CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent des comptes publics

PACP • NUMÉRO 086 • 1re SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le mardi 23 avril 2013

Président

M. David Christopherson

Comité permanent des comptes publics

Le mardi 23 avril 2013

● (1540)

[*Traduction*]

Le président (M. David Christopherson (Hamilton-Centre, NPD)): Je déclare ouverte la 86e séance du Comité des comptes publics de la Chambre des communes.

Chers collègues, je souhaite la bienvenue en votre nom à nos témoins. Ils sont nombreux à être concernés par le sujet et nous leur sommes reconnaissants d'avoir bien voulu se joindre à nous.

J'aimerais tout d'abord que vous nous excusiez de vous avoir fait attendre, mais une décision du président, suivie d'un vote, nous a retenus à la Chambre.

À moins que quelqu'un ne s'y oppose, nous allons commencer conformément aux procédures usuelles.

Selon l'information que j'ai ici, nous allons d'abord entendre la déclaration d'ouverture du vérificateur général. Ce sera ensuite au tour de M. Guimont, qui sera suivi des représentantes du Conseil du Trésor et de celle du Centre de la sécurité des télécommunications Canada. Le dernier témoin, mais non le moindre, sera le représentant de Services partagés Canada. Nous suivrons ensuite la rotation habituelle en prenant soin de ne pas dépasser les temps de parole.

À moins d'avis contraire, je cède maintenant la parole au vérificateur général du Canada, M. Ferguson, qui va prononcer sa déclaration d'ouverture.

Vous avez la parole, monsieur.

M. Michael Ferguson (vérificateur général du Canada, Bureau du vérificateur général du Canada): Merci.

[*Français*]

Monsieur le président, je vous remercie de nous avoir invités à témoigner aujourd'hui devant le comité pour discuter du chapitre de notre rapport de l'automne 2012 intitulé « Protéger l'infrastructure canadienne essentielle contre les cybermenaces ».

Je suis accompagné de Wendy Loschiuk, vérificatrice générale adjointe, et de Tedd Wood, directeur principal responsable de cet audit, qui a récemment pris sa retraite.

Nos travaux pour cet audit ont pris fin en juillet 2012. Par conséquent, nous ne pouvons pas commenter les mesures qui ont peut-être été prises depuis.

[*Traduction*]

Monsieur le président, la plupart des éléments de l'infrastructure essentielle du pays appartiennent au secteur privé ou aux administrations provinciales, mais le gouvernement fédéral a un rôle important à jouer pour aider à prévenir les cyberattaques et à réduire les vulnérabilités. En effet, il a accès à des sources d'information auxquelles les propriétaires d'éléments de l'infrastructure n'auraient peut-être pas accès. Il peut recueillir et analyser les renseignements sur les menaces et établir des partenariats avec des intervenants pour en faciliter le partage.

En 1999, le Comité spécial du Sénat sur la sécurité et les services de renseignements a recommandé que le gouvernement examine d'abord sa capacité d'évaluer et de réduire les vulnérabilités de l'infrastructure, et ensuite, sa capacité de prévenir les attaques matérielles et cybernétiques et d'intervenir le cas échéant. En 2000, le gouvernement a mis sur pied un groupe de travail qui était chargé de conseiller les ministres sur la façon de protéger l'infrastructure essentielle. Le groupe a constaté qu'il fallait mettre en place une stratégie nationale et, en 2001, le gouvernement a déclaré qu'il protégerait l'infrastructure essentielle en établissant des partenariats ainsi qu'en surveillant et en analysant les cybermenaces qui pesaient contre les systèmes fédéraux.

Monsieur le président, nous avons constaté qu'entre 2001 et 2009, le gouvernement a fait peu de progrès par rapport à ces deux recommandations, malgré la publication de plusieurs politiques et stratégies et un financement récurrent.

[*Français*]

Le recours à des réseaux sectoriels constituait un élément crucial des partenariats. Le gouvernement était censé établir ces réseaux et rassembler les intervenants clés avant mai 2011. Certains réseaux sont en place, mais il reste encore du travail à faire.

Le gouvernement avait recensé 10 réseaux sectoriels. Toutefois, seulement 6 de ces réseaux sectoriels comptaient des représentants de tous les groupes de l'industrie qui devraient siéger à la table, et seulement 5 d'entre eux avaient discuté de cybersécurité.

[*Traduction*]

Le gouvernement doit voir à ce que tous les réseaux sectoriels soient pleinement opérationnels. Nous avons relevé, par exemple, que le réseau sectoriel de l'énergie et des services publics est dynamique et que ses membres ont un niveau de satisfaction et d'engagement très élevé. À mon avis, cela montre que les réseaux peuvent fonctionner et représenter pour le gouvernement un moyen d'établir un partenariat avec les intervenants. Le gouvernement a accepté de donner des conseils sur la couverture appropriée des réseaux sectoriels d'ici décembre 2013.

[*Français*]

En 2005, le gouvernement a mis sur pied le Centre canadien de réponse aux incidents cybernétiques, qui devait surveiller et analyser les cybermenaces 24 heures sur 24 et 7 jours sur 7. Toutefois, le centre n'a jamais été ouvert selon l'horaire prévu. D'ailleurs, il n'a pas non plus de plan en ce sens, bien que, depuis notre audit, les heures d'ouverture du centre soient plus longues.

[*Traduction*]

Nous avons également constaté que le Centre canadien de réponse aux incidents cybernétiques ne disposait pas toujours d'un tableau d'ensemble de l'évolution des cybermenaces au pays et à l'échelle internationale, car il ne recevait pas toujours de l'information complète et opportune à ce sujet. Sans une connaissance exhaustive de l'évolution des cybermenaces, le centre peut difficilement analyser la situation et donner des conseils en la matière. Dans certains cas, les intervenants ne connaissaient même pas l'existence du centre et ignoraient son rôle.

Dans sa réponse à notre recommandation, le gouvernement a convenu d'augmenter la capacité opérationnelle et les autres capacités du centre. Depuis 2010, année du lancement de la Stratégie de cybersécurité, le gouvernement a réalisé des progrès. Il a créé Services partagés Canada pour regrouper certains services gouvernementaux en technologies de l'information. Le gouvernement s'attend à ce que cette initiative améliore la sécurité. Le Plan de gestion des incidents en matière de TI définit plus clairement les rôles et les responsabilités des principaux organismes fédéraux responsables de la sécurité. Un forum et des tribunes intersectoriels ont été tenus et un portail Web de partage de l'information a été créé.

Cependant, l'un des principaux défis que doit affronter le gouvernement est l'évolution rapide des cybermenaces. En fait, des cadres supérieurs nous ont dit craindre que les cybermenaces n'évoluent plus rapidement que la capacité du gouvernement à les neutraliser.

● (1545)

[*Français*]

Nous avons constaté que même s'il avait adopté des politiques et des stratégies pour donner suite aux préoccupations en matière de sécurité, Sécurité publique Canada n'avait pas publié de plans d'action pour recenser les priorités ni les échéanciers pour suivre la situation. Sans ces plans d'action, le ministère a eu du mal à évaluer ses progrès pour vérifier dans quelle mesure le gouvernement arrivait à ne pas se laisser dépasser par les cybermenaces. Dans sa réponse à notre recommandation, Sécurité publique Canada a convenu d'établir un plan d'action interministériel afin de mettre en oeuvre la Stratégie de cybersécurité.

Monsieur le président, je conclus ainsi ma déclaration d'ouverture. C'est avec plaisir que je répondrai aux questions des membres du comité.

Merci.

Le président: Merci, monsieur.

[*Traduction*]

Je vous remercie de votre exposé. Avant de poursuivre, j'aimerais mentionner que M. Reid remplace M. Williamson.

Je vous souhaite la bienvenue, monsieur. J'espère que vous vous plairez parmi nous.

M. Scott Reid (Lanark—Frontenac—Lennox and Addington, PCC): Merci.

Le président: Merci.

Monsieur Guimont, vous avez la parole.

[*Français*]

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

[*Traduction*]

Je suis heureux d'être ici pour discuter des progrès accomplis par Sécurité publique Canada en ce qui concerne le chapitre 3 du rapport d'automne 2012 du vérificateur général du Canada.

[*Français*]

Voici les fonctionnaires qui m'accompagnent.

De Sécurité publique Canada, nous avons Lynda Clairrmont, qui est sous-ministre adjointe principale, secteur de la sécurité nationale, ainsi que M. Robert Gordon, qui est conseiller spécial en cybersécurité.

De Services partagés Canada, nous avons M. Benoît Long, qui sous-ministre adjoint principal, Direction générale de la transformation, stratégie de service et conception.

Du Centre de la sécurité des télécommunications Canada, nous avons Mme Toni Moffa, qui est chef adjointe, Sécurité des technologies de l'information, de même que M. Scott Jones, qui est directeur général par intérim, cyberdéfense.

[*Traduction*]

Comme vous l'avez dit, je suis accompagné de Corinne Charette, dirigeante principale de l'information, et de Colleen D'Iorio, directrice exécutive, Sécurité et gestion de l'identité, toutes deux du Secrétariat du Conseil du Trésor.

Monsieur le président, j'accueille favorablement le rapport du vérificateur général, qui comprenait un certain nombre de recommandations importantes quant aux façons de maintenir la sécurité de nos cyberréseaux, tant à l'intérieur qu'à l'extérieur du gouvernement.

[*Français*]

Depuis octobre, mon ministère a réalisé de grands progrès, et aujourd'hui je dépose un plan d'action de la gestion qui donne un aperçu de nos prochaines étapes.

[*Traduction*]

Monsieur le président, la cybersécurité est une responsabilité que se partagent tous les ministères et organismes à tous les niveaux, les alliés internationaux, les partenaires de l'industrie et chaque Canadien.

Nous ne pouvons maintenir la résilience et la sécurité de nos réseaux qu'en utilisant une approche intégrée, telle qu'elle est établie dans la Stratégie de cybersécurité du Canada. La stratégie comprend trois piliers: protéger les systèmes gouvernementaux, nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral et aider les Canadiens à rester en sécurité en ligne.

[*Français*]

Le gouvernement fédéral a appuyé sa stratégie au moyen d'un financement considérable: un investissement de 90 millions de dollars au moment de son lancement et, tout récemment, la somme supplémentaire de 155 millions de dollars sur une période de cinq ans en vue de s'attaquer encore davantage aux cybermenaces en évolution.

[*Traduction*]

Je me servirai des deux premiers comme guides pendant que je discuterai de nos progrès liés au rapport du vérificateur général.

En ce qui concerne le premier pilier, le vérificateur général a demandé à Sécurité publique Canada d'élaborer un plan d'action public avec des produits à livrer et des échéanciers pour notre stratégie. Je suis heureux d'annoncer que ce plan a maintenant été élaboré et qu'il a été diffusé la semaine dernière. Il établit une approche active et axée sur les partenariats pour nous permettre de communiquer plus clairement nos progrès aux Canadiens, et fait ressortir la nécessité, pour tous les Canadiens et pour les propriétaires et les exploitants de systèmes essentiels, d'apporter leur contribution. En outre, nous avons élaboré, en collaboration avec des ministères et organismes clés, une stratégie de mesure du rendement horizontale qui nous aidera à faire le suivi de nos progrès dans les mois et les années à venir.

● (1550)

[*Français*]

En ce qui concerne le deuxième pilier, qui consiste à protéger les réseaux de systèmes essentiels à l'extérieur du gouvernement fédéral, le vérificateur général a recommandé que nous renforcions la capacité du Centre canadien de réponse aux incidents cybernétiques...

[*Traduction*]

Le président: Excusez-moi.

Pouvez-vous parler un peu moins vite pour aider les interprètes, s'il vous plaît?

M. François Guimont: Oui, bien sûr, je vais ralentir le rythme.

[*Français*]

Le CCRIC, notre centre,

[*Traduction*]

offre des conseils et un soutien, et coordonne l'échange de renseignements et la réponse aux incidents de cybermenaces touchant aux systèmes à l'extérieur du gouvernement fédéral.

Depuis octobre dernier, le CCRIC a entre autres réalisé ce qui suit. Il a mis en oeuvre un système national de notification des menaces d'incidents cybernétiques dans le but de fournir des avis automatiques des incidents cybernétiques aux propriétaires et aux exploitants de cybersystèmes essentiels. Il a également amélioré le dialogue avec ses partenaires à l'aide de renseignements et d'outils sur son site Web, y compris en établissant un portail de la communauté en ligne. Enfin, il a augmenté ses heures de fonctionnement à 15 heures par jour, sept jours par semaine, et il offre des services sur place, dans le but de couvrir toutes les heures d'ouverture de ses clients.

Au moyen d'un nouveau système téléphonique, le personnel du CCRIC est désormais accessible 24 heures sur 24, sept jours par semaine, afin de servir ses partenaires des secteurs public et privé. Il convient également de signaler que depuis le lancement de l'horaire de fonctionnement de 15 heures par jour, sept jours par semaine, en novembre, le CCRIC n'a reçu aucun appel en dehors de ces heures.

[*Français*]

Monsieur le président, dans les mois qui suivront, nous continuerons de renforcer l'engagement des sous-ministres provinciaux et territoriaux. Nous augmenterons également la fréquence de nos réunions avec le secteur de l'infrastructure essentielle afin d'accroître la sensibilisation aux cybermenaces.

[*Traduction*]

Et, finalement, nous continuerons de collaborer étroitement avec nos homologues de l'Australie, du Royaume-Uni, de la Nouvelle-Zélande et des États-Unis en vue d'échanger les réactions stratégiques et opérationnelles aux préoccupations en matière de cybersécurité.

Sur ce, monsieur le président, je vous remercie du temps que vous m'avez consacré. J'attends vos questions avec intérêt.

Le président: Merci.

Nous allons maintenant passer à Mme Charette.

Mme Corinne Charette (dirigeante principale de l'information, Secrétariat du Conseil du Trésor): Bonjour, monsieur le président.

Je suis ravie d'être ici pour discuter des progrès réalisés par le Secrétariat du Conseil du Trésor du Canada en ce qui concerne le chapitre 3 du Rapport du vérificateur général du Canada publié à l'automne 2012.

Comme l'a signalé le sous-ministre Guimont dans ses commentaires, la cybersécurité est une responsabilité partagée. À titre de dirigeante principale de l'information du gouvernement du Canada, je me suis engagée à ce que le secrétariat participe à la protection des systèmes d'information fédéraux contre les cybermenaces, qui sont en constante évolution. Dans son rapport de l'automne 2012, le vérificateur général a demandé au SCT de mettre à jour les politiques et les plans pertinents afin de tenir compte des nouveaux rôles et responsabilités de Services partagés Canada en matière de sécurité de la technologie de l'information.

Je suis heureuse de dire que nous avons déjà mis à jour le Plan de gestion des incidents en matière de technologies de l'information — le PGI TI — pour définir les rôles de SPC en la matière et que nous l'améliorons constamment. Nous procédons actuellement à l'actualisation de l'ensemble des politiques sur la sécurité afin d'y intégrer les rôles et responsabilités de SPC; les documents devraient être publiés cette année, comme prévu.

[*Français*]

Le vérificateur général a également noté que le SCT avait accordé une grande priorité à la communication pangouvernementale des pratiques exemplaires en matière de sécurité des TI. Ces efforts ont mené à la conception d'un programme de sensibilisation à la sécurité qui donnera au personnel du gouvernement une formation de base normalisée sur les principes de sécurité.

Nous continuons de coordonner nos efforts avec les principaux organismes chargés de la sécurité et tous nos partenaires de la collectivité de la sécurité, à la fonction publique, afin de renforcer notre sécurité de façon collective.

Monsieur le président, je vous remercie de cette occasion de m'adresser à vous. C'est avec plaisir que je répondrai aux questions des membres du comité.

● (1555)

Le président: Merci beaucoup.

[*Traduction*]

Nous allons maintenant passer à Mme Moffa. Vous avez la parole, madame.

[*Français*]

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

Bonjour.

[*Traduction*]

Conformément à son mandat en matière de sécurité des TI, le CSTC donne des conseils et des directives et fournit des services relativement à la protection de l'information électronique et des infrastructures d'information importantes pour le gouvernement. Il produit aussi des renseignements sur les cybermenaces étrangères. Nous communiquons l'information sur les cybermenaces et les conseils en matière d'atténuation à Sécurité publique, qui les communique à son tour à d'autres ordres de gouvernement et au secteur privé, s'il y a lieu.

Dans son rapport, le vérificateur général a dit craindre que le CSTC ne fournisse pas régulièrement au Centre canadien de réponse aux incidents cybernétiques de Sécurité publique de l'information opportune et complète sur les menaces contre les systèmes d'information du gouvernement du Canada. Le CSTC et le CCRIC entretiennent des liens étroits, et au moment de la vérification, les mécanismes de communication sécurisée pour la transmission de renseignements classifiés comportaient des lacunes.

Nous avons comblé ces lacunes, et nous accueillons maintenant deux jours par semaine un représentant du CCRIC au sein de notre Centre d'évaluation des cybermenaces, ce qui nous a permis de nous doter d'une capacité de communications vocales sécurisées en plus de rendre plus accessibles les communications informatiques sécurisées.

Le rapport fait aussi mention des fonds que le CSTC a reçus depuis 2001. Il en a investi une partie dans des activités visant à accroître la production de renseignements sur les cybermenaces étrangères. Nous avons amélioré la détection, l'analyse et l'atténuation des cybermenaces pour les systèmes fédéraux. Nous préparons également une formation à l'intention des praticiens du gouvernement fédéral appelés à intervenir en cas de cybermenaces. De plus, nous collaborons avec nos collègues du Conseil du Trésor et des Services partagés pour concevoir et développer des architectures sécurisées destinées aux systèmes gouvernementaux. Les fonds ont aussi servi à améliorer notre capacité globale à exécuter nos programmes à l'appui des activités menées dans le cadre de notre mandat, notamment celles qui sont liées à la cybersécurité.

Bien que la plupart des renseignements que nous produisons soient hautement classifiés, nous cherchons constamment à fournir de l'information sur les menaces et des conseils sur la sécurité des TI au-delà du gouvernement fédéral.

[*Français*]

Je vous remercie de votre attention. Je serai heureuse de répondre à vos questions.

Le président: Merci beaucoup.

[*Traduction*]

Nous allons passer à M. Long. Vous avez la parole, monsieur.

[*Français*]

M. Benoît Long (sous-ministre adjoint, Direction générale de la transformation, stratégie de service et conception, Services partagés Canada): Merci beaucoup, monsieur le président.

[*Traduction*]

Je suis ravi d'être parmi vous pour rendre compte des progrès réalisés par Services partagés Canada dans le cadre du rapport du vérificateur général sur la protection de l'infrastructure canadienne essentielle contre les cybermenaces, publié en octobre dernier.

Services partagés Canada a été créé le 4 août 2011 et a pour mandat de consolider et de moderniser l'infrastructure des TI du gouvernement du Canada, y compris en rendant plus sécuritaire l'infrastructure numérique qui soutient les systèmes du gouvernement, en particulier la messagerie électronique, les centres de données et les réseaux.

Le nouveau rôle évolutif de Services partagés Canada correspond aux recommandations du vérificateur général concernant la sécurité de l'infrastructure des TI. Le maintien de l'intégrité des infrastructures des TI essentielles du gouvernement du Canada est l'une des priorités du ministère.

[*Français*]

Service partagés Canada joue un rôle clé à quatre égards.

Tout d'abord, il agit dans la prévention des cybermenaces en utilisant des produits et des services d'infrastructure fiables ainsi qu'en faisant de la sensibilisation et en offrant de la formation sur la sécurité.

Deuxièmement, il joue un rôle dans la détection des cybermenaces et des intrusions abusives à l'aide de surveillance, de détection, d'identification, de priorisation et de signalement d'incidents en temps réel partout au sein du gouvernement du Canada. Cela comprend l'analyse judiciaire, l'analyse des journaux ainsi que les évaluations de sécurité et de vulnérabilité.

Troisièmement, Services partagés Canada joue un rôle en ce qui concerne les réponses et la coordination des réponses aux incidents de cybersécurité et de sécurité des TI, y compris les mesures correctives, l'évaluation des menaces, les communications et les analyses après incident ainsi que les reconfigurations et les remplacements.

Enfin, son rôle touche la reprise rapide des services, grâce à des services spécialisés de reprise après indicent de sécurité des TI, à des conseils et à de l'orientation en matière d'atténuation, ainsi qu'à la correction des vulnérabilités.

[*Traduction*]

Comme l'indique le rapport du vérificateur général, nous travaillons, avec les fonctionnaires du Secrétariat du Conseil du Trésor, aux recommandations comprises dans la vérification, dont la révision des politiques du gouvernement en matière de sécurité, afin qu'y soient pris en compte les nouveaux rôles et les nouvelles responsabilités de Services partagés Canada.

Services partagés Canada travaille aussi à l'amélioration de son Centre de protection de l'information, afin que ses 43 ministères clients puissent compter jour et nuit sur un organe de protection centralisé doté de meilleures capacités de rétablissement et d'une équipe spécialisée dans le rétablissement de la TI en cas d'incident. Dans le cadre de ce travail, nous procédons à la mise en oeuvre d'un système de rappel en cas de cyberattaque ainsi qu'à la mise à niveau des dispositions en matière de sécurité concernant l'acquisition de biens et de services.

En dernier lieu, Services partagés Canada travaille beaucoup avec ses ministères et organismes partenaires, tant sur le plan de la planification que sur celui du fonctionnement, afin d'assurer que la population canadienne continue de profiter de services de TI efficaces, sécuritaires et de haute qualité.

● (1600)

[*Français*]

Monsieur le président, je serai heureux de répondre à toutes les questions des membres du comité.

Le président: Merci beaucoup.

[*Traduction*]

Voilà qui met fin à nos observations préliminaires.

Maintenant, chers collègues, nous allons commencer l'alternance d'interventions habituelle, en commençant par M. Saxton.

Monsieur Saxton, la parole est à vous.

M. Andrew Saxton (North Vancouver, PCC): Merci, monsieur le président.

Nous remercions les témoins d'être ici aujourd'hui. Mes questions s'adressent au sous-ministre de la Sécurité publique et à ses collègues.

Ma première question, monsieur le sous-ministre, porte sur le fait que le gouvernement libéral qui nous a précédés n'avait pas de stratégie en matière de cybersécurité. Pouvez-vous expliquer quand une telle stratégie a été mise en place?

M. François Guimont: Merci pour votre question. La stratégie a été présentée en 2010. À certains égards, elle tient compte des approches préconisées ailleurs dans le monde. Par conséquent, si l'on devait comparer la cyberstratégie canadienne avec ce qui se faisait dans d'autres pays au même moment, on s'apercevrait qu'il y a des ressemblances.

M. Andrew Saxton: Merci.

Pouvez-vous expliquer le rôle du Centre canadien de réponse aux incidents cybernétiques?

M. François Guimont: Tout d'abord, monsieur le président, il faut savoir que le centre, dont nous avons la responsabilité, s'attaque aux problèmes qui surviennent à l'extérieur. Par comparaison, le Centre de la sécurité des télécommunications Canada, le CSTC, traite des cybermenaces dont les systèmes gouvernementaux font l'objet et réagit en conséquence. Le CCRIC, notre centre de réponse, se concentre par conséquent sur les menaces extérieures, dans le secteur privé, les provinces et les territoires. Son action se fait donc, dans un premier temps, à l'échelle macro.

En deuxième lieu, le centre est chargé de répondre aux appels des victimes de cyberattaques dès qu'il les reçoit. Il aidera la victime — une société ou un particulier — à cerner le type de menace dont elle fait l'objet, à trouver la sorte de logiciel malveillant auquel elle pourrait avoir affaire. Lorsque cela est fait, le centre essaie de venir en aide à la victime, puisque celle-ci s'est adressée à lui pour l'informer du problème et solliciter son aide. Le centre fera ensuite le tri des renseignements recueillis en tentant de comprendre ce qui s'est passé afin d'en faire part aux autres particuliers et organismes susceptibles de subir le même sort, et pour les aider à se protéger. Donc, une partie du travail consiste effectivement à émettre des avis.

De mémoire, je crois que le centre a émis quelques 11 000 avis en 2012, et ce, à très grande échelle. Sa fonction se résume à peu près à cela. Il s'occupe aussi de formation, de communication et de partenariats. Et, comme je l'ai expliqué dans ma présentation, nous disposons maintenant d'un portail dans lequel notre personnel et le public en général peuvent trouver de l'information et des avis en matière de sécurité.

Pour conclure, je tiens à souligner que le site Web du centre a été utilisé, toujours en 2012, environ 227 000 fois, si je ne m'abuse. Il y a donc d'innombrables interactions avec les personnes qui cherchent des réponses à une foule de questions. Et on ne parle pas seulement de cyberattaques, mais bien de renseignements de toutes sortes.

Voilà, en résumé, les fonctions du CCRIC.

M. Andrew Saxton: Merci.

Je crois qu'il y a eu certaines questions concernant leurs heures d'ouverture. Pouvez-vous nous expliquer le niveau de service que le centre offre à la population?

M. François Guimont: Merci pour votre question.

Un peu plus tôt, j'ai dit que la cyberstratégie avait été déployée en 2010, et qu'elle disposait d'un budget de 90 millions de dollars. Lorsque le vérificateur général a présenté son rapport, la stratégie a pu bénéficier d'une injection de ressources supplémentaires de l'ordre de 155 millions sur cinq ans. Environ 13 millions sont allés au CCRIC pour lui permettre d'augmenter ses capacités tant pour la réponse aux menaces que pour l'exécution de son travail. Comme je l'ai mentionné dans ma déclaration, il y a aussi une nouvelle capacité « téléphonique », ce qui veut dire essentiellement que le centre répond aux appels 24 heures sur 24. Ainsi, il y a toujours un représentant du CCRIC pour répondre aux appels effectués en dehors des 15 heures, sept jours sur sept, et s'occuper des problèmes qui pourraient se présenter.

● (1605)

M. Andrew Saxton: Merci.

J'ai une question pour Services partagés Canada. Pouvez-vous expliquer le rôle que joue cet organisme pour protéger les systèmes gouvernementaux?

M. Benoît Long: L'organisme Services partagés Canada a été créé récemment. Notre mission première est de renforcer l'infrastructure existante.

Aujourd'hui, comme nous gérons l'infrastructure et les réseaux de 43 ministères, notre rôle est de surveiller les menaces qui pourraient mettre cette organisation en danger et d'y répondre. Notre habileté à cet égard s'améliore et elle a été augmentée dans le cadre de la stratégie que le gouvernement annonçait récemment, laquelle comprend un financement additionnel pour la mise en place d'une capacité de réponse consolidée et centralisée, et d'une protection disponible jour et nuit et à longueur d'année.

Le président: Désolé. C'est tout le temps que vous aviez, monsieur Saxton. Merci.

Passons maintenant à M. Allen. Vous avez la parole, monsieur.

M. Malcolm Allen (Welland, NPD): Merci, monsieur le président.

Merci à vous tous d'être là.

J'ai l'impression que j'aurais besoin d'un ordinateur pour suivre la trace de tout ce que chacun de vous fait. Je ne sais pas exactement comment garder le fil. Je crois qu'un organigramme pourrait nous aider, indiquant clairement qui fait quoi, où, et qui relève de qui. Pour dire vrai, tous vos témoignages nous indiquent que vous êtes très nombreux à vous occuper d'une foule de trucs, et je ne suis vraiment pas convaincu que vous vous parlez encore entre vous, mais il y a une quantité considérable de travail qui se fait.

Par votre entremise, monsieur le président, je crois qu'il serait extrêmement utile pour suivre ce qui se passe d'avoir une sorte de tableau qui pourrait nous indiquer qui fait quoi, qui est comptable à qui et ce que sont les systèmes en jeu.

Nous savons qu'il y a le CCRIC et le CSTC. Il y a Services partagés. Il y a un autre groupe là-bas, ailleurs. Il y a des partenaires participants et des partenaires non participants. À vrai dire, ce que j'ai entendu sur ces entités qui ont des parties ici, des parties là, dans différents organismes, et qui obéissent à différents ministères, à différents sous-ministres et à différents ministres du cabinet, m'apparaît un peu comme un salmigondis. Je ne vois pas d'organisme qui chapeaute le tout et le dirige. J'avoue que la situation n'a rien pour me rassurer.

Monsieur Ferguson, je crois que ce que vous essayiez d'indiquer dans votre rapport est que nous avons besoin de cybersécurité. C'est un outil essentiel à la fois pour le gouvernement et pour le secteur privé. Nous avons besoin d'un système qui puisse fonctionner pour les deux. Je crois que c'est ce que le rapport essaie d'établir. Je ne suis pas convaincu que nous ayons un système qui nous permette vraiment de comprendre qui s'occupe de tout ça.

Monsieur Ferguson, vous avez parlé du CCRIC et du fait que son mandat s'appliquait en tout temps. Êtes-vous toujours de cet avis, c'est-à-dire croyez-vous toujours que ce mandat devrait s'appliquer ou si c'est quelque chose qui ne vous préoccupe pas outre mesure? Nous avons entendu M. Guimont nous parler de l'augmentation des heures de service, mais il n'a rien dit sur l'objet du mandat.

M. Michael Ferguson: Merci, monsieur le président.

Au moment de la vérification, nous avons noté que le mandat du CCRIC était de fonctionner 24 heures sur 24, sept jours par semaine. Nous avons remarqué que ce n'était pas le cas à l'époque. Nous savons cependant que les heures d'ouverture du CCRIC ont été augmentées depuis.

Ce qui est important pour nous, c'est que l'on puisse comptabiliser les incidents en tout temps afin d'y réagir dès que possible. Que la solution soit d'avoir un centre de réponse aux incidents ouvert 24 heures sur 24, sept jours par semaine, ou quelque autre mécanisme, l'essentiel est de s'assurer qu'une protection soit offerte en tout temps.

Je ne peux pas vous dire de façon certaine ce qui s'est fait depuis la vérification ou si les modifications qui ont été apportées sont efficaces. Assurément, pour nous, ce qui importe le plus est qu'il y ait quelqu'un qui puisse recueillir l'information en permanence.

M. Malcolm Allen: Vous avez dit dans votre exposé, monsieur Guimont, que nous en étions à 15 heures par jour, sept jours par semaine, ce qui est une mise à jour par rapport à ce qu'indiquait la vérification. Je présume qu'il s'agit d'une amélioration. Nous sommes plus près des 24 heures que lorsque nous en étions aux huit d'hier. Du reste, vous avez maintenant un nouveau réseau téléphonique qui permet de joindre quelqu'un en tout temps.

Je regrette de faire montre de naïveté ou de désinvolture à ce sujet, mais pouvons-nous présumer que ce quelqu'un se tient éveillé à côté du téléphone? Qu'arrive-t-il si celui qui est de garde dort profondément et qu'il n'entend pas le téléphone sonner? Qu'avons-nous réussi? Je crois qu'il est facile de répondre à cela: pas grand-chose. Je vais répondre à ma propre question.

Le fait demeure, monsieur, croyez-vous que quelqu'un qui est vraiment en devoir, et pas seulement sur appel...? Ce sont deux choses distinctes. Être sur appel signifie que vous êtes disponible. Je présume que les 15 heures dont on parle ne sont pas durant la nuit, cette période habituellement visée par le travail sur appel. Affirmez-vous que les personnes qui travaillent sur appel sont censées être éveillées à ce moment-là? Cela signifie-t-il qu'ils travaillent durant ce quart, à regarder le téléphone pour voir si quelqu'un appelle?

● (1610)

M. François Guimont: Merci pour votre question.

Tout d'abord, au cas où vous voudriez savoir pourquoi nous avons porté nos heures de service à 15, sachez que la formule 15-7 vise à couvrir nos fuseaux horaires d'un océan à l'autre. Deuxièmement, nous avons recherché un équilibre entre l'offre de bonnes ressources à l'intention des usagers et la prestation de ce service adapté. Nous avons établi que la formule 15-7 assortie d'un service téléphonique 24 heures sur 24 convenait. Troisièmement, je veux signaler que, depuis que nous avons commencé à offrir ces services bonifiés, nous n'avons reçu aucun appel nous indiquant qu'il y avait un problème, ce qui fait que nous n'avons jamais été mis dans une telle situation.

Je ne sais pas ce qu'en pensent mes collègues, mais je n'ai eu vent d'aucun appel. Jusqu'à preuve du contraire, j'ose espérer que nous avons là ce qu'il faut pour bien répondre aux appels, le cas échéant.

M. Malcolm Allen: Nous ne faisons pas cela avec le service des incendies, monsieur. Ils ne sont pas sur appel. Nous les faisons attendre à la caserne au cas où il y aurait un feu, mais en souhaitant qu'il n'y en ait pas. Je fais un parallèle avec des menaces à la sécurité parce qu'il n'y en a pas eu, mais il pourrait y en avoir.

Le président: Merci, monsieur Allen.

M. Malcolm Allen: Cela veut dire qu'il nous faut quelqu'un sur place, en chair et en os.

Le président: Merci, monsieur Allen. Votre temps est écoulé.

Passons maintenant à M. Kramp. La parole est à vous, monsieur.

M. Daryl Kramp (Prince Edward—Hastings, PCC): Merci, monsieur le président.

Encore une fois, un grand merci à tous nos témoins de nous honorer de leur présence. Ce qui m'a frappé, bien entendu, c'est toute la différence entre la technologie d'il y a 20 ans et celle d'aujourd'hui. Si vous aviez parlé de cybersécurité à cette époque, les gens auraient froncé les sourcils en vous demandant de quoi il s'agissait. Maintenant, avec la mondialisation des technologies de l'information, et ainsi de suite, la donne est complètement différente, et il est à mon sens inconcevable d'espérer pouvoir faire le travail seul. C'est là où les partenariats avec le public s'avèrent tout à fait cruciaux eux aussi.

Considérant que l'humain est un animal grégaire, nous devons selon moi aller chercher tout l'apport que nous pouvons d'autres domaines que nous n'avons même pas envisagés. La vérité est que la technologie en ligne touche vraisemblablement à toutes les sphères de l'activité humaine. Nous devons par conséquent pouvoir compter sur la collaboration du public pour nous aider.

Où les Canadiens peuvent-ils aller pour en savoir davantage sur la cybersécurité? Qui les avertira des risques et des moyens par lesquels ils pourraient contribuer à régler certains de nos problèmes? Nous devons être en mesure d'inciter les Canadiens à nous aider. Comment le faites-vous?

M. François Guimont: Merci pour cette question.

Monsieur le président, permettez que je revienne sur ce commentaire voulant que les choses aient beaucoup changé depuis 20 ans. Lorsque je faisais de la science et que je voulais faire montre de mes capacités au personnel qui tentait de me mettre au courant des « cyberenjeux », j'évoquais le fait que j'avais appris le Fortran et l'APL. Et ils me regardaient comme si j'étais arrivé d'une autre planète. Oui, les choses ont beaucoup changé. Je ne sais même pas si ces langages existent encore.

Pour en revenir à la question, le troisième volet de notre cyberstratégie consiste à donner le pouvoir aux Canadiens de poser les bons gestes. Je trouve que la question renferme un précieux énoncé qu'il importe de comprendre. Cela renvoie aussi à la question soulevée plus tôt au sujet des règles et des responsabilités. Nous sommes très nombreux à être concernés par ces enjeux, et cela n'est pas sans raison. Nous avons tous notre mot à dire sur la cybersécurité. Ce qui est vrai pour le gouvernement l'est aussi pour la société. Nous avons besoin du secteur privé — la grande, la moyenne et la petite entreprise —, de nos collègues des provinces et des territoires et de tous les Canadiens, du premier au dernier. Le troisième volet porte justement là-dessus, et je crois qu'il est juste de dire que nous avons une campagne très active sur la cybersécurité qui interpelle toute la population. Autrement dit, des trucs et des notions ont été suggérés, et les Canadiens devraient se les permettre.

Les membres du comité sont probablement au courant, contexte oblige, que c'est maintenant 80 p 100 des Canadiens qui se servent d'Internet, soit pour le commerce, soit pour des raisons sociales, alors l'exposition aux risques est très grande. Le gouvernement n'est pas là pour tout faire à leur place ou pour leur dire quoi faire, d'où la grande importance du volet de la cyberstratégie visant à responsabiliser les Canadiens. Nous avons préparé une campagne et nous y avons consacré des ressources, mais, au final, c'est à chaque Canadien et à chaque Canadienne d'assumer ses responsabilités, et c'est parfait qu'il en soit ainsi.

● (1615)

M. Daryl Kramp: Merci.

Faire participer les Canadiens, c'est une chose, mais jusqu'où devons-nous aller à cet égard? Ce qui me préoccupe, bien entendu, c'est qu'Eaton n'informe pas Simpsons de ses activités. Il y a beaucoup de personnes qui pourraient être plus nuisibles s'ils avaient une quantité phénoménale de renseignements. Donc, nous ne voulons pas les aider et les encourager. De quelle façon pouvons-nous protéger l'intégrité de ce que nous essayons de faire tout en maintenant la transparence au sujet de notre capacité, sans pour autant donner trop d'informations aux personnes qui pourraient en faire mauvais usage? Comment détermine-t-on cette limite? Qu'en pensez-vous?

Je ne suis pas certain de savoir qui serait le mieux placé pour répondre.

M. François Guimont: Si vous le permettez, monsieur le président, je demanderais à Mme Clairmont de répondre.

Mme Lynda Clairmont (sous-ministre adjointe principale, Secteur de la sécurité nationale, ministère de la Sécurité publique et de la Protection civile): Pour ce qui est de la sensibilisation, il y a sur le site Web de la Sécurité publique, il y a ce qu'on appelle « Pensez cybersécurité », un site Web où les citoyens peuvent trouver divers conseils sur ce qu'ils peuvent faire pour rester en sécurité. Nous adoptons le même point de vue que vous, en ce sens qu'il s'agit d'un partenariat. Il nécessite la participation du secteur privé, des divers ordres de gouvernement et des citoyens.

De plus, nous avons un lien avec « Stop. Think. Connect. », un programme de sensibilisation à la cybersécurité coparrainé en partie par des entreprises du secteur privé aux États-Unis. Le département de la sécurité intérieure des États-Unis permet aussi aux citoyens d'évaluer leur profil de risque cybernétique.

M. Daryl Kramp: Très bien. Merci.

Monsieur Long, le gouvernement a présenté l'initiative de services partagés en 2011 dans l'intention, manifestement, d'améliorer la sécurité des technologies de l'information. Avez-vous réussi à établir l'équilibre nécessaire entre la sécurité et la transparence? Quels sont vos commentaires à ce sujet?

M. Benoît Long: Je vous remercie de la question; je vous en suis reconnaissant. Oui, le mandat de Services partagés Canada décrit clairement les étapes que nous devons suivre pour assurer la sécurité des infrastructures. Donc, nous avons déjà commencé la consolidation de cette infrastructure dans 43 ministères en harmonisant les pratiques et les approches adoptées dans chaque ministère pour sécuriser ces systèmes.

Comme vous pouvez l'imaginer, avant la création de notre organisme, chaque ministère faisait de son mieux, à sa façon. Le financement et l'effort varient d'un ministère à l'autre. De toute évidence, nous sommes maintenant capables de le faire de façon horizontale pour assurer l'uniformité et aussi pour assurer la conformité aux normes établies par le Conseil du Trésor. Il s'agit d'un important pas en avant.

Actuellement, nous procédons aussi à la refonte de ces services de façon à intégrer la sécurité à la conception, pour intégrer les principes de sécurité, pour intégrer la sécurité en fonction de la façon dont ces services seront utilisés au gouvernement, ce qui est un aspect assez important.

Enfin, j'ajouterais que du côté de l'approvisionnement, nous avons amélioré les exigences existantes en matière de sécurité dans le but d'assurer la sécurité des biens et services que le gouvernement acquiert par l'intermédiaire des ministères. Cela permettra d'améliorer la capacité de déploiement et d'assurer la sécurité du matériel et des services qui y sont liés.

Le président: Très bien. Merci; le temps est écoulé.

Madame Blanchette-Lamothe, la parole est à vous.

[*Français*]

Mme Lysane Blanchette-Lamothe (Pierrefonds—Dollard, NPD): Merci.

J'aimerais parler un peu des réseaux sectoriels. Tout d'abord, on dit que Sécurité publique Canada devrait s'assurer que tous les réseaux sectoriels sont pleinement établis et fonctionnels, comme le prévoit la stratégie nationale et le plan d'action.

Ma première question est simple. Les 10 réseaux sectoriels sont-ils maintenant fonctionnels? Pouvez-vous me fournir de l'information sur cette évolution?

M. François Guimont: À ma connaissance, les 10 réseaux sont actifs. Les observations du vérificateur général étaient, jusqu'à un certain point, liées au fait que les secteurs n'étaient pas tous égaux.

Nous travaillons en ce moment à élaborer un document qui donnera des directions, car tous ces secteurs ne sont pas gérés par Sécurité publique Canada. Nous avons une table intersectorielle que nous présidons, où les membres viennent et où on peut coordonner notre travail, mais différents secteurs sont gérés par différents ministères. Nous travaillons donc à élaborer un guide, qui sera réalisé en décembre 2013. Une version brouillon sera disponible en juin 2013. Cela aidera les différents ministères à s'assurer que les secteurs sont complets et que les activités dans ces secteurs le sont également.

Les secteurs ont aussi une certaine responsabilité. Il n'incombe pas seulement au gouvernement de rassembler ces gens; ils doivent aussi créer les liens dont ils ont besoin à l'intérieur de leur secteur pour s'assurer d'une bonne représentation. Nous allons donc augmenter le nombre de réunions, car je crois que c'est important. Ces secteurs ne travaillent pas seulement sur le cyberespace, mais touchent à l'infrastructure en général. Nous augmenterons donc la place accordée à la question du cyberespace dans ces tables d'infrastructure.

On fait ce qu'on doit faire par rapport aux observations du vérificateur général, qui dans ce domaine étaient appropriées, selon nous.

● (1620)

Mme Lysane Blanchette-Lamothe: J'imagine que vous avez abordé la question des représentants qui siègent à ces réseaux sectoriels. On voit que 6 réseaux sectoriels sur 10 n'ont pas de représentants de tous les groupes de l'industrie considérés comme les principaux intervenants.

Dites-vous que vous n'avez aucune responsabilité par rapport à cela et que rien ne sera mis en place pour améliorer la participation aux réseaux sectoriels?

[*Traduction*]

Mme Lynda Clairmont: Je suppose que la question était de savoir si tous les intervenants de divers secteurs participent aux réseaux sectoriels.

Parmi les choses que nous faisons — et que nous pourrons terminer en juin prochain —, nous communiquons avec les secteurs et les ministères qui y participent et nous cherchons à savoir s'ils ont un nombre adéquat de membres pour chacun des réseaux sectoriels. Je veux simplement confirmer que nous avons entrepris ces travaux.

[*Français*]

Mme Lysane Blanchette-Lamothe: Et si la composition de ces réseaux n'est pas satisfaisante, allez-vous prendre une part de responsabilité et vous assurer que tout sera fait pour qu'elle soit satisfaisante?

[*Traduction*]

Mme Lynda Clairmont: Oui, tout à fait. Il s'agit toutefois d'un partenariat; nous voudrons donc consulter les secteurs, les secteurs privés, pour savoir qui, à leur avis, elle est placée pour le faire. De toute évidence, notre rôle est de coordonner ces choses et de nous assurer qu'elles sont mises en oeuvre, et c'est ce que nous faisons.

[*Français*]

Mme Lysane Blanchette-Lamothe: Serez-vous en mesure de nous tenir informés de votre progrès à cet égard?

[*Traduction*]

Mme Lynda Clairmont: Oui.

[*Français*]

Mme Lysane Blanchette-Lamothe: Merci.

Pour ce qui est du secteur privé, on constate que ce ne sont pas tous les acteurs qui se rapportent au CCRIC au sujet des attaques perpétrées. Cela semble être un problème. En effet, M. Ferguson mentionne dans son rapport que sans connaissance exhaustive de l'évolution sur le terrain, c'est difficile pour le centre d'analyser la situation et de donner des conseils en la matière.

Que pouvez-vous faire pour améliorer les rapports provenant du secteur privé?

[*Traduction*]

M. François Guimont: Si vous le permettez, monsieur le président, M. Gordon va répondre à cette question.

M. Robert Gordon (conseiller spécial, Cybersécurité, Centre canadien de réponse aux incidents cybernétiques, ministère de la Sécurité publique et de la Protection civile): Nous intervenons auprès des gens du secteur privé de deux façons.

D'abord, nous les encourageons en les informant des produits que le gouvernement produira en retour pour qu'ils connaissent l'importance de nous dire ce qui se passe. Leurs commentaires ont été très positifs. Le nombre de rapports que nous produisons chaque année a augmenté et le nombre de commentaires que nous recevons du secteur privé est en augmentation.

Récemment, j'ai assisté à une réunion de l'Association canadienne de l'électricité, où les gens se sont dits très heureux de la réponse du gouvernement. Elle a incité ses membres à fournir le plus de renseignements possible au gouvernement, car cela permet d'améliorer la qualité de l'information que le gouvernement pourra fournir.

Ces discussions continues ont entraîné une nette amélioration, en qualité et en quantité, des rapports que nous avons produits au cours des deux dernières années. Il reste encore beaucoup de travail à faire, et c'est ce que nous entreprendrons à mesure que nous avançons.

Le président: Merci. Madame, le temps est écoulé; je suis désolé.

Nous passons à M. Shipley. La parole est à vous, monsieur.

M. Bev Shipley (Lambton—Kent—Middlesex, PCC): Merci.

Merci aux témoins.

Dans son exposé, le vérificateur général a parlé des infrastructures essentielles qui appartiennent au secteur privé ou aux administrations provinciales. Le gouvernement fédéral a un rôle important à jouer pour aider à prévenir les cyberattaques et à réduire les vulnérabilités. Il a accès à des sources d'information qui pourraient ne pas être accessibles. Il peut recueillir et analyser les renseignements sur les menaces et peut établir des partenariats avec les intervenants.

Le gouvernement fédéral peut, de façon non directive, exercer un rôle important, une certaine autorité. Dans votre exposé, j'ai mentionné les partenariats. À votre avis, y a-t-il actuellement des partenariats adéquats entre le secteur privé et le gouvernement?

● (1625)

M. François Guimont: Je vous remercie de la question.

Je vais faire quelques commentaires, puis je céderai la parole à ma collègue, Mme Clairmont.

Étant donné l'environnement de la menace dans lequel nous évoluons, je pense que les partenariats et la collaboration dans tous les secteurs de la société — y compris une intervention plus directe auprès des Canadiens — doivent évoluer. Ce serait mon premier commentaire.

Deuxièmement, si nous voulons que les gens ou les entreprises se donnent les outils nécessaires et réagissent correctement, il leur faut être informés; je suis tout à fait d'accord sur ce point. Nous avons pris des mesures pour fournir aux gens des renseignements plutôt délicats qui doivent faire l'objet d'une autorisation de sécurité, ce qui leur permettra de connaître les menaces potentielles et de savoir si leur réaction est proportionnelle aux connaissances que nous avons de l'environnement.

Je cède la parole Mme Clairmont, qui vous donnera plus de renseignements à ce sujet.

Mme Lynda Clairmont: Je pense que nous intervenons auprès du secteur privé à plusieurs niveaux et de plusieurs façons.

Nous le faisons notamment par l'intermédiaire du CCRIC, de l'EIISI, l'Équipe d'intervention en cas d'incident de sécurité informatique. Comme M. Gordon l'a indiqué, en cas de vulnérabilité ou de problème lié à leur système, nous invitons les entreprises à communiquer avec nous par l'intermédiaire de ces organismes. Plus elles nous fournissent des renseignements, plus elles constatent que le CCRIC représente une valeur ajoutée et plus elles font appel à nous. Cela évolue aussi.

Nous avons affaire au secteur privé par l'intermédiaire des gens des secteurs des infrastructures essentielles, que nous rencontrons assez régulièrement. Dans le cadre de forums multisectoriels, nous tenons des séances d'information à divers échelons. Il y a aussi le forum intersectoriel, qui réunit les gens de tous les secteurs pour discuter de questions d'intérêt commun, dont la sensibilisation à la cybersécurité.

Nous continuons d'établir des relations avec divers intervenants, à divers niveaux, tant ici qu'avec nos alliés du secteur privé. Comme M. Guimont l'a indiqué, je pense que c'est un processus continu qui s'apparente davantage à un périple qu'à une destination, si vous me permettez de m'exprimer ainsi.

M. Bev Shipley: Merci beaucoup.

Cela aide à souligner quelque peu le besoin croissant de même que l'importance d'intensifier la collaboration avec le secteur privé et les autres ordres de gouvernement aussi, parce qu'il y a beaucoup de renseignements délicats que nous ne comprenons tout simplement pas ou auxquels nous n'avons pas accès.

Monsieur Guimont, j'aimerais revenir à vos commentaires sur le financement qui a été accordé, c'est-à-dire les 90 millions de dollars et la somme supplémentaire de 155 millions de dollars sur une période de cinq ans. Vous avez parlé des 15 heures, et vous avez brièvement décrit comment cela fonctionne, étant donné les différents fuseaux horaires que nous avons au Canada.

Pouvez-vous nous dire comment cela fonctionne vraiment, étant donné les différents fuseaux horaires que nous avons au Canada? La raison pour laquelle je pose la question, c'est que vous avez dit que pendant les heures creuses, il n'y a pas eu d'appel nécessitant une intervention. Je ne suis pas certain des mots exacts; j'ai donc utilisé une paraphrase.

Pourriez-vous m'aider à cet égard? Au pays, comment cela fonctionne-t-il, étant donné le décalage de quatre heures et demie entre les fuseaux horaires? Comment cela fonctionne-t-il, puisqu'il n'y a personne pendant ces heures creuses? Je sais que le système téléphonique est en place, mais...

M. François Guimont: Oui, certainement. Essentiellement, la formule 15-7 représente ce que j'appellerais une journée de travail typique, les heures ouvrables, d'un océan à l'autre. C'est le principe de base. Sept jours, c'est cela, exactement; donc, il s'agit d'une semaine complète.

Je vais laisser Mme Clairmont ou M. Gordon parler de... Quelqu'un doit être disponible pour répondre aux appels téléphoniques lorsqu'il y en a — probablement selon une rotation de personnel —, mais je vais laisser mes collègues en parler davantage.

M. Robert Gordon: Ma réponse comporte deux volets. D'abord, en plus du service de garde sur appel qui permet aux gens de communiquer par téléphone avec un membre du personnel des services d'intervention opérationnelle, nous avons aussi le Centre des opérations du gouvernement, qui fait également partie du ministère de la Sécurité publique, et où le personnel assure la permanence 24 heures par jour, sept jours par semaine. Donc, si jamais il nous était impossible de communiquer avec la personne qui est sur appel, il est possible de communiquer immédiatement avec une personne qui assure la permanence au Centre des opérations du gouvernement.

M. Bev Shipley: Est-ce un plan d'urgence?

M. Robert Gordon: Oui.

Mme Lynda Clairmont: Cela fait partie du ministère de la Sécurité publique.

M. Robert Gordon: Oui. Cela fait partie des paliers d'intervention. Donc, si un incident prend de l'ampleur, le Centre canadien de réponse aux incidents cybernétiques ferait appel au Centre des opérations du gouvernement pour élargir la portée de la réponse du gouvernement, de plusieurs façons, et aussi pour demander l'intervention des gens aux échelons supérieurs du gouvernement, si nécessaire.

L'autre aspect, c'est que lorsque nous traitons avec nos clients — les gens qui seraient susceptibles de nous appeler, les entreprises —, la nature des cyberattaques dont nous nous occupons est telle que l'attaque se produit sur une période donnée. Il est peu probable de pouvoir l'observer en temps réel. Donc, habituellement, dans les entreprises, les gens qui constatent ces problèmes travaillent le jour, ce qui signifie que nous travaillons essentiellement selon le même horaire, parce que la détection de ces attaques peut prendre plusieurs jours et que les entreprises elles-mêmes feront beaucoup d'analyse. C'est après avoir observé ces problèmes que l'on contactera le Centre canadien de réponse aux incidents cybernétiques.

Un programme similaire existe aussi chez nos alliés. Le Royaume-Uni, l'Australie et la Nouvelle-Zélande utilisent le même système.

● (1630)

Le président: Je suis désolé; le temps est écoulé, monsieur Shipley. Merci.

Monsieur Byrne, la parole est à vous.

L'hon. Gerry Byrne (Humber—St. Barbe—Baie Verte, Lib.): Merci, monsieur le président.

Ma question s'adresse au vérificateur général.

Monsieur Ferguson, pourriez-vous nous parler de la valeur des plans d'action pour le Parlement et pour vous en tant qu'agent du Parlement, dans le cadre de l'examen des progrès d'une vérification législative?

M. Michael Ferguson: Monsieur le président, je pense que je vais utiliser un exemple du chapitre dans lequel nous avons déterminé que ces plans d'action n'existaient pas au moment de notre vérification, de sorte qu'il nous a été impossible, en réalité, de mesurer les progrès réalisés à cet égard.

Je pense que cela résume bien la valeur d'un plan d'action. On y indique ce qui doit être fait et on précise à quel moment il faut le faire. Ensuite, on peut évaluer les progrès en fonction de cela.

L'hon. Gerry Byrne: Merci beaucoup.

À votre avis, serait-il vrai de dire que si un ministère est le principal objet d'une vérification ou qu'il en fait partie, mais qu'il n'est pas nécessairement la priorité... Par exemple, environ 13 ministères étaient inclus ou touchés par cette vérification de gestion en particulier.

Pour le Parlement et pour vous, en tant qu'agent du Parlement, serait-il utile que chaque ministère ayant fait l'objet de la vérification présente un plan d'action en réponse à une vérification législative?

M. Michael Ferguson: En général, cela dépendrait des recommandations que nous avons présentées. S'il s'agit d'un plan d'action en réponse à une de nos vérifications, nous nous attendons à ce que les ministères visés par nos recommandations présentent un plan d'action. S'ils estiment avoir besoin de plus de renseignements de certains autres organismes, nous nous attendons alors à ce qu'ils tentent de les obtenir.

L'hon. Gerry Byrne: Les plans d'action qui ont été présentés au comité aujourd'hui satisfont-ils à ces critères?

M. Michael Ferguson: Je ne peux donner mon avis à cet égard. Nous n'avons pas encore examiné les plans d'action en détail.

L'hon. Gerry Byrne: D'après ce que j'ai pu comprendre, les plans d'action ont été présentés tout récemment, mais le ministère de la Sécurité publique a indiqué que son plan d'action a été présenté la semaine dernière.

Monsieur Guimont, le plan d'action qui a été présenté au comité aujourd'hui est-il identique au plan d'action qui a été publié la semaine dernière?

M. François Guimont: Comme l'a demandé le comité, le plan d'action de gestion porte précisément sur chacune des recommandations du BVG, systématiquement. Nous l'avons déposé. Il a été préparé et présenté et, si je me rappelle bien, il a été mis en oeuvre, à l'exception d'une ou deux mesures.

L'autre plan d'action est le plan d'action plus exhaustif demandé par le BVG. Nous sommes tout à fait d'accord avec le vérificateur général. Il a fallu un certain temps, mais nous avons préparé le plan d'action, qui a été publié. Nous l'avons rendu public le 18 avril, je crois. En passant, il comprend des mesures pluriministérielles, ce qui signifie que les ministères sont tenus de mettre en oeuvre certaines mesures dans un délai donné. En fonction des recommandations du BVG, le tout est regroupé en fonction des divers piliers de notre stratégie, ce qui est logique parce qu'il s'agit de notre cadre de travail.

Les ministères, dont le mien, sont tenus de réaliser un certain nombre de choses. Nous avons regroupé les tâches existantes, les tâches permanentes et les tâches exécutées. En fin de compte, ce qu'il faut savoir, c'est que le plan d'action exhaustif comporte certains des éléments du plan d'action de gestion que nous avons présenté en réponse au rapport du BVG.

L'hon. Gerry Byrne: Merci beaucoup, monsieur Guimont.

L'un des problèmes, à mon sens, c'est qu'un comité parlementaire reçoit un plan d'action de deux pages afin que le Parlement puisse demander des comptes au gouvernement au sujet d'une question cruciale comme la cybersécurité. Mais ce que le ministère a rendu public, comme mode de communication, je présume, c'est un plan d'action plus complet, et les deux ne semblent pas concorder, selon moi.

Ce que nous avons ici est un élément du compte rendu, devant un comité parlementaire, mais ce que vous nous indiquez, c'est que vous avez préparé un plan d'action beaucoup plus complet qui n'a pas été déposé au Parlement. Or, nous sommes tout de même censés exiger cela de vous, n'est-ce pas?

● (1635)

M. François Guimont: En réalité, pour que ce soit bien clair, le plan d'action de la gestion présenté au comité selon vos exigences, que nous reconnaissons, prévoyait notamment l'élaboration d'un plan d'action plus complet. Notre plan d'action pour le BVG, pour le comité, a été préparé très rapidement, car il nous fallait pouvoir répondre aux diverses recommandations du BVG. Le plan d'action plus complet a été plus long à préparer. Il a fallu beaucoup de travail et de consultations pour en obtenir l'acceptation.

L'hon. Gerry Byrne: En tout respect, je dois vous interrompre. Vous avez dit avoir présenté le plan de gestion détaillé la semaine dernière et avoir présenté le plan d'action plus important au comité aujourd'hui.

Le président: Vous pouvez répondre, puis le temps sera écoulé.

Madame.

Mme Lynda Clairmont: Le plan que nous avons présenté au comité aujourd'hui est le plan d'action qui donne suite à la vérification, mais il ne s'agit pas du plan d'action qui tient compte de l'ensemble de la stratégie en matière de cybersécurité, lancée en 2010. Comme l'a dit M. Guimont, la stratégie de 2010 en matière de cybersécurité prévoyait un certain nombre de mesures en vertu des trois piliers. Le plan d'action qui a été publié sur le site Web, mentionné dans la vérification du BVG, est notre réponse à la façon dont le gouvernement expose les mesures prises à la suite de la mise en place de la stratégie.

Le président: Monsieur Byrne, vous pourrez prendre à nouveau la parole dans quatre interventions; si vous voulez alors revenir sur cette question, vous le pourrez.

Monsieur Aspin, la parole est à vous.

M. Jay Aspin (Nipissing—Timiskaming, PCC): Merci, monsieur le président.

Je souhaite la bienvenue à nos témoins.

Monsieur Guimont, j'ai moi aussi utilisé Fortran et APL et je partage donc votre étonnement.

Des voix: Oh, oh!

M. Jay Aspin: Le rapport du BVG parlait notamment des progrès relatifs aux secteurs des infrastructures essentielles. Pourriez-vous nous dire quels progrès ont été réalisés?

M. François Guimont: Certainement. Je vais dire quelques mots, puis céder la parole à Mme Clairmont.

D'abord, nous avons une table composée de 10 secteurs — transport, finance, énergie, production d'eau, par exemple. Il y en a 10.

Ensuite, nous avons une table intersectorielle, dans laquelle nous réunissons ces diverses tables sectorielles afin de créer un programme d'action commun.

Les trois fonctions de base de ces tables sectorielles ou intersectorielles concernent l'ensemble des infrastructures essentielles: les risques liés à de multiples dangers auxquels nous pouvons être confrontés. Ils sont liés à la cybersécurité, mais pas seulement à cela. Pour revenir à ce que je disais tout à l'heure, les cybermenaces prennent maintenant plus d'espace et de temps, et nous mettons l'accent là-dessus.

Nous établissons des partenariats et des relations par l'entremise de ces tables, en échangeant des renseignements afin d'informer les gens sur divers enjeux auxquels ils sont ou peuvent être confrontés. Nous échangeons ces renseignements et nous traitons en général de questions liées à la gestion des risques.

Je vais maintenant céder la parole à Mme Clairmont.

Mme Lynda Clairmont: En fait, Bob devait en parler.

M. Robert Gordon: Merci.

Nous avons pu prendre des mesures très précises en plus des mesures générales dont a parlé M. Guimont. Nous avons établi, en ce qui a trait à la gestion du risque, un certain nombre de guides et de guides de planification qui sont utiles à divers secteurs d'infrastructures essentielles.

Nous participons également à un plan d'action américain pour les infrastructures essentielles. Nous avons entrepris avec les Américains un programme d'évaluation de la résilience régionale dans lequel nous effectuons des évaluations transfrontalières. Par exemple, nous avons effectué six évaluations cette année au Nouveau-Brunswick. La première étape consistait à examiner les aspects physiques, notamment les sections transfrontalières ou les postes frontaliers à Woodstock et à Edmundston, le port de Saint John, les installations d'Irving Oil, et l'usine de GNL, où nous avons entrepris ces évaluations et fourni des conseils aux propriétaires et opérateurs de ces systèmes sur la façon d'améliorer la sécurité.

Nous allons maintenant le faire dans le reste du Canada. Nous menons un autre projet pilote en Ontario, et un autre en Saskatchewan. Nous ajouterons une cybercomposante.

Nous avons également créé un certain nombre d'initiatives d'échange d'information... un cadre pour orienter l'échange d'information au sein des secteurs d'infrastructures essentielles et des points d'accès pour l'échange de renseignements afin de faciliter certains de ces échanges également.

● (1640)

M. Jay Aspin: Merci.

Si vous le permettez, monsieur Guimont, je sais que vous y avez fait allusion plus tôt, mais j'aimerais que vous nous parliez plus précisément de ce que le gouvernement du Canada fait pour veiller à ce que les Canadiens puissent utiliser le cyberespace en toute sécurité.

M. François Guimont: C'est le troisième pilier. Nous avons un site Web pour la campagne, où les Canadiens peuvent poser des questions et obtenir des renseignements. Mais comme je l'ai dit plus tôt, même si nous leur fournissons ces renseignements, au bout du compte, ils doivent assumer certaines responsabilités, et je crois qu'ils le font. Les gens sont davantage sensibilisés aux cyberréalités qu'il y a cinq ans, ou peut-être trois ans. Honnêtement, c'est aussi en raison des reportages médiatiques.

Je vais céder la parole à Lynda ou à...

Mme Lynda Clairmont: Je peux commencer.

En plus d'avoir créé notre site Web Pensez cybersécurité et de participer à l'initiative Stop. Think. Connect., dont j'ai parlé tout à l'heure, nous collaborons aussi avec les États-Unis et d'autres pays alliés au mois de la sensibilisation à la cybersécurité, en octobre. Nous participons à toutes sortes d'activités avec le secteur privé et les citoyens afin d'améliorer la sensibilisation à la cybersécurité.

Par exemple, nous collaborons avec des magasins qui vendent beaucoup d'appareils de télécommunications — comme les iPods et les autres appareils qu'utilisent les jeunes. Il y a des renseignements sur la sécurité à l'intérieur, mais nous avons des dépliants que... Nous les distribuons afin que les parents les voient davantage, et pas seulement les enfants.

Il y a donc un certain nombre d'initiatives auxquelles nous travaillons et que nous coordonnons, tant sur le plan national, avec les provinces et les territoires, qu'à l'extérieur du pays, avec des partenaires internationaux.

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

M. Jay Aspin: Sommes-nous en sécurité dans le cyberespace?

M. François Guimont: C'est une question intéressante, car certaines menaces, dans l'environnement où nous vivons, changent peut-être un peu moins avec le temps.

M. Gordon et d'autres spécialistes m'expliquaient, madame Clairmont, que le monde virtuel évolue très rapidement. Quand on y pense, c'est un monde où les besoins sont limités. Il faut un minimum d'appareils techniques, de serveurs ou d'ordinateurs, d'intelligence et de temps libre, si je peux m'exprimer ainsi.

En ce sens, il s'agit d'une menace en évolution. Je pense que nous sommes tout aussi actifs. Nous avons une stratégie, des intervenants et des ressources. Je crois qu'il nous faut rester sur nos gardes. Le monde virtuel évolue rapidement, et nous devons tenir compte de cette réalité.

Le président: Très bien, merci.

Monsieur Guimont, je vous remercie d'avoir répondu brièvement.

Poursuivons. Monsieur Giguère, vous avez la parole.

[*Français*]

M. Alain Giguère (Marc-Aurèle-Fortin, NPD): Merci, monsieur le président.

Je remercie les témoins d'être ici.

Tout d'abord, j'aimerais que ce document-ci soit déposé. Il s'agit du Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada.

J'aimerais faire une observation à M. Guimont.

Vous soulignez, à la page 7 de votre rapport, que vous allez dépenser 155 millions de dollars en cinq ans, et à la page 6 de ce même rapport, il est indiqué que ce montant sera dépensé en quatre ans. Cela fait quand même une différence de 30 millions de dollars. J'aimerais qu'à l'avenir les chiffres soient un peu plus pondérés.

Monsieur le vérificateur général, vous avez indiqué au paragraphe 3.20 de votre rapport que depuis 2001, 780 millions de dollars avaient été dépensés. Vous avez même indiqué que vous aviez souligné qu'un budget de 200 millions de dollars approuvé spécialement pour la cybersécurité ne correspondait à aucun financement relié aux activités de protection contre les cybermenaces. C'est quand même beaucoup.

Peut-on savoir où est passé l'argent? Également, comment se fait-il qu'avec un tel budget, l'ensemble des services ne soit pas parvenu à établir un service de sécurité contre les cybermenaces?

● (1645)

[*Traduction*]

M. Michael Ferguson: Sur le plan du budget, ce que nous disons dans le chapitre, c'est que lorsque bon nombre de ces budgets ont été alloués, la cybersécurité était considérée comme faisant partie d'un système plus vaste de sécurité. Comme on l'a mentionné, le monde virtuel a évolué. Au début, on considérait qu'il ne s'agissait que de l'une des nombreuses menaces.

En fait, ce que nous avons déterminé, c'est... Parce que le budget était intégré au financement d'autres types de menaces, il n'était pas possible pour nous de déterminer combien était alloué expressément à la cybersécurité. De plus, nous voulions des plans généraux pour savoir quelles activités étaient appuyées et pouvoir ensuite comparer les progrès réalisés.

[*Français*]

M. Alain Giguère: Merci beaucoup.

On a observé que sur les 780 millions de dollars, 570 millions de dollars avaient été accordés au Centre de la sécurité des télécommunications Canada. Après avoir tant dépensé, en quoi le Canada est-il mieux protégé? J'aimerais aussi que vous nous soumettiez un rapport sur le détail des dépenses de ces 570 millions de dollars, s'il vous plaît.

[*Traduction*]

M. François Guimont: Si vous le permettez, monsieur le président, je vais laisser répondre ma collègue du CSTC.

Mme Toni Moffa: Merci.

Comme je l'ai dit tout à l'heure et comme l'a mentionné le vérificateur général, le total des 570 millions de dollars englobe les activités de programmes relatives à la cybersécurité qui ne portent pas nécessairement sur la cybersécurité.

Ce que nous avons investi dans nos activités à l'appui de la cybersécurité inclut notamment l'amélioration et le renforcement de la production de renseignements sur les cybermenaces étrangères, car cela fait partie de notre mandat en matière de renseignement étranger. De plus, nous avons amélioré notre capacité de détecter et d'analyser les menaces à l'égard des systèmes du gouvernement fédéral. Sur les réseaux gouvernementaux, en particulier ceux qui sont gérés par Services partagés Canada, qui regroupent les connexions Internet pour les systèmes du gouvernement, nous déployons des technologies capables de détecter les cybermenaces qui ne sont pas détectées par les technologies commerciales parce qu'elles sont fondées sur des renseignements classifiés sur les menaces. Cela ajoute un autre niveau de sécurité aux systèmes fédéraux .

Nous effectuons la détection et l'analyse de l'information que nous trouvons. Lorsque des menaces surviennent, nous pouvons en informer les ministères et leur offrir des conseils sur la façon de réduire les risques, ainsi que des conseils à long terme afin qu'ils renforcent leurs systèmes et évitent la répétition de ces problèmes.

Avec une partie du financement que nous recevons, nous gérons un centre de formation en sécurité des TI...

[*Français*]

M. Alain Giguère: Vous allez quand même nous faire parvenir le détail des dépenses de ces 570...

Mme Toni Moffa: Le détail des dépenses?

[*Traduction*]

En répondant à cette question, nous révélerions notre niveau de capacité dans ces domaines, ce que nous considérons comme de l'information classifiée. Il serait imprudent de le divulguer à ceux qui veulent nous faire du tort.

Je vais essayer de vous fournir un résumé des diverses activités, mais nous considérons que le niveau réel d'investissement dans ces domaines, en particulier en ce qui a trait à nos capacités technologiques, est une information classifiée pour des raisons de sécurité nationale.

Le président: Nous commençons à aborder des questions d'ordre constitutionnel, ici.

Monsieur Giguère, votre temps est écoulé, mais je vais vous donner l'occasion de faire un commentaire au sujet de l'information que vous demandez, afin que je sache où cela pourrait mener.

Voulez-vous poursuivre, monsieur, ou êtes-vous satisfait de la réponse obtenue? Si vous l'êtes, très bien. Nous allons poursuivre.

[*Français*]

M. Alain Giguère: Non, je ne peux pas me satisfaire d'une pareille réponse.

Le pays a investi considérablement dans le Centre de la sécurité des télécommunications Canada, soit 570 millions de dollars.

On nous dit qu'on a fait des travaux et que le Canada est mieux protégé qu'avant. Malheureusement, le rapport indique qu'on ne l'a pas...

● (1650)

[*Traduction*]

M. Andrew Saxton: J'invoque le Règlement, monsieur le président. Le temps de parole de mon collègue est expiré, mais vous le prolongez.

Le président: Non, je ne fais rien que je n'aie fait pour quelqu'un d'autre. Je lui donne une possibilité. Il va conclure très rapidement, et je vais continuer. Nous allons ensuite déterminer si nous avons un problème ou non.

Je ne crois pas en voir un actuellement, mais je vérifie si c'est le cas ou non.

Poursuivez et concluez rapidement, s'il vous plaît.

[*Français*]

M. Alain Giguère: Nous sommes le Comité permanent des comptes publics. Nous devons garantir que l'argent des contribuables est bien dépensé et qu'il est dépensé là où le gouvernement a dit qu'il devait l'être.

Nous avons accordé 570 millions de dollars à cette organisation, et on nous donne des généralités. Je demande des détails. Je veux savoir à quoi a été consacré cet argent.

Nous avons demandé que l'argent soit consacré à un système particulier. Je veux savoir si cela a été fait. C'est l'essence même de ce comité.

[*Traduction*]

Le président: Très bien.

Nous allons laisser cela de côté et y revenir si nécessaire.

Monsieur Hayes, vous avez la parole.

M. Bryan Hayes (Sault Ste. Marie, PCC): Merci, monsieur le président.

Ma question s'adresse à M. Guimont.

Jim Burpee, président-directeur général de l'Association canadienne de l'électricité, a déclaré: « Dans le cadre de la Stratégie nationale et du plan d'action sur les infrastructures essentielles, lancés par le gouvernement il y a deux ans, tous les intervenants travaillent de concert pour surmonter les défis que représente la cybersécurité au Canada. »

Je vais y arriver, mais revenons à ce plan d'action. Je ne comprends pas; il parle d'un plan d'action lancé il y a deux ans, alors que vous parlez d'un plan d'action publié le 18 avril.

Pouvez-vous m'éclairer à ce sujet? Combien y a-t-il de plans d'action? Pour quelle raison ces plans d'action ont-ils été publiés? À quelles dates l'ont-ils été?

M. François Guimont: Je vous remercie de la question. D'abord, il y a essentiellement la réponse de la gestion, comme je l'appellerais, aux recommandations du BVG, qui a été remise au comité, et qui porte très précisément sur les recommandations acceptées par le ministère. Voilà le premier point.

Deuxièmement, l'une de ces recommandations proposait d'élaborer un plan d'action global afin de pouvoir suivre les progrès ainsi que les résultats observés. Nous l'avons fait. Il nous a fallu des mois. C'était beaucoup de travail, et c'est normal. Ce n'est pas inhabituel. Il a été rendu public le 18 avril. Nous avons aussi élaboré un cadre de mesure en vue de suivre l'évolution des progrès; il est aussi disponible.

Les tables sectorielles ont toutes un type de plan d'action. Elles s'emploient à déterminer le risque, à gérer le risque et à échanger l'information. De plus, nous allons augmenter la fréquence des rencontres sur la cybersécurité, et ce, en prévision des mesures que nous conviendrons tous qu'il faut prendre afin de faire face à une cybermenace, par exemple. Elles sont toutes liées, en quelque sorte; je les décrirais comme « distinctes mais connexes ».

M. Bryan Hayes: Le plan dont parle le président de l'Association canadienne de l'électricité fonctionne très bien, selon lui. Dans d'autres réseaux sectoriels, il ne semble pas aussi bien fonctionner. J'aimerais que vous m'expliquiez pourquoi, en ce qui a trait à l'Association canadienne de l'électricité, le plan semble très bien se dérouler, alors que dans d'autres secteurs, cela ne semble pas être le cas.

Quel secteur, alors, est la prochaine priorité? J'ai l'impression qu'il est difficile de gérer tous les secteurs en même temps. Existe-t-il un plan de mise en oeuvre des priorités sectorielles, pour ainsi dire?

M. François Guimont: Si vous le permettez, je vais demander à Mme Clairmont de bien vouloir répondre.

Mme Lynda Clairmont: Je pense que vous parlez de la stratégie et du plan d'action sur les infrastructures essentielles qui ont été élaborés avec les provinces et les territoires. Chacun des réseaux sectoriels en fait partie, et je crois que dans le secteur de l'électricité, cela fonctionne très bien. D'autres secteurs ne sont peut-être pas nécessairement au même niveau, mais ils progressent.

M. Bryan Hayes: Donc, quelles sont les leçons apprises quant à la raison pour laquelle cela fonctionne si bien dans un secteur, mais pas très bien dans d'autres?

Mme Lynda Clairmont: Je pense que certains secteurs sont plus diversifiés. Certains secteurs étaient déjà plus structurés au départ. Certains secteurs sont plus cohérents. Ils ont des fonctions semblables. Par exemple, dans le secteur alimentaire ou les réseaux alimentaires, il y a un grand nombre d'éléments, alors que les banques et le réseau électrique sont plutôt centralisés.

● (1655)

M. Bryan Hayes: Monsieur Guimont, où nous situons-nous par rapport à nos deux plus proches partenaires du milieu de la sécurité et du renseignement? Le rapport indiquait qu'il s'agissait du Royaume-Uni et de l'Australie. Comment nos systèmes de cybersécurité se comparent-ils à ceux de ces deux pays?

M. François Guimont: Je vous remercie de me poser la question. Je vais d'abord parler de notre relation avec le Royaume-Uni, avec qui nous entretenons des liens très étroits. Nos économies sont liées de façon significative, si bien que nos relations sont nombreuses. Je me suis entretenu avec un certain nombre de personnes lors d'un séjour à Washington il y a de cela quelques mois. J'ai appris que la cybersécurité est un sujet prioritaire. Voilà pour la première observation que je voulais faire.

Deuxièmement, je n'ai pas fait le déplacement pour une simple rencontre. Nous nous sommes également engagés à prendre un certain nombre de mesures avec les États-Unis, ce que nous avons fait en bonne et due forme. Mme Clairmont en parlera dans un instant.

Troisièmement, nous ne traitons pas uniquement avec les États-Unis, le Royaume-Uni, la Nouvelle-Zélande, etc.; nous traitons aussi avec d'autres pays. Les principes sont toujours les mêmes: échanger des renseignements, établir des stratégies communes et prévoir les problèmes éventuels avant qu'ils ne se matérialisent. Mme Clairmont a récemment participé à une réunion sur le prétendu système Five Eyes. Elle pourra vous en parler également.

Mme Lynda Clairmont: Je vais vous dire une ou deux choses. Tout d'abord, nos stratégies en matière de cybersécurité s'alignent étroitement sur celles de nos plus proches alliés. Elles sont toutes très semblables. Elles ont toutes été annoncées à des moments différents, si bien que notre façon de les mettre en oeuvre est un peu différente.

En me préparant pour la réunion et en réfléchissant à comment nos stratégies s'alignent sur celles de nos alliés, j'y suis allée vraiment par thème. Il y a quelques thèmes qui reviennent dans nos pays aux vues similaires. L'échange de renseignements est un aspect essentiel dans toutes les stratégies et approches en matière de cybersécurité — communiquer les bons renseignements aux bonnes personnes et au bon moment. De plus, je pense que les partenariats public-privé sont vraiment importants également. Les engagements internationaux pour faire en sorte que nous transmettions des messages semblables à l'échelle internationale sont également importants. Enfin, il faut protéger nos citoyens au moyen de campagnes de sensibilisation et d'initiatives de lutte contre la criminalité et contre la fraude.

Pour ce qui est des États-Unis plus particulièrement, nous avons annoncé notre plan d'action de la sécurité intérieure du département de la Sécurité en 2012, qui comporte essentiellement trois buts. Premièrement, on cherchait à améliorer la gestion des incidents cybernétiques — leur US-CERT est l'équivalent de notre CCRIC — et à échanger davantage de ressources humaines et de renseignements en temps opportun. Deuxièmement, on visait à établir un engagement conjoint et échanger des renseignements avec le secteur privé, car un grand nombre des industries privées sont les mêmes d'un pays à l'autre. Troisièmement, nous voulions poursuivre notre collaboration relativement à nos campagnes de sensibilisation à la cybersécurité.

Le président: Bien, vous avez fait le tour de la question. Votre temps est écoulé. Merci beaucoup.

Nous allons maintenant revenir à M. Byrne. Vous avez la parole, monsieur.

L'hon. Gerry Byrne: Merci, monsieur le président.

L'une des préoccupations de notre comité et du Parlement, c'est d'obliger le gouvernement à rendre des comptes. L'un des problèmes que le vérificateur général a soulevés dans le rapport, c'est que l'on semble réticent à fournir les montants précis qui sont dépensés sur les menaces à la cybersécurité.

Le vérificateur général a souligné qu'environ 780 millions de dollars sont alloués pour diverses activités, mais les ministères semblent beaucoup hésiter à approfondir la question pour établir précisément quelle proportion de ces 780 millions a été consacrée à la cybersécurité. Seriez-vous prêt à fournir cette information au comité, monsieur Guimont?

M. François Guimont: Merci de la question.

Monsieur le président, je peux certainement fournir certains renseignements sur les 780 millions de dollars, à commencer par le fait que quatre présentations au Conseil du Trésor ont été approuvées. Cette somme était échelonnée sur 10 ans et était répartie parmi 13 ministères. Je conviens que ce n'est pas un sujet simple. On s'inquiète un peu concernant les ressources et où elles ont été consacrées.

Au cours de cette période de 10 ans, 21 millions de dollars ont été affectés à la cybersécurité. J'aimerais donc prendre quelques instants pour dire que la cybersécurité de nos jours n'est plus ce qu'elle était il y a 10 ans. Ces fonds étaient destinés à l'infrastructure essentielle, aux problèmes liés à tous les types de dangers, dont la cybersécurité. Mais la cybersécurité était différente il y a 10 ans. Nous devons tous nous rappeler que c'était après les attentats du 11 septembre et que nous étions dans ce monde, pour ainsi dire.

De ces 780 millions de dollars, 570 millions ont été approuvés dans le cadre du processus du Conseil du Trésor, des rapports sur les plans et les priorités, des rapports ministériels sur le rendement et de toutes les déclarations au CSTC. Comme l'a expliqué Mme Clairmont, les ressources ont été investies à l'échelle macroscopique.

Pour terminer, je dirai brièvement que 190 millions de dollars ont été alloués à différentes questions relatives à l'infrastructure, de façon générale, et non pas particulièrement à la cybersécurité.

C'est à l'échelle macroscopique, et j'ai des exemples de la façon dont les ressources ont été réparties.

Je veux enchaîner brièvement — et je ne m'éterniserai pas trop — sur la question très valable de savoir pourquoi 155 millions de dollars ont récemment été annoncés sur cinq ans alors qu'il est question de quatre ans dans le plan d'action. C'est pour la simple raison que lorsqu'une annonce est faite, les ressources ne sont pas automatiquement débloquées. Nous avons dû passer par un processus d'approbation qui a pris un certain temps, pour des raisons de diligence raisonnable, et nous disposons donc de quatre ans pour investir ces 155 millions de dollars. Je tenais à le signaler aux fins du compte rendu.

● (1700)

L'hon. Gerry Byrne: Merci beaucoup, monsieur Guimont. Je vous en suis reconnaissant.

Quoi qu'il en soit, le vérificateur général a toutefois constaté que 780 millions de dollars avaient été accordés. Il a relevé que 570 millions de dollars ont plus précisément été versés au Centre de la sécurité des télécommunications du Canada.

L'une des choses qui nous inquiètent toujours un petit peu, c'est le processus de double comptabilisation, où le gouvernement peut dire que 780 millions de dollars ont été dépensés pour la cybersécurité en cas de cybermenace et, en cas d'une menace d'insurrection d'individus qui se sont radicalisés au pays, on fait soudainement usage de ces 780 millions de dollars.

Il est utile d'éclaircir les choses, du point de vue de l'obligation du Parlement de rendre des comptes. Je ne demande pas d'apporter des précisions sur des projets particuliers, ce qui pourrait aller à l'encontre des exigences en matière de sécurité nationale, mais d'apporter des précisions sur quelles sont exactement les priorités pour la cybersécurité par rapport à d'autres choses.

Cela dit, je dois passer à un autre sujet car mon temps est précieux.

Nous sommes ravis, monsieur Guimont, qu'un document public très complet et beaucoup plus détaillé sur un plan d'action lié à la cybersécurité ait été fourni. Accepteriez-vous de remettre à la greffière ce document intitulé « Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada », une stratégie pangouvernementale, en tant que plan d'action gouvernemental lié au rapport du vérificateur général?

Accepteriez-vous d'appliquer le même contrôle parlementaire, ce qui oblige le gouvernement à rendre des comptes? Ce qui se trouve dans ce document et dans ces deux pages concorde en ce qui concerne l'obligation de rendre des comptes au comité et notre production de rapports.

Seriez-vous d'accord de présenter ce document en tant que plan d'action ministériel, pour la gouverne du comité, et de rendre des comptes concernant le document?

M. François Guimont: La réponse est oui.

Le président: Merci.

Il vous reste 17 secondes.

L'hon. Gerry Byrne: Je pense que je vais m'arrêter là.

Le président: Très bien. Merci. Nous apprécions votre discrétion.

Vous avez maintenant la parole, monsieur Dreeshen.

M. Earl Dreeshen (Red Deer, PCC): Merci beaucoup, monsieur le président.

Je vous remercie, monsieur Guimont. Je peux ajouter Pascal, COBOL et BLISS également. Si je ne tapais pas au clavier avec un seul doigt, je serais probablement rester dans ce domaine, mais on n'a désormais besoin que d'un pouce, si bien que je m'en tire pas mal.

Pour ce qui est du site Web, vous avez dit avoir eu 227 000 requêtes. Il est bien utilisé, et je pense que c'est important. Bien entendu, vous mentionniez également le fait que vous ne recevez aucun appel en dehors des heures normales.

Je sais que l'un des sujets dont nous avons parlé à l'automne quand nous avons discuté de la question pour la première fois, c'était l'idée de passer de 8 à 15 heures pour être ouverts malgré le décalage horaire de cinq heures et demie. Je pense que c'était important. Je peux comprendre pourquoi nous en avons parlé, et peut-être en raison des discussions que nous avons eues, vous avez insisté un petit peu pour qu'on s'assure de couvrir les neuf autres heures. Je respecte cela.

Quand j'examine le rapport et ce que le gouverneur général dit au sujet des 780 millions de dollars et comment les autres fonds ont été répartis, notamment les agents de la sécurité publique qui parlent des 20,9 millions des 210 millions de dollars restants, je respecte cette comptabilité. Je pense que ce sont les chiffres que le vérificateur général a examinés et sur lesquels il a tiré ses conclusions.

Il y a quelques points dont je tiens vraiment à discuter avec vous également. Pourriez-vous décrire les étapes que le Forum national intersectoriel a suivies pour ce qui est des activités de gestion du risque et comment elles sont conjointement menées à l'échelle du Canada? J'aimerais entendre vos observations sur ce que nous avons constaté.

Monsieur le vérificateur général, qu'avez-vous observé à la lumière de ce Forum national intersectoriel? D'après vous, a-t-il donné les résultats escomptés en matière de gestion du risque?

● (1705)

M. Michael Ferguson: Je demanderais à Mme Loschiuk de répondre à cette question.

Mme Wendy Loschiuk (vérificatrice générale adjointe, Bureau du vérificateur général du Canada): Merci beaucoup.

Nous considérions le Forum national intersectoriel comme étant une activité qui avait débuté en 2010. Nous le percevions comme une façon d'améliorer les communications. Nous voulions donc en parler très brièvement. Il en est question au paragraphe 338 du chapitre, dans lequel on fait état des bons progrès réalisés. Nous considérions ce forum comme une initiative visant à rassembler des groupes qui n'avaient pas encore eu l'occasion de pleinement se concerter en tant que réseaux.

De ce point de vue, nous le percevions comme une mesure active qui prenait la place des réseaux qui n'étaient pas encore complètement établis.

M. Earl Dreeshen: Merci.

Madame Charette, dans votre déclaration liminaire, vous avez décrit comment le SCT a mis un accent renouvelé sur une sensibilisation accrue et des pratiques exemplaires en matière de sécurité de la TI à l'échelle du gouvernement. Je me demande si vous pourriez passer en revue certaines de ces pratiques exemplaires.

Mme Corinne Charette: Merci beaucoup.

C'est une excellente question. En fait, nous avons pris un certain nombre de mesures. En premier lieu, nous avons longuement interrogé nos agents de sécurité du ministère pour connaître quels étaient, d'après eux, les besoins dans les collectivités pour accroître la sensibilisation du public à la sécurité. Avec leur aide, nous avons essentiellement élaboré un cadre de formation en matière de sécurité du gouvernement du Canada et mis sur pied un groupe de travail sur la formation des spécialistes de la sécurité. Nous reconnaissons que sensibiliser tous les fonctionnaires à la cybersécurité est également un élément important de l'initiative. On est en train d'élaborer le matériel de formation au moyen du cadre.

Au cours du mois sur la cybersécurité, qui a lieu en octobre, nous essayons de bien faire comprendre l'importance de la cybersécurité à tous les fonctionnaires. Nous travaillons également beaucoup sur la sensibilisation à une bonne conduite sur le Net au sein du ministère, par exemple, en n'ouvrant pas toutes les pièces jointes aux courriels, car même avec les meilleurs filtres de pourriels ou les filtres en général, il existe des moyens très habiles de duper les gens pour accéder à leurs courriels, qui sont en fait des logiciels malveillants.

Nous avons également presque terminé de rédiger un avis relatif à la politique en matière de TI à l'intention des ministères sur ce qu'ils doivent faire pour assurer la sécurité des médias portatifs et sensibiliser les gens au fait que les médias portatifs constituent un moyen d'introduire des menaces, si on les télécharge dans les systèmes du gouvernement. Nous travaillons donc sur plusieurs fronts pour sensibiliser les fonctionnaires à tous les niveaux, les employés, le personnel de la TI, les agents de sécurité du ministère, ainsi que tous les cadres, pour faire en sorte qu'ils comprennent tous leur rôle pour ce qui est de maintenir un niveau de sécurité satisfaisant.

Le président: Désolé, monsieur Dreeshen, mais votre temps de parole est écoulé. Merci.

Il nous reste du temps pour entendre deux autres intervenants. Le prochain sera M. Allen. Je crois savoir que vous allez partager votre temps de parole avec Mme Blanchette-Lamothe, et c'est très bien. Vous avez la parole.

M. Malcolm Allen: Merci, monsieur le président.

Ma question s'adresse à M. Ferguson, à la page 10 de la version anglaise de votre rapport, au paragraphe 3.20, vous dites que des fonds de l'ordre de 780 millions de dollars ont été approuvés. Vous avez indiqué ne pas avoir été en mesure d'établir où ces fonds ont été alloués précisément. Au bas du paragraphe, vous dites avoir relevé 200 millions de dollars supplémentaires.

Ces sommes sont-elles cumulatives, monsieur, c'est-à-dire qu'on additionne les 200 millions aux 780 millions de dollars? Est-ce ce que vous dites dans ce paragraphe?

M. Michael Ferguson: C'est exact.

M. Malcolm Allen: Nous approchons la marque du 1 milliard de dollars. Nous sommes rendus à 980 millions de dollars, pour être exact. Ma question aux ministères est donc la suivante: compte tenu du fait que nous n'avons pas été en mesure de dire au vérificateur général comment nous avons dépensé les fonds sur les questions liées à la cybersécurité, le ministère peut-il retracer où le financement a été affecté?

De plus, par l'entremise de la présidence, j'aimerais que cela devienne un poste budgétaire pour déterminer comment ces fonds ont été répartis parmi les 13 ministères, car il est maintenant question de 1 milliard de dollars. J'aimerais en fait savoir à quoi l'argent a servi, y compris pour des choses qui n'étaient pas directement en lien avec la cybersécurité. J'aimerais savoir comment cet argent a été dépensé exactement. Je vais vous laisser le soin, monsieur le président, de prendre une décision et de donner instruction aux témoins en conséquence.

Je vais maintenant céder le reste de mon temps de parole à Mme Blanchette-Lamothe.

● (1710)

Le président: Madame.

[*Français*]

Mme Lysane Blanchette-Lamothe: Merci.

J'ai une question concernant l'intrusion de janvier 2011 mentionnée dans le rapport du vérificateur général.

Cette intrusion, qui a été assez importante, visait à obtenir de l'information, à prendre le contrôle et à extraire de l'information de nature délicate. On sait que cela a coûté cher de réagir à cette attaque et que cela a pris du temps à s'en remettre complètement.

Que pensez-vous d'un mécanisme obligatoire de délivrance d'un avis en cas de perte de données ou d'un accès non autorisé aux données? Cela permettrait peut-être de mieux protéger les renseignements personnels des Canadiens en cas de cyberattaque.

Si ce n'est pas une option que vous envisagez, que prévoyez-vous faire pour protéger les renseignements personnels des Canadiens?

[*Traduction*]

Le président: Qui veut répondre à cette question? Avez-vous une préférence?

Quelqu'un veut-il y répondre? Que quelqu'un prenne la parole, s'il vous plaît?

M. Robert Gordon: Monsieur le président, je serais ravi de répondre à cette question...

[*Français*]

M. François Guimont: Monsieur le président...

Le président: Monsieur Guimont, vous avez la parole

M. François Guimont: Monsieur le président, permettez-moi de répondre à cette question qui, selon ce que j'en comprends, touche la protection de l'information personnelle, d'une certaine façon, comme le troisième pilier de la stratégie le mentionne.

Je pense singulièrement aux Canadiens. Les gens ont la responsabilité de protéger leur propre information. C'est la première chose.

Par ailleurs, en ce qui a trait aux systèmes gouvernementaux où travaille mon collègue M. Long, j'aimerais simplement noter que nous avons un nombre très élevé de systèmes de courriels et que nous nous dirigeons vers un seul système.

Nous avons aussi plus de 200 centres de données. Certains sont un peu plus vieux, d'autres un peu plus jeunes; c'est un mélange. Nous nous dirigeons vers environ 20 centres de données.

Tout cela sous-entend que nous essayons de fermer des fenêtres qui pourraient être risquées et susceptibles de faire l'objet de cyberattaques. Bien sûr, si cette information touche de l'information personnelle, nous diminuons ainsi les risques que de l'information personnelle canadienne soit rendue publique.

Ce sont les deux exemples que je donnerais relativement à ce que nous faisons.

Mme Lysane Blanchette-Lamothe: J'ai une dernière question pour vous.

Un peu plus tôt, mon collègue a demandé si notre cyberespace était sécuritaire et vous avez répondu que c'était pas mal le cas. Or, on sait que le rapport du vérificateur général émet des doutes quant à notre capacité d'intervenir et de prévenir les cyberattaques.

Que pourrait-on ajouter au plan d'action que vous avez mis en place et à toutes vos ressources, pour maximiser notre efficacité à contrer les cyberattaques et notre capacité à y répondre?

M. François Guimont: Je me suis joint au ministère en novembre, et depuis, la question du cyberespace a représenté une priorité pour moi. Ce n'était pas tant ma décision, mais de par la nature de l'enjeu, on parle beaucoup de cette question au sein du ministère. C'est ma première observation.

Par ailleurs, je parle aussi pour mes collègues du gouvernement fédéral et du secteur privé. J'ai eu des discussions avec M. John Manley, du Conseil canadien des chefs d'entreprise. Je veux aussi avoir des rencontres avec un groupe de personnes qui pourraient nous aider à mieux comprendre la dynamique au sein du secteur privé.

Je vous dirais qu'il y a une prise de conscience, et c'est par là qu'il faut commencer. Je ne veux pas dire qu'elle était absente avant, mais on se rend compte qu'avec l'évolution des cybermenaces, on doit travailler de concert encore plus qu'avant. Ce n'est pas une formule magique, mais s'il y avait un élément à mettre sur la table qui pourrait être déterminant par rapport à la protection, je dirais qu'il faudrait ultimement une meilleure coopération, un bon échange d'information, des plans d'action et faire le suivi des actions que nous entreprenons. Je sais qu'il y en a plusieurs, je le reconnais maintenant. Je pense que c'est la recette pour mieux prévenir les menaces.

Mme Lysane Blanchette-Lamothe: En ce qui a trait au suivi...

[*Traduction*]

Le président: Désolé, madame, mais votre temps est écoulé.

Monsieur Saxton, la parole est à vous.

● (1715)

M. Andrew Saxton: Merci, monsieur le président.

Je vais partager mon temps de parole avec mon collègue, M. Dreeshen. Je propose qu'il commence, puis je conclurai.

Le président: C'est une drôle de façon de s'y prendre, mais cela nous convient.

On vous écoute, Earl.

M. Earl Dreeshen: Merci beaucoup.

Si on procède ainsi, c'est parce que j'ai décidé d'intervenir un peu à la dernière minute.

En ce qui concerne le rapport du vérificateur général, si nous pouvions revenir au paragraphe 3.21, j'aimerais obtenir des précisions à cause de la question que M. Allen a soulevée tout à l'heure. Voici ce que dit la première phrase: « Par ailleurs, des 780 millions de dollars octroyés, nous avons noté que le gouvernement avait approuvé l'attribution d'environ 570 millions de dollars au Centre de la sécurité des télécommunications Canada ». Ensuite, si on va à la fin du même paragraphe, on peut lire ceci: « Les représentants de Sécurité publique Canada ont toutefois indiqué qu'environ 20,9 millions des 210 millions de dollars qui restaient avaient servi à protéger l'infrastructure essentielle contre les cybermenaces [...]. »

J'en déduis donc que les 780 millions de dollars sont composés des 570 millions de dollars plus les 210 millions de dollars, n'est-ce pas? J'ai entendu M. Allen dire que le montant s'élevait à presque un milliard de dollars, mais ce n'est pas vraiment le cas, n'est-ce pas?

Je me suis appuyé sur ce que j'ai lu dans le rapport.

M. Michael Ferguson: On peut demander à Mme Loschiuk de répondre à la question.

Mme Wendy Loschiuk: Lorsque nous avons repéré les crédits affectés, nous avons essayé d'en suivre la trace pour voir à quelles fins ils avaient servi. Nous n'avons pas pu faire une ventilation plus détaillée que ce qui est présenté dans le rapport. Nous avons réussi à établir, comme vous l'avez expliqué, qu'un montant de 570 millions de dollars avait été accordé à une organisation, mais nous voulions aussi savoir à quoi avaient servi les 210 millions de dollars qui restaient; ce montant avait été accordé à d'autres organisations.

Cependant, dans le cadre de notre examen, nous avons également pu déterminer qu'un financement continu avait été octroyé au cours de nombreuses années et qu'il s'agissait des 200 millions de dollars qui restaient, mais nous n'avons pas beaucoup de détails sur cet aspect. Il s'agit uniquement d'un financement continu accordé aux ministères.

M. Earl Dreeshen: Merci. Je voulais simplement avoir une précision à ce sujet. Je ne voyais pas où se trouvait l'autre montant de 200 millions de dollars dans le rapport. Je m'appuyais uniquement sur les 570 millions de dollars plus les 210 millions de dollars.

Sur ce, je cède la parole de nouveau à M. Saxton.

Le président: Très bien.

Monsieur Saxton.

M. Andrew Saxton: Merci, monsieur le président.

Tout d'abord, je tiens à remercier le ministère de la Sécurité publique d'avoir fourni le plan d'action que notre comité avait demandé en présentant une motion en réponse aux recommandations du vérificateur général. Je remercie également le plan d'action qui a été publié le 18 avril. Les deux étaient très utiles.

J'aimerais maintenant demander au sous-ministre de bien vouloir faire le point sur les trois piliers, c'est-à-dire: protéger les systèmes gouvernementaux, nouer des partenariats pour protéger les cyber-systèmes essentiels à l'extérieur du gouvernement fédéral et aider les Canadiens à se protéger en ligne.

M. François Guimont: Merci, monsieur le président.

J'espère, madame Clairmont, que votre voix vous permettra de nous faire un bilan de la situation. Je vous en serais reconnaissant.

Mme Lynda Clairmont: D'accord; si vous avez du mal à comprendre, je demanderai à Bob de prendre la relève.

Essentiellement, dans le cadre du plan d'action, nous avons examiné les diverses activités qui étaient en cours et la façon dont nous pourrions les encadrer. En ce qui concerne les systèmes gouvernementaux, nous travaillons beaucoup à améliorer le CCRIC, le CSTC et les systèmes du Conseil du Trésor, ainsi que les services partagés. Je crois que nous avons une très bonne approche pour protéger les systèmes gouvernementaux.

Nous menons également un certain nombre d'autres activités, comme Corinne et Benoît l'ont expliqué. Le deuxième pilier, les partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral, met l'accent sur les secteurs des infrastructures essentielles pour les perfectionner davantage, tendre la main au secteur privé, faire participer les secteurs de façon bilatérale et améliorer ces relations. Dans ce domaine, j'inclurais les relations et les activités de sensibilisation que nous menons auprès de pays aux vues similaires — les États-Unis, le Royaume-Uni, l'Australie et certains pays de l'Europe.

Le dernier élément consiste à s'assurer que les Canadiens ont des occasions de s'informer sur les cybermenaces et qu'ils disposent des outils nécessaires pour se protéger. J'encourage tout le monde à consulter les sites Web « Pensez cybersécurité » et « Stop. Think. Connect. », parce qu'on y trouve de bons conseils. Parfois, on ne prend pas le temps de les mettre en pratique.

Voilà, en gros, de quoi il s'agit.

M. Andrew Saxton: Merci beaucoup.

Le président: Cela met fin à la série d'interventions. Avant de lever la séance, toutefois, nous devrons nous occuper de quelques demandes de renseignements.

Auparavant, j'aimerais attirer votre attention sur l'observation faite par le vérificateur général au neuvième paragraphe de son rapport, où il conclut en disant que les fonctionnaires craignent que l'environnement des cybermenaces évolue plus rapidement que la capacité du gouvernement de suivre le rythme des changements. Si c'est vrai, il est inévitable que, tôt ou tard, nous perdions la course et que nous ayons de graves problèmes.

Monsieur Guimont, qu'en pensez-vous?

● (1720)

M. François Guimont: J'ai mentionné que le rapport du BVG avait été bien accueilli. C'est un bon examen. On y trouve de bonnes recommandations, et le plan d'action à long terme que nous avons produit est conçu pour nous aider à rectifier le tir. Cependant, je serai très direct dans mes propos. Il s'agit d'une tendance en évolution. La situation change tout le temps, et nous devons suivre le rythme des changements. C'est un effort collectif. Ce n'est pas l'apanage du gouvernement fédéral. Tout le monde doit être de la partie. Nous allons consacrer beaucoup d'énergie pour consulter les gens et nous assurer que tout le monde est sur la même longueur d'onde.

Le président: Merci. Je vous en suis reconnaissant.

Chers collègues, certains d'entre vous ont demandé des renseignements. La question qui se pose ici, c'est comment nous allons nous y prendre. Nous avons créé un comité officieux pour s'en occuper, mais il n'y a pas encore eu de réunions. J'ai noté six éléments au sujet desquels nous avons besoin d'obtenir des explications. J'aimerais avoir la pleine collaboration des membres. N'oubliez pas que nous n'avons pas encore établi de règles à cet égard.

Nous allons essayer d'examiner un point à la fois, à l'improviste, pour voir si nous pouvons arriver à une entente. Dans le cas contraire, mettons en place un processus rapide. Ainsi, nous aurons traité ces demandes, à tout le moins, de façon improvisée. Je vais commencer par les éléments qui me paraissent les plus faciles — mais on ne sait jamais —, puis je passerai aux plus difficiles.

Au début de la séance, M. Allen a demandé à recevoir un organigramme, et je crois que le sous-ministre a fait un signe de la tête pour indiquer qu'il pouvait nous en fournir un. Quand cela sera-t-il possible, monsieur Guimont?

M. François Guimont: Si vous n'y voyez pas d'objection, monsieur le président, normalement, on nous donne un délai de deux semaines. Si cela convient aux membres du comité, nous vous fournirons ces renseignements à l'intérieur de ce délai.

Le président: Cela vous convient-il, chers collègues? Deux semaines? Est-ce acceptable?

Des voix: Oui.

Le président: D'accord. C'est bien. Parfait, merci. C'était le premier point.

Deuxièmement, Mme Blanchette-Lamothe a demandé un compte rendu des progrès accomplis. C'était un peu rapide, mais j'en ai pris note, et je pense que, là encore, le sous-ministre a opiné du bonnet. J'en ai déduit que c'était un oui, mais je n'ai pas entendu de précisions à ce sujet.

Pouvez-vous me donner une idée de la façon dont vous allez respecter l'engagement de nous fournir cette information?

M. François Guimont: À titre de précision, monsieur le président, s'agit-il exclusivement des progrès réalisés aux tables sectorielles?

Le président: Permettez-moi de vérifier auprès de la députée qui a posé la question.

Madame?

[*Français*]

Mme Lysane Blanchette-Lamothe: Merci.

Compte tenu de tous les plans d'action fort intéressants présentés aujourd'hui, ce serait intéressant d'avoir un suivi des progrès réalisés par ces plans d'action en général.

Comme je n'avais que cinq minutes, j'ai posé des questions sur un aspect particulier d'un plan d'action. Toutefois, ma préférence serait de connaître l'évolution des progrès par rapport aux plans d'action en général, si possible.

[*Traduction*]

Le président: Nous en tenons compte, je crois. C'est déjà ce que nous faisons, n'est-ce pas?

D'habitude, cette information se trouve dans le rapport du comité, après quoi on l'intègre dans notre programme, pour ensuite en faire le suivi. Alors, ces données devraient être saisies dans le cadre du rapport préliminaire. Si ce n'est pas le cas, vous pouvez en faire mention ou demander à votre personnel de nous signifier votre intention de soulever la question au moment de la rédaction de l'ébauche.

Alex est ici, et j'ai l'impression qu'il est d'avis que le rapport contiendra déjà cette information parce qu'il s'agit d'une pratique courante. Nous recevons les plans d'action, mais l'autre moitié de notre travail consiste à remplir notre obligation de faire un suivi et de nous assurer que les recommandations sont concrétisées, à défaut de quoi nous devons convoquer les responsables et leur demander des justifications.

Cela vous convient-il, madame?

[*Français*]

Mme Lysane Blanchette-Lamothe: Oui.

[*Traduction*]

Le président: Merci. On a donc réglé les deux premiers points.

Quant au troisième, j'y reviendrai tout à l'heure.

Quatrièmement, M. Byrne a posé une question à M. Guimont concernant le montant de 780 millions de dollars et celui de 570 millions de dollars. Cherchiez-vous à savoir, monsieur Byrne, comment le montant total des 780 millions de dollars a été réparti? Je vais vous céder la parole pour vous permettre d'apporter cette précision.

L'hon. Gerry Byrne: Merci, monsieur le président.

J'ai posé à M. Guimont une question pour obtenir une réponse au nom du gouvernement. Le vérificateur général a déterminé qu'un financement maximal de 780 millions de dollars avait pu être accordé à 13 ministères et organismes pour des activités de sécurité liées aux infrastructures essentielles et aux systèmes gouvernementaux. En lisant le rapport du vérificateur général, nous avons constaté qu'il y avait eu une tentative ou une volonté d'établir, le cas échéant, quelle part des 780 millions de dollars aurait pu être attribuée exclusivement à la cybersécurité.

Je n'ai pas demandé à obtenir une liste des projets ou des dépenses, mais ce serait très utile si chacun des 13 ministères ayant reçu une partie des 780 millions de dollars pouvait rendre compte au Parlement, par notre intermédiaire, du montant accordé exclusivement aux activités de cybersécurité et aux achats d'immobilisations. J'ajouterais à ce montant les 200 millions de dollars qui ont été établis par la suite.

Monsieur le président, il est clair qu'un financement de 570 millions de dollars a été accordé au Centre de la sécurité des télécommunications Canada. Bien entendu, une partie de ce montant servirait à l'écoute électronique et une autre, à la cybersécurité. On n'utiliserait pas tout l'argent à l'une ou l'autre de ces activités. Au moment de nous fournir ces données, j'aimerais que les 13 ministères nous indiquent très clairement quel montant a été consacré à la cybersécurité. S'il s'avère qu'une partie de l'argent pourrait avoir servi tant à la cybersécurité qu'à l'écoute électronique, par exemple, les ministères devraient préciser le pourcentage ou les proportions, pour que nous puissions déterminer le montant établi par le gouvernement du Canada pour les dépenses liées à la cybersécurité.

Est-ce clair, monsieur le président?

● (1725)

Le président: Je vais diviser votre demande en deux parties. D'abord, je vais demander au sous-ministre de nous indiquer si cela lui semble clair: a-t-il compris ce qu'on lui demande? Et deuxièmement, quelle est sa réponse à la demande proprement dite?

Il y a donc deux volets: comprenez-vous la question et, dans l'affirmative, êtes-vous en mesure de fournir l'information, monsieur le sous-ministre?

M. François Guimont: Je comprends la question. La partie difficile, c'est que les ressources ont été réparties sur 10 ans.

Le président: Excusez-moi. Pardon?

L'hon. Gerry Byrne: Je suis désolé, monsieur le président. C'était moi.

Nous pourrions également demander au vérificateur général, monsieur le président, si cela répond à...

Le président: Eh bien, commençons par le sous-ministre et voyons où en sont les choses.

Désolé de vous avoir interrompu. Allez-y, s'il vous plaît.

M. François Guimont: C'est correct, monsieur le président. Pardonnez-moi de vous avoir interrompu de la sorte.

Je disais que la difficulté, c'est que le financement s'étend sur une période de 10 ans; il s'agit d'un investissement de 10 ans. J'ai bien précisé qu'on avait approuvé quatre présentations au Conseil du Trésor; c'est donc dire que les ministres ont établi des exigences, lesquelles ont été approuvées, d'où les investissements... qui ont fort probablement été déclarés. Il s'agit de reconstruire le passé. Voilà, en partie, le défi qui nous attend, pour ainsi dire. Ces ressources étaient là. Des investissements ont été consentis. Évidemment, il y a des exemples qui montrent à quelles fins les investissements ont servi, mais de là à déterminer précisément ce qui s'est passé sur une période de 10 ans, au sein de 13 ministères — voilà le défi, selon moi.

Alors, la question est claire. Le problème concerne davantage ce que je viens de décrire.

Le président: D'accord, je crois que c'est raisonnable.

Monsieur Ferguson, avez-vous quelque chose à dire à ce sujet?

M. Michael Ferguson: Merci, monsieur le président.

Je n'ai pas vraiment d'observations à ajouter, outre le fait que, bien entendu, au moment de préparer le chapitre, nous avons eu du mal, nous aussi, à obtenir tous ces renseignements, parce que nous avons reconnu que les fonds n'étaient pas destinés uniquement à la cybersécurité, mais plutôt à des activités générales. Par contre, nous pouvons certainement nous assurer d'examiner en détail les renseignements dont nous disposons déjà dans nos dossiers, c'est-à-dire ceux que nous avons reçus de la part des ministères, et leur signaler les données que nous avons déjà afin qu'ils puissent nous fournir des renseignements supplémentaires, le cas échéant.

Le président: Permettez-moi de proposer une idée, avant de vous céder la parole.

Pouvez-vous essayer l'approche suivante, monsieur le sous-ministre? Au moment de faire une demande de renseignements, nous devons examiner plusieurs points — et je ne veux pas brûler les étapes, car le comité n'en est pas encore rendu là. En tout cas, un des points dont nous tenons compte, c'est le caractère raisonnable des demandes; après tout, il faut bien demander des renseignements pour accomplir notre travail et vous obliger — vous et le reste du gouvernement — à rendre des comptes. Cependant, nous ne pouvons pas lancer une question qui entraîne des dépenses d'un million de dollars, sans être en mesure de justifier si cet argent a été dépensé de façon judicieuse.

J'ai l'impression, en vous écoutant, que nous nous embarquons dans cette voie. En l'absence de règles précises quant à la façon de nous y prendre — et je demande à mes collègues de bien écouter ce que je vous propose —, pourriez-vous d'abord essayer d'obtenir l'aide du vérificateur général, qui vient de nous faire part de son intention de fournir certains renseignements qui risquent d'être utiles? Donnez-nous ce que vous pouvez et autant que vous le pouvez, aussi vite que possible. Ensuite, nous aurons à déterminer si nous jugeons que l'information reçue est complète et acceptable.

Est-ce que cela peut fonctionner? Est-ce qu'on peut essayer cette approche, monsieur le sous-ministre?

● (1730)

M. François Guimont: Je m'engage à en discuter avec le BVG, comme vous le proposez, mais cela risque de prendre du temps, monsieur le président.

Je ne suis pas au courant des renseignements dont dispose le BVG. Ma seule mise en garde, et j'espère que le comité comprendra cela, c'est que ces renseignements risquent de comporter des données de nature délicate relativement aux cybermenaces. Je serais donc reconnaissant si le comité faisait preuve de compréhension à cet égard.

Comme Mme Moffa l'a mentionné, certaines données pourraient être de nature très délicate. Cela dit, je m'engage à en discuter.

Le président: D'accord. Je vous saurais gré de mettre cet avertissement de côté en attendant, car cela ne met pas fin à la discussion. Vous savez fort bien de quoi je parle lorsque je dis que nous tombons dans les questions constitutionnelles concernant le droit inconditionnel du Parlement de demander de l'information. Il y a des procédures pour traiter ces questions — qu'arrive-t-il si cela est considéré comme une question de sécurité? — et le règlement prévoit ensuite des négociations. Au bout du compte, vous savez, monsieur, que vous ne pouvez pas simplement dire aux membres du comité qu'ils ne peuvent pas l'avoir. Ce n'est pas du tout la fin de l'histoire.

Mais nous ne voulons pas nous aventurer dans ces eaux infestées de requins. Il serait préférable que nous trouvions un terrain d'entente.

Alors, monsieur Byrne, et membres du comité, je vous demanderais d'être raisonnables, je pense que c'est juste. Le vérificateur général a reconnu que cela demandait beaucoup de recherche, et même lui n'a pas reçu l'information lorsqu'il l'a demandée, et j'ai l'impression — je ne lui fais pas dire ce qu'il n'a pas dit — qu'il est d'accord avec cet argument.

Pouvons-nous convenir de demander au sous-ministre de nous fournir un rapport sur les questions dont nous avons parlé? Ensuite, quand nous l'aurons en mains, nous pourrons l'examiner et voir s'il convient ou pas.

Allez-y, monsieur Saxton.

M. Andrew Saxton: Monsieur le président, nous avons organisé un sous-comité dans le but précis de traiter ces questions. Je pense que nous devons nous réunir très bientôt. Je crois que nous devrions en parler au sein de ce comité, comme vous l'avez recommandé. Alors parlons-en pendant la réunion du sous-comité.

Je remarque que la sonnerie se fait entendre depuis maintenant plusieurs minutes. Comme nous le faisons normalement quand cela se produit, je propose d'ajourner la réunion et de remercier nos témoins.

Le président: Vous savez que vous ne pouvez pas proposer de motion sur un rappel au Règlement, mais je prends bonne note de votre argument.

Est-ce qu'il s'agit d'une sonnerie de 30 minutes, madame la greffière?

Il s'agit d'une sonnerie de 30 minutes, alors il nous reste un peu de temps.

Je comprends ce que vous dites. Si la majorité finit par dire que nous arrêterons de discuter avec les témoins et nous renverrons la question à un groupe qui ne se réunit pas. J'avais espoir que nous puissions nous entendre sur quelques points de base. Comme je l'ai dit, s'il y a un domaine sur lequel nous ne pouvons pas nous mettre d'accord, si nous pouvons lancer un processus...

Sinon, j'ignore comment nous arriverons à rassembler toutes ces personnes et à pouvoir le faire dès que possible. Nous sommes plus qu'à la mi-chemin. Si vous pouviez me donner un peu de marge, comme nous sommes d'accord jusqu'ici...

M. Andrew Saxton: Nous pourrions toujours écrire une lettre aussi...

Le président: Oui, mais laissez-moi terminer.

M. Andrew Saxton: ... pour faire un suivi. Nous n'avons pas à rassembler les témoins.

Le président: Attendons de voir si nous pouvons continuer à obtenir leur coopération, et nous pourrons mener les travaux à bien. C'est la raison pour laquelle nous sommes ici, alors si je puis me permettre, essayons de le faire.

Quand le recevrions-nous, monsieur?

M. Daryl Kramp: J'invoque le Règlement, monsieur le président.

Le président: Oui.

M. Daryl Kramp: Monsieur le président, je ne suis pas d'accord avec cela.

M. Bryan Hayes: Moi non plus.

Le président: D'accord.

M. Bryan Hayes: Il est 17 h 30 passées. En ce qui me concerne, le comité...

M. Daryl Kramp: Il y a une façon de le faire et ce n'est pas la bonne.

Le président: Quelle est la bonne façon de procéder?

M. Daryl Kramp: La bonne façon de procéder est de faire preuve de bon sens. Nous avons une divergence d'opinions. Moi aussi je veux obtenir autant d'information que possible. Mais comme vous l'avez dit, monsieur le président, il y a une différence entre « raisonnable » et...

Si nous avons affaire à une preuve accablante, c'est une chose. Nous allons créer une lourde responsabilité si nous allons dans ce sens. Ce sera toute une tâche de présenter l'information. Cette information se rapporte-t-elle à la déclaration du vérificateur général, à l'enquête actuelle, à ce problème en suspens? Je pense que nous avons besoin d'avoir cette discussion sur ce point en particulier.

Je suis disposé à étudier certaines questions sur lesquelles nous sommes tous d'accord. Faisons-le.

Le président: D'accord, mais nous sommes près du but.

M. Daryl Kramp: Mais avec une divergence d'opinions...

Le président: Mais nous n'avons pas de divergence d'opinions. Je comprends ce que vous dites.

M. Gerry Byrne: Monsieur le président, baissez le ton.

Le président: En êtes-vous capable?

M. Gerry Byrne: Oui.

Le président: D'accord, si vous pouvez baisser le ton, j'écoute.

L'hon. Gerry Byrne: Monsieur le président, je crois que nous devrions tous reconnaître que M. Guimont est un fonctionnaire fiable qui a su gagner notre confiance. S'il peut le faire, il le fera.

Mais j'aimerais transmettre un message non pas à M. Guimont, mais au gouvernement. S'il fallait qu'une cybermenace se produise, que le gouvernement affirme que nous consacrons *x* montant d'argent à la cybersécurité, alors qu'il sait que ce n'est pas vrai, parce qu'il est incapable de dire à un comité parlementaire combien il consacre à la cybersécurité. Je ne voudrais pas me retrouver à la place du gouvernement, si tel était le cas.

Alors faisons confiance au fonctionnaire pour nous transmettre l'information. S'il peut le faire rapidement, génial. S'il ne peut pas, car c'est simplement une tâche... le vérificateur général a dit qu'il a des dossiers susceptibles de l'aider. Si à un moment donné, le ministère est incapable de fournir cette information, nous pouvons demander au vérificateur général quelle information il leur a transmise. Mais pour l'instant, on a fait une demande. Voyons si nous pouvons fournir...

● (1735)

Le président: L'idée était de donner à M. Guimont l'occasion de nous fournir ce qui est raisonnable, alors je ne crois pas que quiconque soit en désaccord. M. Guimont va essayer de le faire et de nous donner ce qu'il peut. Lorsque nous recevrons l'information, nous verrons où nous en sommes. C'est une chose de faite.

Ensuite, il y avait une autre demande, encore une fois de M. Byrne, concernant un plan d'action ministériel plus vaste, mais je pense que nous l'avons déjà faite. Vous avez demandé qu'il soit déposé. Je pense que nous pouvons considérer que c'est pas mal fait maintenant, n'est-ce pas? Le voilà.

Oui, c'était facile. Considérez que c'est réglé.

M. Daryl Kramp: Monsieur le président, je ne considère pas que l'autre question soit réglée. Vous avez dit que ce l'était. Je crois le contraire.

Le président: Celle que je viens tout juste de mentionner?

M. Daryl Kramp: C'est exact. Celle dont nous parlions à l'instant.

Le président: C'est le rapport que M. Byrne avait et qui est juste ici, et c'était simplement...

M. Daryl Kramp: Non, non, la demande.

Le président: Oui.

M. Daryl Kramp: La demande. Vous avez dit qu'elle était réglée dans la mesure...

Le président: Pour la question précédente?

M. Daryl Kramp: Oui.

Le président: Je croyais que nous en avions convenu.

M. Daryl Kramp: Non, c'est ce que je veux dire, nous ne sommes pas d'accord.

Le président: Nous avons demandé à M. Guimont ce qu'il pouvait nous fournir...

M. Daryl Kramp: Non, monsieur le président...

Le président: Simplement ce qui est facile à fournir. Peut-il le faire? Ensuite nous allons y jeter un coup d'oeil et voir où nous en sommes. Voilà pourquoi j'ai demandé où était le désaccord. Il me l'a offert, et j'ai accepté son offre.

Nous pourrions faire fausse route si nous l'obtenons et décidons... et nous nous lançons dans une grande discussion sur la question de savoir si c'est assez ou pas. Mais le moment n'est pas venu de se livrer bataille, nous pourrions le faire un autre jour. En ce moment, nous nous sommes tous mis d'accord pour que le sous-ministre nous envoie ce qu'il peut. Cela me semble être relativement facile.

Ensuite, nous sommes passés à l'autre point, et il m'en reste un, et ensuite nous passerons au suivant. On a demandé où est passé le milliard de dollars. J'ai noté la question. Je ne vois personne se précipiter pour en parler, alors je vais la laisser tomber. Pour la dernière, je veux qu'on fasse la même chose qu'avec le sous-ministre. C'est la question évidente qui nous met immédiatement dans le pétrin.

Madame Moffa, encore une fois, je vais essayer de suivre le même processus. Auriez-vous l'amabilité de nous envoyer ce dont vous aurez besoin, ce que vous pouvez? Si les membres du comité décident qu'ils ont besoin de renseignements supplémentaires, et cela nous amène dans les questions de sécurité, il existe des procédures pour traiter la question. Je ne vous place pas dans cette situation en ce moment, nous ne nageons pas dans ces eaux constitutionnelles. Comme le sous-ministre, je demande simplement si vous pouvez, comme vous l'avez offert, nous donner une réponse initiale concernant ce que vous pouvez faire.

Mais ne parlez pas de l'avertissement, car dès que vous le ferez, vous me mettrez dans la fâcheuse situation de défendre le droit des membres à un accès sans entrave aux documents. Alors si vous pouviez aussi nous donner ce que vous pouvez, ce que vous avez, dans les deux ou trois semaines, comme le fait le sous-ministre, le comité examinera les documents. Ensuite, si l'on doit se battre, l'on se battera. Au moins, cela nous permet de terminer la réunion d'aujourd'hui, cela nous donne de l'information et nous permet de nous laisser sur une note aussi positive.

J'aime les notes positives. Les notes positives sont géniales.

J'en profite pour remercier infiniment nos témoins, en particulier le vérificateur général, le sous-ministre et toutes les délégations.

Au nom de mes collègues, merci beaucoup. C'est un plaisir de travailler avec vous et nous vous savons gré de ce que vous faites. Nous nous reverrons sûrement tous très bientôt.

La séance est levée.