agit donc de deux questions, l'une pour monsieur Gordon et l'autre pour monsieur le commissaire adjoint.

M. Robert Gordon: Nous diffusons divers renseignements pour tous nos clients à l'extérieur du gouvernement fédéral, des réponses à des questions très techniques aux notes informationnelles plus générales, en passant par des renseignements ou des avis sur les points vulnérables que nous observons. Il y a donc une panoplie de produits.

Lorsqu'un incident, ou une série d'incidents, se produit, nous donnons aux organismes une marche à suivre qu'ils peuvent suivre pour rétablir leur système après des attaques de type spécifique. Nous leur envoyons une liste de contrôle pour qu'ils puissent régler ces incidents ou intervenir eux-mêmes lorsqu'ils se produisent.

L'hon. Wayne Easter: Monsieur Malizia.

Comm. adj. James Malizia: En ce qui concerne la façon dont nous travaillons avec nos partenaires internationaux, si des menaces émanent d'un autre pays, nous travaillerons avec nos homologues responsables de l'application de la loi pour pouvoir faire avancer l'enquête. Dans le cybermonde, plusieurs pays peuvent être en cause. Il se peut qu'il n'y ait pas seulement un pays.

L'hon. Wayne Easter: Puis vous passez...

● (1220)

Le président: Je suis désolé, monsieur Easter, vous avez largement dépassé votre temps de parole.

Monsieur Kerr, s'il vous plaît, vous avez quatre minutes.

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

Merci également de votre présence aujourd'hui.

Le processus d'aujourd'hui revient un peu à marcher sur des oeufs. Nous savons que vous venez ici avec une certaine appréhension parce qu'il y a des choses que vous ne pouvez par révéler. Nous en sommes conscients. Toutefois, vous comprenez aussi que nous avons besoin d'en arriver à un consensus quant à l'orientation que nous suivrons, c'est pourquoi nous continuons à vous presser de questions. J'apprécie donc votre prudence.

Dans ce contexte, de façon générale, comment traitez-vous les menaces dont les députés vous font part? Par exemple, si l'un d'entre nous croyait avoir un grave problème et allait vous voir, pourriez-vous le guider sur la façon de surmonter ce problème, si c'était le cas?

Comm. adj. James Malizia: Certainement. Merci, monsieur le président.

Comme vous le savez, les ministres de la Couronne ont le droit de recevoir la protection de la GRC au Canada et à l'étranger, le cas échéant, en vertu de l'article 17 du Règlement de la GRC. Il va sans dire que toute menace proférée contre un député fait l'objet d'une enquête de la police de juridiction. Selon la région, il peut s'agir de la GRC ou non.

Je le répète, lors de la réception de cette information, une évaluation des menaces et des risques est effectuée. Nous avons une équipe dévouée, au sein de notre appareil de sécurité nationale, qui procède à ces évaluations. Le dossier est examiné immédiatement dans la perspective des mesures de protections offertes par nos services et c'est à ce moment que nous déterminons si nous devons fournir des mesure de sécurité préventives, c'est-à-dire notre programme de protection, pendant que nous poursuivons l'enquête.

Nous continuons d'évaluer et de surveiller la situation au cours de l'enquête sur la menace. Je le répète, les mesures de sécurité seront adaptées en fonction du déroulement des opérations et en fin de compte, bien sûr, l'enquête se poursuivra de façon à déterminer si les preuves disponibles sont suffisantes pour porter des accusations en vertu du Code criminel.

M. Greg Kerr: D'accord. Merci.

Je suis certain que l'un des grands problèmes auxquels vous êtes confrontés dans un pays démocratique, c'est évidemment que la protection des renseignements personnels est un enjeu important. Les gens sont très sensibles à l'ingérence dans leurs affaires, leur utilisation d'Internet et ainsi de suite. Est-ce que cela constitue pour vous une frustration, un défi ou un problème important lorsque vous tentez parfois d'approfondir des questions que vous savez être préoccupantes? Je le répète, je comprends que nous parlons de façon générale, mais est-ce que l'existence des exigences en matière de protection des renseignements personnels représente une difficulté réelle lorsque vous tentez de trouver des réponses?

Comm. adj. James Malizia: Je peux dire qu'il y a des cas où nous sommes capables de réussir à suivre la trace et à identifier les contrevenants et, selon la complexité des dossiers, il y a des moments où nous n'y arrivons pas. Bien sûr, nous allons au devant de tous les outils et toutes les ressources modernes qui peuvent nous aider à faire face à l'évolution constante des crimes nationaux et transnationaux.

M. Greg Kerr: Je suis conscient que l'évolution est constante.

Je suis conscient que la protection des renseignements personnels est absolument essentielle à des fins de sécurité et pour de nombreuses autres raisons, mais, dans les nombreux dossiers au niveau international, constatez-vous une amélioration des pratiques exemplaires grâce aux rapports avec les intervenants d'autres pays? Autrement dit, comme je suis certain que tout le monde essaie d'être à l'avant-garde, est-ce que cela vous permet d'acquérir de nouvelles méthodes et de nouvelles procédures, ou d'être au fait des derniers développements? J'essaie évidemment de m'exprimer de façon très générale. Je me demande seulement si, en général, dans la perspective de la protection de nos concitoyens, vous apprenez beaucoup au contact d'autres partenaires du monde entier?

Comm. adj. James Malizia: Certainement, nous avons établi dans le monde entier des partenariats de confiance qui nous permettent de collaborer et de mettre des idées en commun dans divers domaines et pour diverses innovations en ce qui concerne les pratiques exemplaires.

M. Greg Kerr: D'accord.

Monsieur Gordon, avez-vous quelque chose à ajouter?

M. Robert Gordon: Nous avons de très bons accords de partage avec de nombreux pays. Ils se sont révélés très utiles et dynamiques, en ce qui concerne les pratiques exemplaires du point de vue technique, mais aussi du point de vue des politiques. À mesure que des pays élaborent des cyberstratégies, de nombreuses idées sont mises de l'avant et nous les mettons vigoureusement en commun. C'est donc un processus très utile pour nous.

M. Greg Kerr: D'accord. Merci.

Je n'irai pas plus loin de toute façon, monsieur.

Le président: Merci.

Madame Latendresse, vous avez quatre minutes.

● (1225)

[*Français*]

Mme Alexandrine Latendresse: Merci beaucoup.

Merci beaucoup d'être ici et de témoigner. Ce que vous nous dites est très intéressant, et il est bien d'en savoir plus à ce sujet.

Revenons au cas que nous devons étudier présentement. Nous parlons d'une vidéo qui a été mise en ligne sur YouTube. Pouvez-vous nous dire s'il y a des façons de retracer, entres autres, l'adresse IP de la personne qui a mis cette vidéo en ligne sur YouTube?

Comm. adj. James Malizia: Ma position ne me permet pas de donner des détails relativement au cas dont vous parlez.

Mme Alexandrine Latendresse: Je parle d'un point de vue général. Lorsque quelqu'un met une vidéo en ligne sur YouTube, y a-t-il une façon de retrouver son adresse IP?

Comm. adj. James Malizia: Ainsi que je l'ai mentionné au début, il y a des situations où nous sommes en mesure d'identifier les individus. C'est du cas par cas. Tous les cas sont uniques et certains sont complexes. Parfois, nous ne sommes pas en mesure de le faire.

Mme Alexandrine Latendresse: Vous avez beaucoup parlé des menaces qui peuvent être faites contre des ministres ou des députés. Continuons sur ce que disait M. Albrecht plus tôt.

Si un ministre venait vous voir demain matin avec une lettre anonyme écrite sur papier, contenant sensiblement le même genre de message, soit une demande de retirer tel projet de loi faute de quoi des choses seraient révélées sur lui, une investigation serait-elle éventuellement menée à ce sujet?

Comm. adj. James Malizia: Peu importe la forme de la menace que nous recevons — à titre d'information, bien sûr —, nous faisons une analyse et, si requis, nous procédons à une enquête criminelle.

Mme Alexandrine Latendresse: Que ce soit une lettre ou une vidéo anonyme, il peut y avoir investigation. Il n'y a pas de distinction fondamentale à ce sujet, n'est-ce pas?

Comm. adj. James Malizia: Vous voulez savoir si nous enquêtons dans les deux cas? Oui, nous enquêtons dans tous les cas.

Mme Alexandrine Latendresse: Ainsi, le fait que ce soit une vidéo dans le cas présent ne change rien à l'importance accordée à la menace.

Comm. adj. James Malizia: Je ne peux pas faire de commentaires sur le cas présent, mais je peux vous dire que nous allons enquêter dans les cas dont j'ai décrit la forme auparavant.

Mme Alexandrine Latendresse: J'imagine que vous avez vu la vidéo. Avez-vous vu la vidéo dont on parle et que nous sommes censés analyser pour déterminer s'il y a eu bris de privilège?

Comm. adj. James Malizia: Oui.

Mme Alexandrine Latendresse: Selon vous, cette vidéo contient-elle des éléments qui pourraient être matière à charge? On peut constater qu'il y a eu bris des règles parlementaires parce que la vidéo contrevient au droit d'un ministre ou d'un député de déposer un projet de loi. Toutefois, y a-t-il quelque chose dans cela qui relève d'un point de vue criminel?

Comm. adj. James Malizia: Ma position ne me permet pas de faire des commentaires sur une enquête criminelle qui est en cours.

Mme Alexandrine Latendresse: Y a-t-il quelque chose que ce comité peut faire par rapport à la situation présente?

Comm. adj. James Malizia: Nous encourageons les députés ou les ministres à rapporter les menaces qu'ils reçoivent pour que nous puissions faire enquête.

Bien sûr, notre mandat ne porte pas sur la cybersécurité. Je vais donc renvoyer la question à mon collègue de Sécurité publique Canada, qui est ici.

[*Traduction*]

M. Robert Gordon: La sensibilisation générale à la nature des menaces, ou des problèmes, est utile pour conscientiser les gens. Sécurité publique Canada se livre à une campagne d'envergure pour sensibiliser les Canadiens en général. Il est très utile de sensibiliser les citoyens à la nature des menaces et des risques, de façon préventive ou initiale, avant même que des incidents ne surviennent.

Le président: Monsieur Hawn, vous avez quatre minutes.

L'hon. Laurie Hawn: Merci, monsieur le président.

Je remercie aussi nos témoins de leur présence.

Monsieur Gordon, vous avez parlé des menaces qui visent les systèmes essentiels étrangers au gouvernement fédéral et M. Easter vous a posé une question à ce sujet. À votre avis, à quel niveau se situent ces vulnérabilités et quelles sont leurs tendances? Le nombre de menaces augmente-t-il? Est-ce que leur gravité va croissant? Avons-nous le contrôle de la situation?

M. Robert Gordon: Chaque jour, nous en apprenons davantage sur les menaces. L'une des méthodes que nous utilisons activement consiste à nous adresser au secteur privé par l'intermédiaire de divers forums des réseaux centraux des infrastructures essentielles que nous avons créés. Nous établissons un lien de confiance avec le secteur privé pour que les intervenants de ce secteur nous fassent part de leurs expériences. Nous mettons aussi en place des mécanismes qui permettent à ces intervenants de mettre en commun les types d'expériences ou de cyberattaques qu'ils observent. Ils apprennent donc les uns des autres et nous apprenons d'eux en même temps.

● (1230)

L'hon. Laurie Hawn: Je veux revenir aux observations de M. Albrecht et de M. Easter, à savoir si la menace proférée vise personnellement le ministre Toews. Je cherche à obtenir une opinion, mais, à mon avis, la menace ne vise pas seulement le ministre Toews, elle vise le système dans son ensemble.

Le ministre Toews n'est qu'un représentant d'un système et il fait quelque chose que quelqu'un n'apprécie pas. C'est le système qui est en cause, pas seulement le ministre Toews. À mon avis, la menace vise le système gouvernemental et non un seul ministre. Avez-vous une opinion personnelle à ce sujet?

M. Robert Gordon: Non, je n'ai pas d'opinion personnelle à ce sujet.

L'hon. Laurie Hawn: D'accord. Disons donc qu'il s'agit de ma propre observation.

Monsieur le commissaire adjoint, nous avons parlé des expériences d'autres pays et il s'avère que le FBI et d'autres organismes semblables ont connu un succès mitigé dans ce genre de dossier. Est-ce que la GRC a mené des enquêtes semblables récemment ou s'agit-il de la première enquête du genre à votre connaissance ou dont vous pouvez parler? Je ne demande pas de détails, mais seulement s'il y a eu d'autres enquêtes.

Comm. adj. James Malizia: Je peux dire que la GRC a mené des enquêtes de ce genre dans le passé. Comme nous l'avons déjà dit, notre sous-direction technologique est spécialisée dans ce genre de domaine.

L'hon. Laurie Hawn: Pouvez-vous nous donner une idée de la réussite ou de l'échec de ces autres enquêtes, ou nous dire si elles sont en cours?

Comm. adj. James Malizia: Bien entendu, je n'ai pas d'exemple à fournir au comité aujourd'hui, mais je peux affirmer qu'il y a eu dans le passé des enquêtes couronnées de succès.

L'hon. Laurie Hawn: Bien.

En ce qui concerne le point soulevé par Mme Latendresse quant au format de la menace, sur papier ou électronique, l'extorsion demeure de l'extorsion en vertu de la loi. Il importe peu qu'il s'agisse d'une lettre ou d'un courriel, n'est-ce pas?

Comm. adj. James Malizia: La GRC mènera une enquête peu importe le format.

L'hon. Laurie Hawn: Quelqu'un — je pense que c'était vous, monsieur le commissaire adjoint — a parlé de la méconnaissance de la loi. Ces gens ne se rendent pas compte qu'ils contreviennent à la loi. Je suppose que certains d'entre eux pourraient prétendre ignorer la loi et avoir été influencés par leur enthousiasme en faveur d'une cause quelconque en raison d'une certaine naïveté. Êtes-vous familier avec ce genre d'attitude? Quelqu'un pourrait dire: « Mon Dieu! Je ne savais pas, alors ça va. Vous ne pouvez pas engager des poursuites contre moi. »

Comm. adj. James Malizia: Il y a eu des cas où des personnes ont invoqué cette raison, mais il se peut aussi — et c'est ce que nous souhaitons dans les cas où nous avons des motifs valables pour porter des accusations — que cela ait un effet dissuasif.

L'hon. Laurie Hawn: Que pensez-vous des travaux en cours en ce moment? Je répète ce que j'ai déjà dit, je ne pense pas que nous avons de grandes possibilités de retrouver ces individus. Nous en trouverons peut-être un, mais qui sait combien d'autres il y a.

Pensez-vous que les travaux en cours contribuent à faire mieux comprendre aux gens que ce n'est pas un jeu, que ces actes sont des crimes et qu'ignorer la loi ne sera pas considéré comme une excuse? Est-ce que ce processus est au moins utile à cet égard?

Comm. adj. James Malizia: Ma position ne me permet pas de faire des commentaires sur les travaux du comité ni sur le processus, mais je peux dire que les avancées technologiques ont créé un environnement où les gens parviennent à devenir anonymes. Les criminels tirent évidemment parti de l'anonymat qu'offre Internet pour dissimuler leur identité et mener des activités criminelles graves. Nous entendons pourchasser sans réserve ces individus.

L'hon. Laurie Hawn: Donc, que vous soyez un professionnel ou un amateur enthousiaste, la loi vous traitera de la même façon.

Comm. adj. James Malizia: Oui.

L'hon. Laurie Hawn: Merci.

Le président: Monsieur Zimmer.

M. Bob Zimmer: Une fois de plus, merci de votre présence aujourd'hui.

Dans d'autres types d'activités criminelles, on parle d'agents d'infiltration. Cette question s'adresse plus particulièrement à M. Pickett. Utilisez-vous des agents anonymes chargés de l'application de la loi pour attirer les criminels ou attendez-vous qu'un crime soit commis?

Surint. Tony Pickett: Je suis désolé. Il serait inapproprié que je fasse des commentaires sur une technique policière.

● (1235)

M. Bob Zimmer: Je voulais quand même poser la question.

J'ai aussi une question au sujet de YouTube et des autres sites qui sont utilisés par divers groupes, comme Twitter et les autres. Ma question ne s'adresse pas nécessairement à M. Pickett, mais à n'importe quel membre du groupe. Est-ce que vous avez établi des relations avec ces sociétés ou ces entreprises afin que, si vous avez besoin d'accéder à certains renseignements liés à des activités criminelles, les liens créés disposent ces sociétés ou entreprises à partager des renseignements qui mèneront à l'arrestation du criminel?

Surint. Tony Pickett: Encore une fois, je ne peux pas faire de commentaires sur les relations que nous avons établies avec des entreprises en ce qui concerne les techniques que nous utilisons pour tenter d'arrêter des criminels ou de faire cesser des activités criminelles.

M. Bob Zimmer: D'accord.

J'aimerais aussi vous demander quels conseils vous donneriez aux Canadiens à l'égard de l'utilisation des médias sociaux. Quels conseils donneriez-vous à quelqu'un que vous considérez comme un ami — je ne dis pas que vous ne nous traitez pas comme des amis, mais donner des explications peut simplifier les choses — pour qu'il se protège le mieux possible, disons contre ce genre d'attaques?

M. Robert Gordon: Le site Web de Sécurité publique Canada offre des conseils pour le grand public, c'est-à-dire pour les gens qui ne sont pas des spécialistes des technologies de l'information, qui ne travaillent ni dans un service de TI, ni dans une société, ni dans un ministère.

Nous donnons au public des conseils sur les meilleurs moyens de se protéger.

M. Bob Zimmer: Pouvez-vous nous donner quelque avis aujourd'hui, comme ça, spontanément, quelques petits conseils?

M. Robert Gordon: Une chose consiste à veiller à ce que vos pare-feu soient mis à jour. Lorsque la société qui fournit votre pare-feu vous envoie une mise à jour, installez-la s'il vous plaît, parce que cette mesure repoussera effectivement un grand pourcentage des attaques qui pourraient autrement atteindre votre ordinateur.

Autre chose, avant de cliquer sur un fichier joint qui vous a été envoyé, pensez-y. Nous utilisons le dicton suivant: « Arrêtez et réfléchissez avant de cliquer. » Est-il raisonnable que la personne qui est censée vous avoir envoyé le courriel y joigne ce fichier? Parfois, nous devons enseigner cela à nos propres employés. Vous pouvez peut-être même téléphoner à la personne pour lui demander si elle a envoyé ce fichier avant de l'ouvrir. Cette mesure sera profitable à long terme, car elle permet d'empêcher un grand nombre d'attaques d'atteindre leur but.

M. Bob Zimmer: Certainement.

Une dernière chose.

Mon collègue, M. Hawn, a d'ailleurs déjà fait allusion à cela. Monsieur le commissaire adjoint, je pense que vous avez déjà répondu à cette question. Je m'adresse donc au reste du groupe. Quelles sont les chances que nous attrapions les gens qui représentent des menaces au XXI^{e} siècle? Avez-vous des données à ce sujet? Y a-t-il des chances qu'on les attrape ou quelles sont les possibilités?

Comm. adj. James Malizia: Je suis dans l'impossibilité de vous fournir des statistiques, mais je peux dire que chaque enquête est unique. Je le répète, nous sommes parfois en mesure d'identifier l'individu ou les individus, parfois nous ne le sommes pas.

M. Bob Zimmer: Il me semble que, comme vous l'avez dit précédemment, il y a des enquêtes où vous avez réussi à attraper le méchant.

Comm. adj. James Malizia: Oui, cela a été le cas.

Le président: Y a-t-il des questions? Monsieur Albrecht, vous avez quatre minutes.

M. Harold Albrecht: Merci, monsieur le président. Je ne pense pas que j'aurai besoin de quatre minutes.

Je n'ai pas de question à adresser aux témoins, mais je veux les remercier d'avoir comparu aujourd'hui et pour le grand professionnalisme de leurs réponses. Je veux réagir aux propos que M. Easter a tenus il y a quelques minutes, lorsqu'il a dit que le fait de demander à un ministre de se retirer ou de donner sa démission n'était certainement pas une menace. Je partage votre avis, monsieur Easter, mais cela est une toute autre chose que de menacer de révéler des renseignements personnels sur quelqu'un si cette personne ne retire pas la mesure législative qu'elle a présentée.

En tant qu'ancien ministre de la Couronne, je pense que vous devez savoir que menacer quelqu'un de publier des renseignements personnels, qui peuvent d'ailleurs avoir été obtenus par des moyens détournés comme le piratage de comptes personnels, tombe dans une catégorie tout à fait différente que de simplement prendre la parole à la Chambre et demander la démission d'un ministre. J'espère que vous êtes conscient de cela.

Merci.

Le président: D'accord.

Il n'y a plus personne sur ma liste et nous vous remercions de votre présence aujourd'hui.

Y a-t-il autre chose dans l'intérêt du comité aujourd'hui?

Je vous souhaite donc à tous de très joyeuses Pâques et nous vous reverrons à notre retour du congé.

La séance est levée.