CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

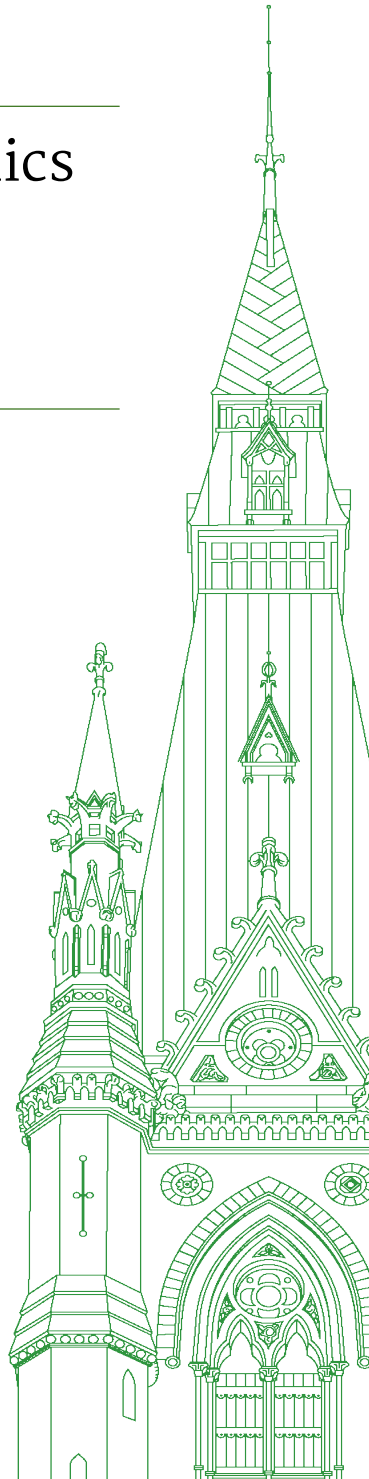
45e LÉGISLATURE, 1re SESSION

Comité permanent des comptes publics

TÉMOIGNAGES

NUMÉRO 022

Le lundi 26 janvier 2026



Président : John Williamson

Comité permanent des comptes publics

Le lundi 26 janvier 2026

● (1100)

[*Français*]

Le président (John Williamson (Saint John—St. Croix, PCC)): Bonjour, tout le monde.

J'ouvre maintenant la séance.

[*Traduction*]

Je tiens d'abord à vous souhaiter une bonne rentrée parlementaire après le temps des Fêtes. J'espère que tout le monde est reposé et prêt à se remettre au travail.

La température ces derniers jours n'est pas trop déprimante, même si je crois comprendre que la situation est pire à Toronto.

Jean Yip (Scarborough—Agincourt, Lib.): En effet, monsieur le président, il est tombé chez nous au moins 45 centimètres de neige.

Le président: Avez-vous déjà appelé les forces armées en renfort?

Jean Yip: Non, pas encore. En fait, nous sommes très fiers de nous débrouiller par nous-mêmes.

[*Français*]

Le président: Je vous souhaite la bienvenue à la 22e réunion du Comité permanent des comptes publics de la Chambre des communes.

[*Traduction*]

La séance d'aujourd'hui se déroule dans un format hybride, conformément au Règlement. Les membres du Comité seront donc présents en personne ou par l'entremise de l'application Zoom.

Je tiens à remercier tous nos invités d'être venus ici en personne aujourd'hui.

Avant de commencer, j'aimerais rappeler les points suivants aux participants. Veuillez attendre que je vous reconnaisse par votre nom avant de prendre la parole. Enfin, je vous rappelle que tous les commentaires doivent être adressés à la présidence.

[*Français*]

Conformément à l'article 108(3)g) du Règlement, le Comité entreprend l'examen du rapport sur la cybersécurité des réseaux et des systèmes du gouvernement, tiré des rapports d'automne 2025 de la vérificatrice générale du Canada et renvoyé au Comité le mardi 21 octobre 2025.

[*Traduction*]

Permettez-moi de vous présenter les invités que je viens de remercier de s'être déplacés en personne aujourd'hui malgré le mauvais temps.

Du Bureau du vérificateur général, nous avons le plaisir d'accueillir Andrew Hayes, sous-vérificateur général, ainsi que Jean Goulet, directeur principal. Messieurs, c'est un plaisir de vous recevoir.

Du Secrétariat du Conseil du Trésor, nous avons le plaisir d'accueillir Dominic Rochon, dirigeant principal de l'information du Canada, ainsi que Po Tea-Duncan, dirigeante principale de la sécurité de l'information du gouvernement du Canada. Je vous remercie de votre présence parmi nous aujourd'hui.

De Services partagés Canada, nous recevons Scott Jones, président. Monsieur Jones, c'est un réel plaisir de vous compter de nouveau parmi nous. Nous avons également le plaisir d'accueillir Patrice Nadeau, sous-ministre adjoint principal, Direction générale des services de connectivité et de sécurité. Bienvenue au Comité, monsieur Nadeau.

Enfin, nous accueillons deux représentants du Centre de la sécurité des télécommunications: Caroline Xavier, cheffe, que nous avons déjà eu d'ailleurs l'honneur d'inviter, ainsi que Rajiv Gupta, dirigeant principal, Centre canadien pour la cybersécurité.

Merci à tous d'être venus aujourd'hui. Je pense que nous aurons besoin des deux heures prévues, compte tenu du nombre d'illustres invités présents aujourd'hui. Chaque service disposera d'un temps de parole total de cinq minutes.

Monsieur Hayes, nous allons à présent vous permettre de briser la glace. Allez-y pour cinq minutes, je vous prie.

[*Français*]

Andrew Hayes (sous-vérificateur général, Bureau du vérificateur général): Bonjour, monsieur le président.

Je vous remercie de nous donner l'occasion de témoigner devant votre comité aujourd'hui pour discuter de notre rapport sur la cybersécurité des réseaux et des systèmes du gouvernement, qui a été déposé le 21 octobre 2025.

Je tiens d'abord à reconnaître que nous nous trouvons sur le territoire traditionnel non cédé du peuple anishinabe algonquin.

Je suis accompagné de M. Jean Goulet, qui est le directeur principal responsable de l'audit.

La responsabilité centrale de protéger les systèmes et les opérations de la technologie de l'information du gouvernement incombe conjointement au Secrétariat du Conseil du Trésor du Canada, au Centre de la sécurité des télécommunications Canada et à Services partagés Canada. Ces organisations collaborent entre elles et avec les ministères et les organismes pour prévenir le vol de données et limiter la perturbation des systèmes qui assurent la prestation de programmes et de services à la population canadienne. Bien que le gouvernement fédéral dispose d'outils pour protéger et défendre ses réseaux et ses systèmes contre les cyberattaques, nous avons constaté qu'il y avait d'importantes lacunes dans les services de défense de cybersécurité, la surveillance et les interventions lorsque des attaques se produisaient.

● (1105)

[*Traduction*]

Seulement 42 % des ministères et organismes fédéraux sont tenus, en vertu de la politique du Conseil du Trésor, d'utiliser les services de défense en matière de cybersécurité offerts par Services partagés Canada et le Centre de la sécurité des télécommunications. D'autres organismes fédéraux ont choisi de le faire, mais cette utilisation inégale des services nuit à la capacité du gouvernement d'assurer la protection des renseignements essentiels, et de gérer efficacement les risques.

Par ailleurs, nous avons constaté lors de récentes cyberattaques actives que la coordination entre les trois organismes susmentionnés s'était avérée trop lente. Par exemple, une mauvaise coordination a retardé la réponse du gouvernement lors d'une attaque majeure survenue il y a deux ans. Cela a prolongé la période pendant laquelle les pirates informatiques ont eu accès aux renseignements personnels d'un grand nombre de fonctionnaires.

La protection des réseaux et des systèmes fédéraux nécessite également l'analyse des vulnérabilités potentielles de l'ensemble des appareils informatiques du gouvernement, y compris les ordinateurs portables, les téléphones intelligents, et les serveurs. Fait inquiétant, nous avons constaté que ni Services partagés Canada ni le Centre de la sécurité des télécommunications ne disposaient d'un inventaire complet des appareils gouvernementaux. En l'absence d'un inventaire complet mis à jour, le gouvernement fédéral risque de ne pas être en mesure de réagir rapidement à l'évolution de tous les types de menaces en matière de cybersécurité.

Nous assistons depuis plusieurs années à une multiplication des actes malveillants visant les systèmes numériques du gouvernement canadien, et ces actes sont de plus en plus sophistiqués. Par conséquent, une approche coordonnée et globale de la cybersécurité du gouvernement, une meilleure collaboration, ainsi que la mise à jour des inventaires des appareils informatiques sont essentielles pour protéger les renseignements de la population canadienne.

[*Français*]

Monsieur le président, je termine ainsi ma déclaration d'ouverture. Nous serons heureux de répondre aux questions des membres du Comité.

Merci.

Le président: Merci beaucoup, monsieur Hayes.

Monsieur Rochon, vous avez la parole pour cinq minutes.

[*Traduction*]

Dominic Rochon (dirigeant principal de l'information du Canada, Secrétariat du Conseil du Trésor): Je vous remercie, monsieur le président.

Je suis ravi de vous parler de l'audit de performance de la vérificatrice générale sur la cybersécurité des réseaux et systèmes gouvernementaux, qui constitue le cinquième rapport de la série de rapports de l'automne 2025.

Je suis heureux d'être accompagné aujourd'hui par mes collègues de Services partagés Canada, du Centre de la sécurité des télécommunications, du Bureau du vérificateur général et, en particulier, de Po Tea-Duncan, dirigeante principale de la sécurité de l'information du gouvernement du Canada.

Monsieur le président, il est essentiel de protéger l'infrastructure informatique du gouvernement contre toutes lacunes, afin de protéger tant les données des Canadiens que les services fournis par le gouvernement. À mesure que les Canadiens ont de plus en plus recours aux programmes et services gouvernementaux en ligne, la sécurité de nos réseaux revêt une importance sans précédent.

Le Secrétariat du Conseil du Trésor du Canada est mentionné dans deux des recommandations formulées dans le rapport de la vérificatrice générale. La première recommandation est que le SCT, en consultation avec le Centre de la sécurité des télécommunications, veille à ce que les organismes fédéraux mettent en œuvre les capteurs de cyberdéfense du Centre de la sécurité des télécommunications sur tous leurs terminaux informatiques afin que les vulnérabilités associées puissent être identifiées et corrigées.

La seconde recommandation est que le SCT, Services partagés Canada, et le Centre de la sécurité des télécommunications réévaluent leurs pratiques de gestion des incidents de cybersécurité afin de permettre une meilleure coordination et un accès rapide aux renseignements essentiels.

[*Français*]

Le gouvernement s'est engagé à réduire les risques liés à la cybersécurité afin de protéger ses systèmes et, par conséquent, les renseignements des Canadiens et des Canadiennes, et à assurer la prestation continue de services numériques sécurisés et fiables. Le Secrétariat du Conseil du Trésor accueille favorablement les recommandations de la vérificatrice générale et poursuivra sa collaboration avec Services partagés Canada et le Centre de la sécurité des télécommunications Canada afin d'y donner suite.

En ce qui concerne l'évaluation de nos pratiques de gestion des incidents de cybersécurité pour améliorer la communication rapide de renseignements critiques, le Secrétariat du Conseil du Trésor, en collaboration avec ses partenaires, vérifie régulièrement notre cadre opérationnel, le Plan de gestion des événements de cybersécurité du gouvernement du Canada.

Les leçons tirées des exercices de simulation cybernétique, également appelées « exercices sur table », permettent au SCT de cerner les améliorations qui sont ensuite appliquées au plan afin d'en garantir l'efficacité.

Le gouvernement du Canada, comme toutes les organisations des secteurs public et privé, est confronté à des cybermenaces continues et en constante évolution. Afin de maintenir une forte position de cyberdéfense, le Secrétariat du Conseil du Trésor, en consultation avec le Centre de la sécurité des télécommunications Canada, collaborera avec les organisations fédérales pour s'assurer que les capteurs de défense du Centre sont installés sur tous les points d'extrémité, qu'il s'agisse d'appareils, de serveurs ou de postes de travail.

Nous y arriverons en partie grâce à un outil qui cerne rapidement les points d'extrémité de technologies de l'information sur lesquels aucun capteur n'est déployé. Cela nous permettra, par la suite, de détecter, d'évaluer et de prioriser les vulnérabilités à corriger sur les appareils informatiques des réseaux du gouvernement.

● (1110)

[*Traduction*]

Il convient de noter, monsieur le président, que le Conseil du Trésor du Canada a dévoilé la première Stratégie intégrée de cybersécurité du gouvernement du Canada. Cette stratégie est soutenue par un investissement de 11,1 millions de dollars sur 5 ans figurant dans le budget de 2024. Elle comprend l'établissement d'un programme pangouvernemental de gestion de la vulnérabilité pour permettre un processus coordonné de divulgation des vulnérabilités, ainsi que la formation d'une nouvelle équipe mauve qui imitera les techniques utilisées par les auteurs d'activités malveillantes contre les systèmes gouvernementaux. Ainsi, cela nous permettra de tester de manière proactive les éventuelles lacunes en matière de sécurité.

La stratégie décrit une approche pangouvernementale proactive pour veiller à ce que le gouvernement puisse lutter rapidement et efficacement contre les cybermenaces et éliminer les vulnérabilités dans l'ensemble du patrimoine numérique du gouvernement. La stratégie vise à protéger les systèmes gouvernementaux et les renseignements des Canadiens, et à améliorer la résilience du gouvernement afin d'assurer la prestation continue de services numériques sûrs et fiables. Nous souscrivons aux recommandations de la vérificatrice générale et, de concert avec nos partenaires, nous prenons des mesures pour répondre à ses préoccupations.

Je vous remercie. Après les remarques préliminaires de mes collègues, je répondrai aux questions des membres du Comité.

Le président: Merci beaucoup.

Nous allons à présent céder la parole à M. Jones pour les cinq prochaines minutes.

[*Français*]

Scott Jones (président, Services partagés Canada): Je vous remercie, monsieur le président, de nous donner l'occasion de discuter du rapport de la vérificatrice générale sur la cybersécurité des réseaux et des systèmes du gouvernement.

Avant de commencer, je tiens à reconnaître que nous sommes sur le territoire traditionnel non cédé du peuple anishinabe algonquin. Je suis accompagné de Patrice Nadeau, sous-ministre adjoint principal de la Direction générale des services de connectivité et de sécurité.

Services partagés Canada accepte les conclusions de la vérificatrice générale et travaille à résoudre les problèmes soulevés. Il est important de noter que la vérificatrice générale a constaté que le gouvernement disposait d'outils pour protéger et défendre ses réseaux et que le plan de cybersécurité du gouvernement était solide et complet.

En tant que fournisseur de services informatiques du gouvernement, SPC joue un rôle central.

[*Traduction*]

En effet, Services partagés Canada parvient à bloquer environ 6,5 billions de cybermenaces par an, soit une moyenne de 18 milliards par jour, ce qui garantit le fonctionnement ininterrompu des services gouvernementaux. Pour ce faire, nous utilisons une infrastructure d'entreprise de pointe et des solutions commerciales modernes de cybersécurité qui protègent les systèmes gouvernementaux contre un large éventail de cybermenaces. Par ailleurs, nos équipes mettent en place plusieurs niveaux de défense et de prévention, notamment des pare-feu, des défenses réseau, des mesures anti-déni de service, des outils antivirus et anti-logiciels malveillants, des mesures de cryptage, des réseaux privés virtuels, ainsi qu'un système d'identification robuste sur l'ensemble des services d'authentification.

Nous entretenons d'excellentes relations de travail avec nos collègues du Secrétariat du Conseil du Trésor et du Centre de la sécurité des télécommunications. La collaboration est absolument essentielle, comme l'a souligné la vérificatrice générale, et nous cherchons donc sans cesse des moyens de l'améliorer. Nous effectuons régulièrement des analyses rétrospectives des cyberévénements afin de déterminer comment nous pouvons toujours nous améliorer. Ensemble, SPC et le centre canadien de cybersécurité du CST fournissent des cyberdéfenses sophistiquées qui vont au-delà des capacités commerciales. Notre travail offre l'une des cyberdéfenses les plus sophistiquées au monde.

La cybersécurité est un domaine qui évolue rapidement, et nous travaillons donc sans relâche pour demeurer à la fine pointe des technologies. Cela dit, il reste encore beaucoup à faire, comme l'a souligné à juste titre la vérificatrice générale. Nous partageons les préoccupations de la vérificatrice générale concernant les organisations qui ne sont pas couvertes par le service Internet d'entreprise de SPC. Étant donné que l'environnement des menaces évolue rapidement, il est clair que ce modèle doit lui aussi évoluer. Voilà donc pourquoi SPC s'efforce actuellement de fournir des services de connectivité et de sécurité à 43 ministères et organismes fédéraux. Les travaux en ce sens devraient être achevés d'ici la fin mars 2027.

Par ailleurs, la vérificatrice générale a également mis en avant un projet intitulé Visibilité, sensibilisation et sécurité de point d'extrémité, ou VSSP en abrégé. Il s'agit d'un des outils que SPC ajoute à son environnement de cybersécurité. Le projet VSSP vise à nous permettre de détecter automatiquement les terminaux connectés au réseau, tels que les ordinateurs de bureau et les serveurs, et à s'assurer qu'ils répondent à l'ensemble des exigences en matière de sécurité. Contrairement à notre système de service semi-manuel, le projet VSSP est automatisé et permet d'évaluer en temps réel les vulnérabilités et les impacts. Par ailleurs, le projet VSSP nous permettra également de fournir une réponse automatisée aux cyberévénements. Bien que ce projet ait pris du retard, notre organisation en a tiré un certain nombre d'enseignements. Le projet VSSP a franchi une étape décisive et, depuis le début de sa mise en œuvre en juillet 2025, plus de 36 000 opérations de déploiement ont déjà été réalisées.

La vérificatrice générale a également souligné notre projet visant à mettre au point un système de gestion de solutions de gestion des informations et des événements de sécurité, ou GIES. Je tiens à vous assurer que nous sommes en bonne voie pour attribuer un contrat concurrentiel pour ce projet au début de 2026. Par ailleurs, SPC exploite actuellement une capacité provisoire de GIES, ce qui permet à nos partenaires du Centre canadien de cybersécurité de gérer leurs besoins prioritaires, et de répondre de manière efficace à différents types de cybermenaces.

Dès la création de SPC, nous avons transformé le modèle opérationnel du gouvernement, qui était cloisonné et décentralisé, en une approche pangouvernementale. Cela permet non seulement de réduire les coûts, mais aussi de renforcer la sécurité globale à l'échelle du gouvernement du Canada. Par ailleurs, il est plus facile d'effectuer des investissements, des améliorations et des correctifs au sein d'un seul système intégré plutôt que dans 45 systèmes distincts.

Pour conclure, je tiens à rappeler que notre travail est loin d'être terminé; SPC s'efforce chaque jour de moderniser la gestion des appareils et des logiciels, notamment par la simplification du processus d'approvisionnement. Cela nous permet de réaliser des gains d'efficacité considérables, et de réduire le risque d'incohérences en matière de politiques de sécurité. Par ailleurs, un autre rapport de la vérificatrice générale met en lumière la vulnérabilité de différents systèmes existants. Nous continuons donc également à réduire les doublons, et à remplacer les outils administratifs cloisonnés par des outils standardisés à l'échelle du gouvernement.

● (1115)

[*Français*]

Bref, tout ce que nous faisons pour consolider et moderniser les systèmes informatiques est essentiel pour améliorer la cybersécurité.

Les rapports de la vérificatrice générale du Canada sont aussi un outil important qui nous permet de rendre des comptes et d'améliorer nos opérations. La cybersécurité est un domaine en constante évolution, et les acteurs ne suivent pas toujours nos règles. Les améliorations sont primordiales si nous voulons protéger les systèmes informatiques du gouvernement.

Je vous remercie de m'avoir donné l'occasion de m'exprimer sur ce dossier important. Je serai heureux de répondre à vos questions.

Merci.

Le président: Nous vous remercions, monsieur Jones.

Madame Xavier, vous avez maintenant la parole pour cinq minutes.

Caroline Xavier (cheffe, Centre de la sécurité des télécommunications): Merci.

[*Traduction*]

Bonjour, monsieur le président, mesdames et messieurs les députés.

[*Français*]

Je vous remercie de m'avoir invitée à venir discuter du rapport de la vérificatrice générale du Canada sur la cybersécurité des réseaux et des systèmes du gouvernement du Canada.

[*Traduction*]

Comme vous venez de l'entendre, je m'appelle Caroline Xavier, et je suis la cheffe du Centre de la sécurité des télécommunications, ou CST.

Je suis accompagnée de Rajiv Gupta, dirigeant principal du Centre canadien pour la cybersécurité, qu'on appelle aussi le Centre pour la cybersécurité et qui fait partie intégrante du CST.

[*Français*]

Nous sommes heureux de témoigner aux côtés de nos collègues du Secrétariat du Conseil du Trésor et de Services partagés Canada, avec qui nous collaborons étroitement sur des questions de cybersécurité.

[*Traduction*]

Aujourd'hui, je vais vous donner un aperçu du CST et de notre Centre pour la cybersécurité, puis je vous expliquerai comment nous faisons face au contexte de menaces de plus en plus complexe, qu'il s'agisse de cybermenaces, de risques à la sécurité économique, d'extrémisme violent, d'ingérence étrangère ou de campagnes de désinformation, entre autres choses.

[*Français*]

Avant de commencer, je veux aussi souligner que nous nous trouvons sur les territoires traditionnels non cédés de la nation anishinabe algonquine. Nous soulignons que cette nation occupe ces territoires depuis des temps immémoriaux.

Le Centre de la sécurité des télécommunications Canada, ou CST, est un organisme autonome qui relève du ministère de la Défense nationale et est l'un des principaux organismes canadiens de sécurité et de renseignement.

[*Traduction*]

Dans le cadre de notre mission, nous fournissons du renseignement électromagnétique étranger essentiel sur diverses menaces pour aider le gouvernement à prendre des décisions éclairées et à protéger les intérêts du Canada, en observant rigoureusement les lois canadiennes et les normes de protection de la vie privée. Nous assurons aussi la défense des réseaux et des systèmes d'importance du gouvernement du Canada contre les cyberactivités malveillantes ciblant l'infrastructure numérique du pays.

Par l'entremise du Centre pour la cybersécurité, nous sommes l'autorité technique nationale en matière de cybersécurité, et la seule et unique source d'avis et de conseils spécialisés et dignes de confiance sur le sujet pour la population et les organisations canadiennes. Grâce à ses activités relatives à la cybersécurité, au renseignement électromagnétique et aux cyberopérations étrangères, le CST est particulièrement bien placé pour renforcer la défense et la sécurité du Canada.

L'intégrité du cyberespace canadien est essentielle à l'avenir du pays. Elle soutient notre économie numérique, assure notre sécurité personnelle et renforce notre résilience nationale.

De 2024 à 2025, le CST a produit plus de 3 300 rapports de renseignement étranger et est intervenu dans plus de 2 500 incidents de cybersécurité touchant des institutions fédérales et des partenaires du secteur des infrastructures essentielles. Il a aussi diffusé au-delà de 330 notifications de signes avant-coureurs d'une attaque par rançongiciel à plus de 300 organisations canadiennes, leur fournissant ainsi des avertissements précoces qui ont aidé à prévenir des préjudices graves.

Nous évoluons au même rythme que le contexte des cybermenaces. Notre programme de capteurs de cyberdéfense, qui est reconnu à l'échelle mondiale, permet la détection en temps réel des cyberactivités malveillantes dans les réseaux et les environnements infonuagiques du gouvernement. Ce programme est offert sur demande à l'ensemble des ministères, sociétés d'État et organismes fédéraux, et permet à nos spécialistes de bloquer et de neutraliser les menaces avant qu'elles ne causent des dommages.

Bien que de nombreuses organisations fédérales gèrent leur propre infrastructure de TI, elles peuvent tirer parti du programme de capteurs du CST et demander l'avis de spécialistes du Centre pour la cybersécurité pour renforcer leurs défenses. Aujourd'hui, la plupart des institutions fédérales utilisent au moins un de nos capteurs. Nous continuons d'approfondir notre collaboration avec les sociétés d'État, les exploitants des infrastructures essentielles et nos partenaires provinciaux et territoriaux.

Le CST accueille favorablement le rapport de la vérificatrice générale et appuie ses recommandations, tout particulièrement celles qui portent sur le déploiement accru de capteurs et l'amélioration de la coordination de la gestion des incidents. Comme mes collègues l'ont souligné, nous travaillons en étroite collaboration pour élargir le déploiement des capteurs de cyberdéfense dans les réseaux fédéraux et améliorer les protocoles d'intervention en cas d'incident.

● (1120)

[*Français*]

Ces conclusions s'appuient sur les progrès importants déjà réalisés pour moderniser et sécuriser les systèmes numériques qui fournissent des services essentiels aux Canadiens et Canadiennes. La cybersécurité est une responsabilité partagée et la collaboration reste au cœur de notre approche.

Monsieur le président et membres du Comité, l'environnement de menaces est dynamique, mais notre engagement reste inébranlable. De concert avec nos partenaires, nous continuerons à protéger les systèmes du gouvernement du Canada, de même que les infrastructures essentielles et les systèmes numériques du pays pour que les Canadiens et les Canadiennes puissent compter sur des services sécurisés et fiables.

Encore une fois, nous vous remercions de nous avoir donné l'occasion de témoigner ce matin.

[*Traduction*]

Nous répondrons avec plaisir à vos questions et nous avons hâte de poursuivre le dialogue.

Merci.

Le président: Merci beaucoup à vous tous.

Nous allons maintenant entamer notre première série de questions. Trois députés interviendront à tour de rôle, chacun disposant de six minutes.

Madame Kusie, c'est vous qui ouvrirez le bal cette année. Merci.

Stephanie Kusie (Calgary Midnapore, PCC): Plus tôt ce mois-ci, le premier ministre a annoncé un nouveau partenariat stratégique entre le Canada et la Chine. Cette annonce m'inquiète à bien des égards, mais pour les besoins de la réunion d'aujourd'hui, ce sont surtout la cybersécurité du Canada et la protection de nos renseignements personnels qui me préoccupent.

En 2024, l'Alliance interparlementaire sur la Chine m'a informée, par l'entremise du FBI, que j'avais été la cible d'une cyberattaque orchestrée par la République populaire de Chine. J'avais été ciblée en raison de mon statut de députée. Alors que le gouvernement canadien entame une nouvelle relation économique avec la République populaire de Chine, je suis préoccupée par la façon dont il évalue ces nouveaux partenariats stratégiques avec des pays non démocratiques sur la scène mondiale.

Madame Xavier, pouvez-vous dire au Comité quelles mesures vos organismes et vos ministères prennent pour assurer la cybersécurité et la protection des données sensibles au moment où nous concluons de nouveaux accords avec des gouvernements comme celui de la République populaire de Chine?

Caroline Xavier: Comme je l'ai mentionné dans ma déclaration préliminaire, le CST exerce de multiples mandats au sein d'un seul organisme, notamment la collecte de renseignements étrangers, afin de veiller à ce que les décideurs disposent de l'information dont ils ont besoin pour prendre des décisions. C'est quelque chose que nous faisons depuis près de 80 ans. Notre mandat comporte également un volet dédié à la cybersécurité ou à la cyberdéfense, et il y a un autre volet consacré aux cyberopérations étrangères. Le fait de regrouper tous ces éléments au sein d'un même organisme nous aide vraiment à utiliser les renseignements tirés de la collecte de données à l'étranger pour défendre le Canada, et vice versa. Les milliards d'incidents contre lesquels nous protégeons le Canada nous permettent d'en apprendre davantage sur les auteurs de menaces qui pourraient s'intéresser à notre pays. Cela oriente ensuite ce que nous pouvons faire en matière de renseignement étranger dans le cadre de notre mandat. De plus, grâce aux cyberopérations étrangères, nous pouvons prendre des mesures dans le cyberespace étranger pour nous assurer de continuer à protéger le Canada.

Nous menons nos activités en fonction des priorités en matière de renseignement approuvées par le Cabinet, lesquelles sont revues régulièrement. À l'heure actuelle, notre mandat englobe la protection des infrastructures essentielles et des institutions démocratiques du Canada. Qu'il s'agisse d'États-nations ou de cybercriminels, cela fait partie du mandat que nous remplissons au quotidien, 24 heures sur 24, à longueur d'année. Nous restons déterminés à effectuer notre travail en toute efficacité. Je suis heureuse et fière que nous dirigions une organisation qui met en place une cyberdéfense de calibre mondial. Le travail que nous accomplissons avec nos deux partenaires, soit le Conseil du Trésor et Services partagés Canada, nous permet de continuer à protéger les systèmes du gouvernement du Canada.

● (1125)

Stephanie Kusie: Merci beaucoup de cette réponse détaillée.

Vous avez dit que votre organisation protège notre pays contre des milliards d'interactions ou d'interceptions négatives; or, il me semble évident, d'après mon expérience et celle de plusieurs autres députés, que les acteurs malveillants les plus rusés parviennent encore à infiltrer le système, ce qui me préoccupe beaucoup.

Vous avez mentionné la participation d'autres décideurs. Y a-t-il des ministres qui vous ont donné des directives précises et, le cas échéant, pourriez-vous nous dire de qui il s'agit?

Caroline Xavier: Encore une fois, je vous remercie de me donner l'occasion d'apporter des précisions.

Nos priorités en matière de renseignement sont déterminées par le Cabinet du gouvernement du Canada. Nos services de renseignement...

Stephanie Kusie: De quels membres du Cabinet s'agit-il, s'il vous plaît?

Caroline Xavier: Le Cabinet au complet approuve les priorités du gouvernement du Canada en matière de renseignement...

Stephanie Kusie: Qui donne les directives, je vous prie?

Caroline Xavier: C'est le Cabinet dans son ensemble, sous la direction du premier ministre du pays. Nous avons ainsi publié les priorités en matière de renseignement afin que les Canadiens aient l'occasion de les comprendre. Les priorités sont assez vastes, et nous en tenons compte dans le cadre de notre travail.

Stephanie Kusie: Merci beaucoup, madame Xavier. Je n'ai pas réussi à obtenir beaucoup d'informations claires et utiles sur ces priorités ni sur la façon dont elles sont mises en œuvre, mais je vous remercie quand même.

Monsieur Hayes, votre rapport d'octobre n'est pas le premier à mettre l'accent sur la cybersécurité. Je suis sûre que ce ne sera malheureusement pas le dernier non plus, à mesure que le rôle de la technologie continue de gagner en importance.

Croyez-vous que des acteurs hostiles comme la République populaire de Chine pourraient tenter d'exploiter les lacunes en matière de sécurité que vous avez mentionnées dans ce rapport?

Andrew Hayes: Il ne fait aucun doute que le gouvernement est la cible d'attaques quotidiennes. En effet, il en déjoue des milliards, voire des billions, chaque année. Je pense que le message à retenir de notre rapport, c'est que la vigilance et la rigueur doivent être au cœur des préoccupations de toutes les organisations gouvernementales.

Voici, selon nous, l'un des principaux constats de notre rapport: ce ne sont pas toutes les organisations fédérales qui sont tenues de recourir aux services fournis par Services partagés Canada et le Centre de la sécurité des télécommunications Canada. À notre avis, il s'agit là d'une occasion manquée.

Stephanie Kusie: Je vous remercie.

Monsieur Rochon, au cours de la dernière année, le gouvernement a mis l'accent sur l'intelligence artificielle et son utilisation à l'intérieur et à l'extérieur de l'administration publique fédérale. L'intelligence artificielle ouvre un monde de possibilités, mais aussi un monde d'incertitudes.

Comment les Canadiens peuvent-ils avoir l'assurance que leurs renseignements confidentiels resteront protégés et privés si votre ministère ne peut même pas amener les organisations fédérales à respecter les règles et les politiques existantes en matière de cybersécurité?

Dominic Rochon: Je remercie la députée de sa question, monsieur le président.

Permettez-moi simplement de dire que la difficulté tient au fait que... L'article 7 de la Loi sur la gestion des finances publiques autorise le Conseil du Trésor à appliquer des politiques administratives générales, comme la Politique sur la sécurité du gouvernement et la Politique sur les services et le numérique. Ces politiques s'appliquent aux ministères et aux organismes qui relèvent d'une certaine annexe de la Loi. C'est ainsi que le cadre législatif est établi et, par conséquent, nous ne pouvons pas imposer aux agents du Parlement ou aux sociétés d'État...

Stephanie Kusie: Ce n'est pas très efficace si vous ne pouvez pas imposer...

Le président: Madame Kusie, je crains que votre temps soit écoulé. Nous aurons certainement l'occasion de vous réentendre.

Stephanie Kusie: Merci, monsieur le président.

Le président: La parole est maintenant à Mme Yip.

Vous avez six minutes.

Jean Yip: Merci, et bonne année.

Je tiens à remercier nos témoins d'être venus en cette petite journée de neige ici, à Ottawa. Je vous ferai remarquer que Toronto a reçu 45 centimètres de neige. Il est rare que nous dépassions Ottawa en la matière.

Des voix: Ha, ha!

Jean Yip: Ma question s'adresse aux trois organisations. Comment travaillez-vous à améliorer la collaboration entre vos trois organisations respectives? Quelles mesures avez-vous prises pour aider à protéger la sécurité nationale du Canada?

Monsieur Jones, voulez-vous commencer?

Scott Jones: Bien sûr. Je vous remercie de la question.

Je pense que nous faisons des progrès dans quelques domaines.

Premièrement, les relations que nous avons établies sont le fruit d'une collaboration de plus d'une décennie, à mesure que nous avons mis en place ce système de défense robuste. Même si je suis censé diriger une organisation à vocation technologique, l'efficacité de toute intervention en cas d'incident cybernétique repose sur les relations et la confiance parce que, bien souvent, il faut faire preuve de jugement avant d'avoir toutes les certitudes. Voilà pour le premier point.

Deuxièmement, nous menons des exercices. M. Rochon a parlé de l'équipe violette et de certaines autres initiatives qui ont été lancées récemment à titre d'exercices. L'une des conséquences d'un mécanisme de défense robuste est que... Lorsque j'ai commencé à travailler en cybersécurité avec M. Gupta il y a environ 14 ou 15 ans, pas une journée ne passait sans que nous ayons à réagir à des incidents. Aujourd'hui, nos systèmes gèrent bon nombre de ces choses de manière proactive, et les incidents d'envergure dont nous avons parlé ne se produisent pas souvent. Il faut donc continuer à s'entraîner pour maintenir ces capacités opérationnelles.

Ce sont là quelques-unes des mesures que nous prenons.

Troisièmement, il y a toujours des leçons à tirer de chaque incident. Nous effectuons une analyste complète après coup, sous la direction de mes collègues du Conseil du Trésor. Je vais les laisser en parler, mais c'est un élément très important. Même lorsqu'une intervention se déroule parfaitement bien, qu'aurions-nous pu améliorer? Qu'aurions-nous pu faire plus rapidement? Quelles leçons pourrions-nous en tirer?

Il faut toujours passer par là, et malheureusement, dans presque chaque incident lié à la cybersécurité, il y a une première victime. Notre objectif commun est de veiller à ce qu'il n'y en ait pas d'autres.

● (1130)

Dominic Rochon: Je pourrais peut-être apporter quelques précisions.

Il s'agit en effet d'un travail d'équipe. Comme Mme Xavier l'a souligné dans sa déclaration préliminaire, la cybersécurité ne relève pas d'une seule entité. Nous formons un groupe tripartite chargé de protéger les systèmes dans l'ensemble de l'appareil fédéral.

Au Secrétariat du Conseil du Trésor, nous avons mis en place des règles. En effet, nous avons adopté une stratégie intégrée de cybersécurité pour le gouvernement fédéral. Nous fournissons des conseils et des recommandations. De plus, comme M. Jones vient d'y faire allusion, nous avons un plan de gestion des événements de sécurité du gouvernement du Canada, qui est effectivement suivi. Ainsi, lorsqu'un incident critique survient, nous comprenons les rôles, les responsabilités, etc.

Comme l'a souligné la vérificatrice générale, cette coordination comporte certaines lacunes. Même si nous nous réunissons régulièrement et que nous coordonnons sans cesse nos activités, certains aspects peuvent être améliorés. En mai dernier, nous avons tenu pour la première fois un exercice de simulation à l'échelle de la haute direction, qui a fait intervenir plusieurs ministères et organismes. En nous inspirant des leçons tirées de cet exercice, nous allons mettre à jour notre plan de gestion des événements de sécurité, entre autres choses. Nous veillons également à ce que nos politiques et notre stratégie restent à jour. Comme M. Jones vient de le souligner, nous tirons des leçons de chaque incident critique.

En ce qui concerne nos efforts de coordination, ils vont de la gestion des politiques à l'élaboration des directives et des lignes directrices. C'est également le fruit d'un partenariat avec tous les ministères et organismes. Chacun d'eux doit désigner une personne responsable de la cybersécurité, qui est chargée de comprendre, d'interpréter et d'appliquer nos règles.

M. Jones et son organisation sont responsables des connexions Internet et de tout ce qui concerne l'infrastructure. Il y a ensuite la recette secrète, si l'on veut, c'est-à-dire le centre de cybersécurité dirigé par M. Gupta, qui, en plus de mettre en place des capteurs, mène toutes sortes d'activités de surveillance et communique avec les autres services du Centre de la sécurité des télécommunications pour que nous restions à l'affût des menaces.

Caroline Xavier: La seule autre chose que j'ajouterais, c'est que, comme je l'ai dit plus tôt dans mes observations, les activités de renseignement alimentent assurément tout ce que nous faisons pour fournir des conseils, des orientations et des directives. C'est un aspect utile, en plus des leçons que nous tirons de tous les incidents qui se produisent. En tant qu'organisation axée sur l'apprentissage, nous nous efforçons de toujours faire mieux. Comme l'a mentionné M. Jones, nous continuons d'appliquer ces leçons. J'ajouterais également qu'en tant que groupe tripartite, et compte tenu de la façon dont le gouvernement nous a organisés dans le domaine de la cyberdéfense, nous faisons l'envie de beaucoup grâce à notre mode de fonctionnement.

C'est pourquoi je suis heureuse que nous ayons les capteurs nécessaires pour assurer des interventions automatisées 24 heures sur 24, sept jours sur sept. Nous pouvons ensuite approfondir les analyses lorsque des incidents majeurs surviennent.

Jean Yip: Pourquoi faisons-nous l'envie des autres?

Caroline Xavier: C'est principalement parce que Services partagés Canada fait un excellent travail de coordination de toutes les activités pour fournir un service centralisé à un grand nombre de ministères fédéraux. Ceux qui obtiennent les services partagés sont alors protégés par les capteurs, car cela fait partie du déploiement standard lorsqu'on travaille pour le gouvernement du Canada et qu'on utilise les systèmes du gouvernement du Canada, dont Scott Jones assure la protection.

Monsieur Jones, n'hésitez pas à ajouter des observations. Nous avons entendu dire, par exemple, que le Parlement du Royaume-Uni avait vanté le système de capteurs de calibre mondial du gouvernement du Canada en reconnaissant qu'il s'agissait d'un des meilleurs au monde.

Le président: Merci, madame Yip.

Votre temps est écoulé. Je vous accorderai quelques secondes de plus la prochaine fois.

[*Français*]

Monsieur Lemire, bonjour. Vous avez la parole pour six minutes.

Sébastien Lemire (Abitibi—Témiscamingue, BQ): Merci, monsieur le président.

J'en profite pour vous souhaiter une très bonne année 2026. Je pense qu'elle sera très prometteuse pour les comptes publics. Du moins, on l'espère.

Merci à tous les témoins pour votre participation, et désolé du retard. Le Parlement, parfois, nous interpelle. Ça fait partie de nos fonctions.

J'aimerais d'abord mentionner que la Gendarmerie royale du Canada, Sécurité publique Canada, Affaires mondiales Canada, le Centre d'analyse des opérations et déclarations financières du Canada et le Centre canadien pour la cybersécurité ont publié, le 16 juillet 2025, un avis selon lequel les agents hostiles déployés par le gouvernement nord-coréen pouvaient se faire passer pour des travailleurs des technologies de l'information.

Mme Kelly Hutchinson, stratège en matière de gouvernement numérique et d'approvisionnement au sein du Compass Rose Group à Ottawa, a souligné que le cas de la Corée du Nord était simplement une goutte dans l'océan de ce problème.

Pour sa part, Aaron Shull, directeur de recherche au centre pour l'innovation en matière de gouvernance internationale, a souligné que la dépendance du Canada à la main-d'œuvre sous-traitée à l'étranger, jumelée avec des vérifications inconstantes de sécurité et d'identité, pouvait créer de réels angles d'attaque par l'obtention d'accès à des données sensibles, permettant ainsi de l'espionnage. Il a même parlé de la possibilité d'insérer certaines lignes de code malveillantes dans les systèmes et les logiciels gouvernementaux.

Madame Xavier, du Centre de la sécurité des télécommunications, j'aimerais savoir ce que vous pensez des propos de Mme Hutchinson et de M. Shull. Est-ce que la main-d'œuvre sous-traitée à l'étranger constitue un risque à analyser de façon approfondie dans une stratégie de cybersécurité?

● (1135)

Caroline Xavier: Merci pour la question.

Il est important de souligner, comme nous l'avons fait dans notre évaluation des cybermenaces qui a été publiée en octobre 2024, que nous reconnaissons que nous faisons face à des cybermenaces provenant d'États. Un des États qui a été nommé, c'est la Chine, mais on a aussi nommé la République populaire démocratique de Corée dans notre évaluation, ainsi que la Russie et d'autres.

Donc, oui, nous soutenons l'avis qui a été publié, parce qu'il a été publié en collaboration avec nous et le Centre de la sécurité des télécommunications, dont fait partie le Centre canadien pour la cybersécurité. Ce genre d'avis est une façon de nous assurer que nous sommes tous sur la même longueur d'onde et que nous pouvons présenter de bons avis et de bons conseils pour que le gouvernement canadien puisse se préparer.

Cependant, quand nous publions un tel avis, ce n'est pas seulement pour protéger le gouvernement. Nous voulons aussi nous assurer que les Canadiens et les responsables des infrastructures essentielles sont au courant. En effet, en ce qui concerne les cybermenaces, ce n'est pas juste le gouvernement qui est ciblé quand quelqu'un veut faire du mal au Canada.

Sébastien Lemire: Évidemment, nous sommes très vulnérables face aux États-Unis, et ce n'est pas en signant une entente avec la Chine pour importer des véhicules chinois qu'on va s'aider à garder nos données chez nous.

Cela dit, ma prochaine question est pour M. Rochon ou M. Jones.

Le gouvernement engage de nombreux travailleurs autonomes et des contractants. La question que Mme Hutchinson se pose est intéressante. Que fait le gouvernement pour authentifier les personnes et s'assurer qu'elles sont réellement qui elles sont, dans une ère où la fraude à l'identité est facilitée par des hypertrucages et d'autres outils? Qu'est-ce que vous avez mis en place?

Dominic Rochon: Nous avons mis en place des mesures de sécurité. Les sous-traitants doivent recevoir l'autorisation de travailler pour le gouvernement fédéral. Ils passent à travers différents niveaux de vérification dépendamment de ce à quoi ils vont avoir accès. Il y a des règles en place pour justifier puis certifier leur présence.

Bref, le problème, c'est que la menace va toujours être présente. Il est impossible de garantir à tout moment que nous avons tout couvert, alors nous mettons en place des règles. Nous avons mis en place un cours obligatoire que tous les fonctionnaires doivent suivre chaque année. Nous avons mis en place un programme de gestion des vulnérabilités où nous sommes en train de regarder les risques et nous faisons des suivis. Nous avons mis en place une équipe à la fois rouge et bleue de divers professionnels de la cybersécurité, comme je l'ai mentionné.

Madame Tea-Duncan, voulez-vous en dire davantage sur ces points?

[*Traduction*]

Po Tea-Duncan (dirigeante principale de la securite de l'information du gouvernement du Canada, Secrétariat du Conseil du Trésor): Je vous remercie de la question.

L'équipe violette nous permet de mener des tests en vue de pouvoir contrer certaines des techniques employées par les acteurs malveillants. Cela nous aide à mettre en place les bonnes mesures de détection et de protection pour nous assurer de garder une longueur d'avance sur les cybermenaces.

La Politique sur la sécurité du gouvernement veille notamment à ce que les ministères et les organismes déploient les contrôles de sécurité de base nécessaires. La cybersécurité s'articule autour de différents niveaux de contrôle — comme les cybercapteurs installés aux extrémités du réseau —, mais aussi de la protection des données au sein même de nos systèmes d'information. Tout cela est décrit dans la Politique sur la sécurité du gouvernement.

● (1140)

[*Français*]

Sébastien Lemire: Une des choses qu'on réalise quant aux systèmes de prête-nom, c'est que des compagnies se disent autochtones, mais qu'elles ne le sont finalement pas. À cause des sous-traitants, on ne sait jamais qui fait véritablement le travail, particulièrement lorsqu'il est envoyé en Inde ou dans d'autres pays pour être fait à un faible coût. On se rend compte qu'on est extrêmement vulnérable. Nous leur envoyons nos données. Est-ce qu'il existe un mécanisme pour assurer que le travail est fait par des gens du Canada, au Canada? Est-ce que ça existe ou est-ce correct que les portes d'entrée soient données partout dans le monde?

Dominic Rochon: C'est une question intéressante et difficile.

Chaque ministère et chaque sous-ministre est responsable de regarder comment mettre en place ses programmes. Au Secrétariat du Conseil du Trésor, nous mettons en place des directives pour qu'ils puissent savoir que des risques existent. Il faut regarder un peu la nature du travail et les systèmes auxquels ils vont avoir accès. S'ils ont accès à des systèmes, c'est là où nous, qui sommes devant vous aujourd'hui, avons un rôle à jouer. Il y a aussi des questions du point de vue des chaînes d'approvisionnement pour l'équipement.

Pour toutes ces choses, nous avons des règles en place, puis des procédures pour faire des suivis. En fin de compte, c'est aussi un jeu d'équipe dans le sens où chaque ministère doit s'assurer de suivre nos règles, et nous devons être au courant de l'accès à nos systèmes et de la nature du travail de ces ministères.

Sébastien Lemire: Merci, monsieur Rochon.

Le président: Merci beaucoup, monsieur Lemire.

Nous commençons maintenant le deuxième tour de questions.

[*Traduction*]

Cinq députés disposant de temps de parole variables pourront poser leurs questions.

[*Français*]

Monsieur Deltell, vous avez la parole pour cinq minutes.

Gérard Deltell (Louis-Saint-Laurent—Akiawenhrahk, PCC): Merci beaucoup, monsieur le président.

Bien le bonjour à tous les collègues.

Bonne année 2026 à tous les gens ici et, bien entendu, à tous les Canadiens qui suivent nos travaux.

Messieurs et mesdames, merci beaucoup de votre présence et merci beaucoup de servir notre pays, votre pays, dans une situation aussi délicate que celle de la cybersécurité.

Monsieur le président, nous, les conservateurs, avons de très grandes préoccupations en matière de cybersécurité, et particulièrement quant au régime de Pékin. Ma collègue Mme Kusie, qui est une diplomate de carrière, a raconté son histoire personnelle et tout à l'heure. J'ai été jusqu'à présent épargné, comme peut-être bien des gens ici, mais on n'est jamais à l'abri de ça.

Madame Xavier, en réponse à la question de mon collègue M. Lemire, vous avez fait état des cyberattaques, des cybermenaces des États. Spontanément, le premier pays que vous avez identifié est le régime de Pékin. Pourriez-vous nous en dire davantage?

Caroline Xavier: Merci de la question.

Je n'ai pas fait nécessairement exprès pour mentionner le régime de Pékin en premier. Je voulais juste mentionner le fait que, dans notre évaluation des cybermenaces publiée à l'automne 2024, valable pour deux ans, nous avons clairement dit que nous voyons que certains États s'intéressent au Canada. Oui, nous nommons la Chine, mais nous nommons aussi d'autres acteurs comme l'Iran ou la Russie, entre autres.

En ce qui concerne notre évaluation des cybermenaces à l'époque, il est sûr que nous avons dit que, en effet, c'est un acteur très sophistiqué et très capable. Par contre, ça ne veut pas toujours dire que, même si c'est un acteur de la Chine, c'est nécessairement lié à l'État. Nous savons qu'il existe aussi des cybercriminels. D'ailleurs, dans la même publication, nous avons dit que les actions des cybercriminels sont aussi importantes du point de vue des cybermenaces envers le Canada et partout dans le monde.

Nous avons publié plusieurs autres documents dans lesquels nous avons dit avoir vu des acteurs. Ça fait partie de ce que nous faisons pour essayer d'assurer que le Canada et les infrastructures essentielles sont au courant de la façon de se protéger.

Gérard Deltell: Comme vous l'avez dit, il y a des acteurs, mais ils ne sont pas nécessairement liés à l'État. Toutefois, à partir du moment où on parle d'un État totalitaire, il est difficile de voir ces acteurs comme étant autonomes. On les voit plutôt comme des acteurs directement liés à l'État, particulièrement au régime de Pékin. Vous avez remarqué d'ailleurs que je fais attention de ne pas identifier le pays pour ne pas stigmatiser les Canadiens qui viennent de ce pays. Pour nous le problème, c'est le régime de Pékin, et non les citoyens.

À cet effet, je ne peux pas passer sous silence le fait que de ce côté de la Chambre, nous sommes très préoccupés par la visite qu'a faite la semaine dernière le premier ministre au régime de Pékin. Tous les griefs et tous les sujets contentieux que nous avions en matière de sécurité et en matière des droits de l'homme semblent s'être évaporés. C'est dommage, et nous sommes très préoccupés par cette approche. C'est un point de vue politique, je n'ai pas à vous questionner là-dessus.

Monsieur Rochon, tout à l'heure, en réponse à une question d'un collègue, vous avez dit que c'était un travail d'équipe. Vous avez trois entités ici, au Canada, c'est-à-dire le Centre de la sécurité des télécommunications, Services partagés Canada et le Secrétariat du Conseil du Trésor.

Monsieur Goulet, estimez-vous que ces trois entités travaillent en coordination ou qu'elles travaillent en isolation? Ce n'est pas une question de blâme, mais plutôt une question d'efficacité. Comme la technologie évolue à vitesse grand V, estimez-vous que des améliorations puissent être faites pour que les informations soient davantage partagées?

● (1145)

Jean Goulet (directeur principal, Bureau du vérificateur général): Je vous remercie de la question.

Sans aucune hésitation, nous avons constaté qu'il y avait effectivement une très grande coopération entre les entités. Cela étant dit, ça ne veut pas dire qu'il n'y a pas d'améliorations à y apporter. Nous le mentionnons dans notre rapport, qu'il s'agisse des divers projets qui sont retardés et qui sont quand même très importants pour les besoins en matière de cybersécurité au pays. Il y a définitivement une bonne coopération entre les trois entités.

Gérard Deltell: Monsieur Rochon, qu'est-ce qui pourrait être amélioré, selon vous? Quelles autres entités pourraient être améliorées pour s'assurer que vous êtes plus efficaces?

Dominic Rochon: Merci de la question.

Je vais commencer par dire que des améliorations peuvent toujours être apportées, surtout en ce qui concerne le partage de l'information.

Nous avons des gens très compétents qui travaillent dans les trois organisations. Ce n'est pas tous les jours qu'on a le réflexe de rassembler tout le monde pour résoudre le problème. Nos politiques exigent que, si un incident se produit dans un ministère quelconque, le Centre canadien pour la cybersécurité soit immédiatement averti. À partir de là, celui-ci va commencer son enquête. Je pense qu'il faut apporter des améliorations pour rassembler tout le monde afin qu'on soit tous au courant. Il y a aussi des questions que nous n'avons pas encore mentionnées aujourd'hui en ce qui concerne l'accès à la vie privée. Si des informations personnelles y sont incorporées, il faut absolument ramener le commissaire à la protection de la vie privée dans l'équation. C'est une question d'exercer ces réflexes, d'avoir des exercices pour s'assurer que tout le monde comprend son rôle et ses responsabilités et que tout le monde travaille ensemble.

Le président: Merci beaucoup.

[*Traduction*]

Monsieur Osborne, vous avez la parole pour une période de cinq minutes.

Tom Osborne (Cape Spear, Lib.): Merci, monsieur le président.

Je pense que nous devons garder à l'esprit le fait que les producteurs de canola ou les pêcheurs du Canada atlantique peuvent commercer avec un pays sans que la cybersécurité entre nécessairement en jeu. Je ne suis pas certain qu'il y ait un lien entre les deux. Nous devons donc non seulement renforcer la cybersécurité, mais aussi faciliter nos échanges commerciaux.

Je pense que c'est la première fois que je prononce ces mots... Il y a eu une menace à la sécurité contre les services de santé de Terre-Neuve-et-Labrador. Comme j'ai présidé le comité du Cabinet qui s'est penché sur la question, j'ai une assez bonne idée de cequi est en jeu. C'est la première fois que j'en parle publiquement, parce qu'on nous a conseillé de ne jamais le faire. En notre qualité de parlementaires, nous sommes probablement la cible d'acteurs malveillants qui peuvent aussi bien être des États-nations que des organisations très bien structurées qui tirent profit de manœuvres semblables.

Étant donné la nécessité d'assurer un juste équilibre entre le droit du public de savoir ce qui se passe et la sécurité de notre pays, je pense que nous devons être prudents dans les questions que nous posons ici, vu l'importance du travail que vous accomplissez. Nous devons nous assurer de nous attaquer aux maillons faibles.

J'ai deux questions et la première s'adresse M. Rochon.

En ce qui concerne l'équipe violette, comment nous assurons-nous que ce groupe de professionnels est capable de garder une longueur d'avance dans le contexte d'une problématique qui évolue très rapidement — d'heure en heure, voire de minute en minute, au fur et à mesure que nous mettons en place de nouveaux moyens de défense pour protéger notre information et assurer notre cybersécurité — alors même que des acteurs malveillants s'emploient sans cesse à contourner les mesures que nous prenons à cette fin?

● (1150)

Dominic Rochon: C'est là que le bât blesse. Le défi que nous devons relever au quotidien consiste à garder une longueur d'avance sur des auteurs de menaces utilisant des moyens de plus en plus perfectionnés.

Une députée a parlé aujourd'hui de l'intelligence artificielle. Même si nous sommes emballés par toutes les possibilités que peut offrir l'intelligence artificielle, on peut imaginer que des acteurs malveillants chercheront à s'en servir à mauvais escient.

J'aimerais apporter une précision concernant l'équipe violette. C'est une initiative que nous venons de lancer et qui en est encore pour une bonne part à l'étape du projet pilote. Nous comptons sur les ministères et les organismes pour nous indiquer qu'ils ont mis en place toutes les mesures et toutes les défenses que nous avons préconisées notamment dans nos politiques, notre stratégie cybernétique et nos lignes directrices sur la gestion des vulnérabilités. L'équipe violette intervient sans qu'un ministère ou un organisme soit au courant pour effectuer les vérifications requises et déterminer si ses moyens de défense sont vraiment à la hauteur. Nous le faisons bien sûr en partenariat avec Services partagés Canada et le CST qui ont l'expertise nécessaire et qui savent parfaitement où peuvent se situer les vulnérabilités. Au fur et à mesure que ces choses sont mises en lumière, il nous est possible de mener des tests et de mettre au jour davantage de lacunes en la matière.

Par ailleurs, je pense que mon collègue, M. Gupta, serait mieux placé pour répondre précisément à votre question sur la façon dont nous gardons une longueur d'avance à l'égard de menaces de plus en plus pointues. Sauf erreur, son organisation publie chaque année ou tous les deux ans le rapport sur les cybermenaces. Le CST est constamment à l'affût des nouvelles percées et adapte ses services, ses moyens de défense et ses efforts de repérage afin de pouvoir contrer ce phénomène.

Rajiv Gupta (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): En fait, il est très important pour nous de garder une longueur d'avance par rapport aux menaces qui nous guettent. La situation ne cesse d'évoluer; dès que nous parvenons à sécuriser certaines zones, d'autres deviennent la cible d'acteurs malveillants. C'est exactement ce que nous sommes à même de constater au quotidien. Nous pouvons effectivement compter sur l'équipe violette pour maintenir cette longueur d'avance sur les entités qui nous menacent. Le Conseil du Trésor fait intervenir des experts de premier ordre dans ce secteur pour voir si nous arrivons à les détecter et si d'autres les détectent également, ce qui est un exercice important.

Mme Xavier a mentionné plus tôt la collaboration au sein du CST ainsi qu'avec nos partenaires du Groupe des cinq. Nous assurons une surveillance constante des auteurs de menaces partout dans le monde, en essayant de déterminer les prochaines techniques qu'ils utiliseront et les cibles qu'ils viseront, et nous mettons en œuvre des moyens de défense en conséquence.

Nous organisons des ateliers sur l'innovation avec les meilleurs de l'industrie partout au Canada et dans le monde. À titre d'exemple, la GeekWeek est une activité annuelle pour technophiles qui réunit des représentants d'infrastructures essentielles — banques, entreprises de télécommunications, etc. —, ainsi que de firmes de sécurité et de fournisseurs de services infonuagiques. Nous essayons tous ensemble de déterminer quels seront les prochains défis à surmonter.

Nous le faisons également pour nos actifs classifiés en faisant appel aux meilleurs cyberdéfenseurs au monde qui essaient de comprendre quelles sont ces menaces et comment nous pouvons les contourner. Il va s'en dire qu'il faut pour ce faire s'appuyer sur le renseignement et demeurer à la fine pointe de la technologie pour être en mesure de détecter les menaces et de mettre au point les outils les plus efficaces pour les contrer.

Vous avez parlé de l'intelligence artificielle. Il est très important pour nous de fournir des conseils et des directives sur la façon dont les organisations peuvent l'adopter en toute sécurité. Par ailleurs, nous utilisons également beaucoup l'intelligence artificielle à l'interne, en nous assurant de pouvoir ainsi étendre la portée de nos activités, tout comme les auteurs de menaces le font de leur côté.

Nous sommes à l'avant-garde du développement technologique, mais nous nous procurons également des renseignements sur les menaces provenant de nos propres services, d'entités commerciales et de nos partenaires pour nous assurer de bien comprendre ce qui se passe. Il se peut que nous trouvions encore des lacunes et, par la suite, quelque chose de nouveau, parce que c'est la réalité. La situation évolue sans cesse.

Le président: Merci beaucoup.

Votre temps est écoulé, monsieur Osborne. Je crois que nous reviendrons à vous plus tard.

[*Français*]

Monsieur Lemire, vous avez la parole pour deux minutes et demie.

Sébastien Lemire: Merci, monsieur le président.

Dans ses nombreux rapports, la vérificatrice générale a souligné une utilisation massive des sous-traitants dans le domaine informatique, qui peuvent avoir accès à des informations sensibles sans avoir les autorisations de sécurité ou toute la formation nécessaires. Ottawa dépense près de 3 milliards de dollars par année en services informatiques. En 2022, on parlait d'environ 7 700 sous-traitants dans le domaine de l'informatique. Donc, à mon avis, il y a là une faille énorme.

Monsieur Jones, vous pourriez être la meilleure personne pour répondre à ma question mais, évidemment, une autre personne peut répondre.

Je pense que nous sommes très vulnérables face à l'ingérence étrangère. Nous aurions besoin de garanties de sécurité. Quelles sont les garanties de sécurité exigées par le gouvernement? Est-ce que des vérifications sont faites pour que le travail des entreprises à qui vous donnez un contrat soit fait par des gens de cette entreprise, et non par des sous-traitants? De quelle façon allez-vous adapter vos méthodes d'attribution des contrats pour éviter de faire appel à des travailleurs étrangers situés dans des pays à risque, avec lesquels il y a des tensions diplomatiques? L'ordre mondial étant en train de changer, la liste des pays à qui nous pouvons faire confiance est plutôt limitée.

● (1155)

Scott Jones: Merci de la question.

Je peux seulement parler de l'engagement de sous-traitants et de contractants par Services partagés Canada.

Premièrement, pour accéder au système de Services partagés Canada, il est nécessaire d'obtenir un compte auprès de nous. Nous devons donc vérifier l'identité des individus qui vont avoir accès à nos systèmes et à nos informations.

Deuxièmement, nous évaluons constamment les systèmes de vérification, mais aussi de conservation et de sécurisation de l'information, pour que les individus puissent avoir accès seulement aux informations nécessaires à leur travail.

Ce sont nos processus de sécurité qui s'appliquent avant de donner un compte ou une carte d'identité pour accéder à nos installations, mais aussi pour vérifier l'identité de quelqu'un et le pays où la personne travaille.

Finalement, il y a aussi le processus d'approvisionnement. Le contrat contient des clauses qui nécessitent de l'information, ainsi que des cotes de sécurité liées au programme de sécurité de Services publics et Approvisionnement Canada.

Sébastien Lemire: Merci beaucoup.

Le président: Merci beaucoup.

[*Traduction*]

La parole est maintenant à M. Kuruc.

Vous avez cinq minutes.

Ned Kuruc (Hamilton-Est—Stoney Creek, PCC): Bonjour à tous.

Je vous remercie d'être venus aujourd'hui et je vous souhaite une bonne année.

Ma première question s'adresse à Mme Xavier.

Dans une citation tirée d'un document, vous avez dit que « la montée des cybermenaces facilitées par l'intelligence artificielle représente un problème de taille pour le processus démocratique du Canada ». Quels pays seraient selon vous des acteurs malveillants à cet égard?

Caroline Xavier: Je crois que la citation à laquelle vous faites référence est tirée de notre document sur les cybermenaces qui pèsent sur le processus démocratique. Presque tous les deux ans, nous publions un rapport intitulé *Cybermenaces contre le processus démocratique du Canada*, dans lequel nous évaluons ce que nous apprenons dans une perspective planétaire en cherchant à déterminer quelles menaces pourraient être préoccupantes, surtout s'il doit y avoir des élections générales, municipales ou provinciales. Nous examinons la question uniquement en fonction des activités de cybermenace ciblant ces élections. Nous observons généralement des manoeuvres comme les attaques par déni de service, la mésinformation et la désinformation, la manipulation des systèmes en ligne et des choses de cette nature.

Ned Kuruc: Je suis désolé, mais mon temps est limité.

Êtes-vous en train de dire que c'est un phénomène mondial et qu'il n'y a pas de pays précis que vous pourriez cibler?

Caroline Xavier: Ce que j'allais dire, c'est que dans *Cybermenaces contre le processus démocratique du Canada*, nous avons souligné que la Russie et la Chine sont à l'origine du plus grand nombre d'activités de cybermenace visant des élections étrangères. Il est important de noter que cela se passe à l'échelle mondiale.

Ned Kuruc: Merci beaucoup. Je vous remercie de votre réponse.

Ma prochaine question s'adresse à M. Gupta.

Vous auriez déclaré que « des auteurs de menace tirent de plus en plus profit de l'intelligence artificielle pour accroître l'ampleur et le degré de sophistication de leurs activités, dont des activités qui menacent les institutions démocratiques canadiennes. » Pourriez-vous me dire, en votre qualité d'expert, de quels pays il s'agit?

Rajiv Gupta: Je vous renvoie au même document que Mme Xavier a mentionné, *Cybermenaces contre le processus démocratique du Canada*. C'est d'un point de vue démocratique. Par ailleurs, l'intelligence artificielle démocratise cette capacité, et je pense que de plus en plus de pays continueront de se donner de meilleurs moyens en la matière parce qu'il est plus facile pour tous d'en tirer avantage.

Ned Kuruc: Conviendriez-vous alors avec Mme Xavier que la Chine et la Russie seraient probablement les deux principales menaces... parmi d'autres, évidemment?

Je comprends tout à fait qu'il s'agit d'un problème mondial, mais j'essaie de faire ressortir quelques éléments bien précis. En tant que conservateurs, nous avons toujours eu au sein de notre parti des préoccupations à cet égard. Je tiens d'abord et avant tout à vous féliciter tous les deux de votre excellent travail. Voilà que le premier ministre cherche à conclure de nouveaux accords commerciaux et qu'il semble vouloir se tourner très rapidement vers la Chine. Plus important encore, il s'agit de la Chine, mais lorsqu'il est question des voies de communication les plus importantes, nous devrions plutôt parler du Parti communiste chinois. C'est la véritable préoccupation, par opposition à la Chine et au peuple chinois. C'est le Parti communiste qui gouverne ce pays.

On nous conseille, à moi et à bon nombre de mes collègues conservateurs ici présents, de ne pas utiliser des outils comme TikTok. C'est ce que font 99 % des députés pour des raisons de sécurité, et je suis persuadé que je ne vous apprends rien. Les Canadiens ne peuvent pas acheter de téléphones Huawei. Le gouvernement précédent s'est attaqué à ce problème, et j'étais d'accord.

Il y a maintenant de graves inquiétudes au sujet des véhicules électriques chinois. Ce sera une menace non seulement pour le secteur de l'automobile en Ontario, mais aussi sur le plan de la sécurité. Monsieur Gupta, comment voyez-vous les choses et que diriez-vous de tout cela? L'arrivée de 50 000 véhicules électriques chinois sur notre marché représente-t-elle une menace?

● (1200)

Rajiv Gupta: Du point de vue de la sécurité, les véhicules électriques sont semblables à d'autres plateformes technologiques. Nous avons fourni des conseils et des orientations sur la numérisation croissante des infrastructures essentielles d'une manière générale. Je pense que c'est quelque chose que nous devons garder à l'esprit dans tous les domaines, parce que tout devient connecté à Internet.

En ce qui concerne les véhicules électriques, nous avons des lignes directrices sur la chaîne d'approvisionnement technologique et des évaluations des cybermenaces nationales. Nous avons toutes ces mises en garde que nous publions régulièrement sur notre site Web, et nous continuons de mettre les Canadiens au fait de ces menaces. Nous avons aussi un document traitant spécifiquement de la chaîne d'approvisionnement. Nous publions également des conseils et des lignes directrices sur la sécurité des communications à partir des véhicules. Il y a différents efforts qui sont déployés en ce sens. Je pense qu'il a été mentionné plus tôt que vous avez besoin de défenses à plusieurs niveaux, mais vous devez comprendre exactement dans quelle situation vous déployez les technologies et quelles mesures d'atténuation vous devez mettre en place. Nous recommandons... Pour les applications qui ne sont peut-être pas aussi sûres que vous le souhaiteriez, il y a des mesures d'atténuation que vous pouvez prendre, comme déconnecter Bluetooth et diverses précautions de la sorte, ce qui fait donc...

Ned Kuruc: Y aurait-il cependant un risque accru? Nous ne pouvons pas utiliser TikTok et Huawei, et certains de nos journalistes et députés doivent se servir de téléphones jetables lorsqu'ils vont visiter le Parti communiste chinois. Est-ce que ces véhicules électriques représentent une plus grande menace ou est-ce à peu près la même chose?

Rajiv Gupta: Dans l'ensemble, nous évaluons le risque en fonction d'un certain nombre de facteurs. Comme cela tient en partie à la chaîne d'approvisionnement, on examine les lois des différentes nations au fur et à mesure qu'elles entrent en jeu, on évalue la technologie, notamment pour ce qui est de la qualité et du déploiement des logiciels, puis on soupèse les risques juridiques et les dommages possibles pour la réputation. C'est la façon dont nous évaluons habituellement les produits. La combinaison de tous ces éléments entraîne un risque global. Il y a des produits qui sont mis au point d'une certaine manière et qui présentent des vulnérabilités en raison de lacunes techniques. Vous aurez...

Ned Kuruc: Mais il en va de même...

Le président: Merci. J'ai bien peur que votre temps soit écoulé, monsieur Kuruc.

Ned Kuruc: Merci beaucoup. Je vous remercie de vos réponses.

Le président: La parole est maintenant à Mme Tesser Derksen. Vous avez cinq minutes.

Kristina Tesser Derksen (Milton-Est—Halton Hills-Sud, Lib.): Merci beaucoup, monsieur le président.

Bienvenue à tous. Je suis heureuse que nous soyons de retour.

Je prends certainement à cœur les préoccupations de mes collègues en ce qui concerne les accords commerciaux avec des pays étrangers. Je sais toutefois que ce n'est rien de nouveau, car le gouvernement conservateur de Stephen Harper a négocié en 2014 l'Accord sur la promotion et la protection des investissements étrangers avec la Chine sans aucun débat public, et ce, très discrètement et rapidement.

C'est quelque chose qui couve depuis longtemps. Nous devons garder cela à l'esprit si nous voulons diversifier nos échanges commerciaux. Je me réjouis que nous puissions compter sur une équipe comme la vôtre pour nous guider dans cette démarche.

Pour en revenir au rapport, je tiens à souligner les chiffres stupéfiants qu'on y retrouve. C'est vraiment ce qui a attiré mon attention d'entrée de jeu. Il est question de billions d'interactions différentes du point de vue de la cybersécurité. J'aimerais que vous nous parliez des niveaux de menace, car je sais qu'il ne s'agit pas toujours d'attaques véritables. Sans vouloir minimiser les menaces à la cybersécurité, je suppose que bon nombre d'entre elles sont anodines. L'un d'entre vous — celui ou celle qui se sent le mieux à même de me répondre — pourrait-il commenter la hiérarchie de la qualification des menaces? Ne parle-t-on pas d'incidents, d'événements, puis d'attaques?

Rajiv Gupta: Bien sûr, je peux commencer.

Les perturbations ne manquent pas sur Internet. On vous frappe sans arrêt à des fins de reconnaissance. C'est essentiellement comme si des gens passaient devant chez vous et vérifiaient si vos portes et vos fenêtres sont bien fermées. Cela se produit sans interruption, des millions de fois par seconde. Je tenais simplement à ce que vous le sachiez. M. Jones a parlé de certaines des protections en place pour contrer ces mesures initiales de reconnaissance où l'on teste nos points d'accès. Comme cela n'arrête jamais, le nombre de ces blocages qui entrent en jeu se chiffre en billions.

Il y a des mesures de protection que nous avons mises en place pour contrer les menaces connues. Dès que nous repérons une menace, nous prenons les moyens pour empêcher qu'elle se matérialise, ce qui exige aussi des milliards de blocages.

Ensuite, il y a des menaces qui franchissent ce premier niveau et déclenchent un processus analytique. Nous pouvons alors constater qu'une action quelconque, si on la combine à certains autres éléments, peut devenir suspecte et inquiétante. Comment devons-nous y réagir? Il y en a des dizaines de milliers. Une partie de ce problème est traitée par des analyses automatisées qui amorcent les blocages nécessaires, 24 heures sur 24, sept jours sur sept.

Notre centre des opérations de sécurité, qui représente le deuxième niveau de défense pour le gouvernement du Canada, surveille la situation dans près de 180 ministères différents. Avec tous ces dispositifs automatisés qui bloquent des millions d'actions par jour, nous en arrivons peut-être à quelques centaines d'alertes qui doivent être évaluées par des êtres humains. Nous les examinons et les trions. Nous nous penchons peut-être ainsi sur 1 100 incidents par jour pour l'ensemble du gouvernement du Canada, et il y en a six ou sept qui se révèlent véritablement préoccupants.

Chaque jour, nous nous employons à régler ces incidents bien réels de concert avec nos partenaires ici présents. Lorsqu'on dit que la cybersécurité est un sport d'équipe... Nous nous voyons trop souvent — la nuit, le soir, tout le temps. Chaque jour, il y a environ six ou sept actions au titre desquelles nous intervenons activement et qui deviennent des incidents en bonne et due forme. Nous réussissons généralement à en atténuer les répercussions, mais il arrive que certaines menaces prennent de l'ampleur et nous devons alors tous redoubler d'ardeur pour pouvoir les contrer.

● (1205)

Scott Jones: Je pourrais peut-être ajouter une ou deux choses à ce que vient de dire M. Gupta.

Je l'appelle « monsieur » seulement pour l'occasion, car nous travaillons en étroite collaboration depuis une bonne vingtaine d'années.

M. Nadeau pourrait vous en parler plus en détail. Il ne se passe pas une minute sans qu'un ministère ne fasse l'objet d'une attaque par déni de service. L'équipe de M. Nadeau actionne alors nos défenses automatisées afin de réduire les impacts d'une telle agression. On ne remarque d'ailleurs presque jamais ces attaques grâce aux niveaux de défense que nous avons mis en place.

Lorsque les choses se compliquent, nous devons faire appel aux meilleurs dispositifs de défense disponibles sur le marché. Services partagés Canada est chargé de déployer ces moyens de défense et de les maintenir à la fine pointe de la technologie. Lorsque ces dispositifs sont déjoués — et il y a des pirates qui sont capables de le faire —, nous nous tournons vers nos collègues du Centre canadien pour la cybersécurité et du Centre de la sécurité des télécommunications.

C'est ce que j'appellerais la « recette secrète » du gouvernement du Canada. Nous pouvons ainsi compter sur un continuum d'interventions, plutôt que sur des mesures disparates. Je pense que cette intégration est l'un des éléments clés du rapport de la vérificatrice générale soulignant l'importance de regrouper les efforts pour adopter une approche globale en matière de cybersécurité. Il ne se passe pas une minute sans que nous subissions une attaque par déni de service en provenance de différentes régions du monde.

Kristina Tesser Derksen: Merci beaucoup. Vous avez tout à fait raison. J'ai noté que dans le rapport de la vérificatrice générale, le plan a été jugé « solide et complet ». Félicitations pour cela.

Je crois toutefois que la critique de la vérificatrice générale porte sur le fait que nous disposons de ces outils et de ces systèmes, mais que leur adoption par toutes les organisations n'est pas complète. J'aimerais poser une question à ce sujet.

Y a-t-il des obstacles politiques qui empêchent ces ministères de tirer parti de ces outils? S'agit-il d'un problème logistique? Je sais qu'on pourrait penser que cela pourrait porter atteinte à l'indépendance d'un organisme particulier. Pourriez-vous nous en dire un peu plus à ce sujet? Comment pouvons-nous résoudre ce problème?

Scott Jones: Absolument. Merci de poser la question.

Je pense que la première chose à noter, c'est que le mandat de Services partagés Canada est défini par un décret. Il y a 44 ministères qui doivent utiliser nos services, en particulier en matière de connectivité. Ces services sont ensuite proposés à un certain nombre d'autres entités, y compris, si elles le souhaitent, les sociétés d'État et d'autres encore.

Comme vous l'avez fait remarquer, certaines organisations ont choisi de ne pas y adhérer afin de préserver leur indépendance. Si l'on prend l'exemple du pouvoir judiciaire... Le pouvoir parlementaire a également choisi de ne pas adhérer à Services partagés Canada, pour des raisons d'indépendance, comme vous l'avez souligné. D'autres mesures ont été prises pour compenser cela, mais c'est ce qu'il est important de retenir.

De nombreux ministères ont choisi de ne pas adhérer à Services partagés Canada. Il y a plusieurs raisons à cela. La première est que cela coûte plus cher. Si vous utilisez simplement un accès Internet commercial standard, les mesures de protection commerciales que nous avons mises en place ne sont pas gratuites. Si vous vous passez de ces dispositifs de protection, vous prenez un risque, mais c'est un choix qui vous appartient. Vous n'avez peut-être pas les moyens de vous le permettre. C'est ce que l'investissement dans les petits ministères et organismes cherche à pallier. Il s'agit d'un financement qui leur permet d'accéder à des capteurs qu'ils ne pourraient pas se permettre autrement.

Ce n'est pas un service obligatoire. Pour la plupart des ministères et organismes, il est facultatif. C'est un choix qu'ils ont à faire. Mon ministère travaille en fonction du principe de recouvrement des coûts, alors ils doivent être en mesure de payer la facture.

Le président: Merci beaucoup.

Je veux faire en sorte que nous puissions avoir deux autres tours de table complets. Le gouvernement aura donc deux séries de questions supplémentaires, idem pour l'opposition.

[*Français*]

Le Bloc québécois aussi disposera de deux périodes de questions.

Madame Kusie, vous avez la parole pour cinq minutes.

[*Traduction*]

Stephanie Kusie: Merci beaucoup, monsieur le président.

Je commencerai par dire que je suis très préoccupée par le fait que ce gouvernement décrit systématiquement toute cyberattaque comme étant inoffensive. C'est la sécurité de notre nation qui est encore compromise. Je suis très préoccupée par le nouveau niveau de relations établi par le premier ministre. Cela m'inquiète beaucoup.

Pour poursuivre dans la même veine et comme je l'ai indiqué lors du premier tour de questions, l'APT31 — le groupe qui a piraté les parlementaires — était lié aux services de renseignement chinois. À la lumière de cette découverte, comment le Centre de la sécurité des télécommunications peut-il garantir que les renseignements partagés avec la Chine ne compromettront pas la cyberdéfense canadienne?

Caroline Xavier: Tout d'abord, il est important de reconnaître que, quelle que soit l'ampleur des mesures de cyberdéfense que nous mettons en place — et nous disposons d'un système de défense de grande qualité —, nous ne pouvons jamais garantir l'absence totale d'incidents. Le travail dans le domaine de la cyberdéfense est un sport d'équipe. C'est un travail que nous accomplissons avec toutes les personnes présentes à cette table, mais en plus, chacun doit jouer son rôle en faisant le nécessaire pour se protéger.

Il n'y a pas de partage de renseignements en cours concernant le Parti communiste chinois ou la République populaire de Chine. Nous travaillons à l'échelle mondiale avec de nombreux services de renseignement ainsi qu'avec des organismes internationaux. Cela fait partie de notre travail en matière de cyberdéfense, car il est très important d'apprendre des autres comment en ce qui concerne le fonctionnement de cette dernière.

Je ne m'exprimerai pas sur les intentions du premier ministre. Je vous laisse le soin d'en discuter directement avec lui. Je dirai toutefois que le rôle que joue le Centre de la sécurité des télécommunications au chapitre de la collecte de renseignements étrangers est très important. En particulier, lorsque le gouvernement prend des décisions, puisqu'il arrive que ces dernières se basent sur les intentions des autres.

Voilà les renseignements que nous rassemblons et que nous présentons dans le cadre de notre travail, en plus de tout ce que nous avons appris des nombreux incidents qui se produisent à l'échelle mondiale et de tout ce que nous partageons avec des organismes étrangers, dont le Groupe des cinq. Voilà comment nous fonctionnons, tant au niveau national qu'international.

● (1210)

Stephanie Kusie: Merci beaucoup de votre réponse.

J'ajouterai également que l'ancien premier ministre Harper avait la capacité de gérer nos relations avec le sud, une capacité que l'actuel premier ministre n'a pas. C'est pourquoi il a été contraint de s'incliner devant les dictateurs du monde entier. Je tiens à le préciser très clairement. Harper avait la capacité de gérer cette relation. Ce n'est pas le cas du premier ministre actuel, et c'est pourquoi il est contraint de se plier aux dictateurs, comme nous l'avons vu tout au long de cette semaine.

Pouvez-vous confirmer si, comme l'a mentionné mon collègue, les technologies produites par les entreprises publiques de Pékin seront interdites dans les opérations canadiennes de cybersécurité? Bien entendu, j'inclus là-dedans les opérations quotidiennes.

Caroline Xavier: Comme l'ont mentionné mes collègues, une partie de notre travail consiste à nous assurer que tous les outils que nous utilisons pour la cyberdéfense du Canada sont des outils qui ont mérité notre confiance et qui nous permettent de réduire les vulnérabilités qui nous préoccupent. Ils sont soumis à des tests rigoureux, à des évaluations rigoureuses. Dans les contrats d'approvisionnement relatifs à ces produits, nous définissons clairement les conditions qui doivent être remplies.

Quels que soient les produits que nous utiliserons, quel que soit leur pays d'origine, cela constitue la base du travail qui doit être fait. Cela est particulièrement vrai lorsque nous, le Centre de la sécurité des télécommunications, devons nous en servir, puisque nous voulons assurer à tout prix que la sécurité de nos systèmes n'est pas compromise. Il est donc important de prêter attention à la chaîne d'approvisionnement — comme cela a déjà été dit — et de prêter attention aux entrepreneurs potentiels. Ils doivent encore se soumettre à un processus très rigoureux en matière de sécurité, notamment en ce qui concerne la sécurité de leur personnel, et surtout s'ils doivent travailler pour le Centre de la sécurité des télécommunications et être employés par ce dernier.

Stephanie Kusie: Merci.

Chacun de ces 20 000 véhicules électriques sera examiné afin de détecter la possible présence de logiciels malveillants. Est-ce bien ce qu'il faut comprendre?

Caroline Xavier: Ce n'est pas ce que je dis, monsieur le président. La question posée portait sur le fait de savoir si nous évaluons tout ce qui sera utilisé par le Centre de la sécurité des télécommunications. Ma réponse est oui. Nous veillons à évaluer cela.

J'ajouterais que, en tant que membres de la communauté représentée à cette table, notre travail consiste à donner les meilleurs conseils possibles au gouvernement concernant les systèmes qu'il va utiliser. J'ajouterais également que nous travaillons avec les secteurs des infrastructures essentielles, y compris le secteur des transports, et que ce sont eux qui, je le présume, donneront au gouvernement les meilleurs conseils sur la meilleure façon de déployer les véhicules électriques.

Comme M. Gupta l'a dit, nous avons émis des conseils concernant les appareils connectés, et nous maintenons ces conseils. Nous continuerons à apprendre et à améliorer ces conseils à mesure que nous en saurons davantage. C'est dans cette optique que le projet de loi C-8 est vraiment important, car l'un des secteurs visés est celui des transports. Si ce projet de loi est adopté, nous comprendrons mieux quelles sont les vulnérabilités.

En attendant, nous continuons à travailler et à établir d'excellentes relations avec le secteur des transports, et nous disposons d'organes de gouvernance qui nous permettent de mieux comprendre ce qui s'y passe.

Le président: Merci beaucoup. Le temps imparti est écoulé.

Nous revenons maintenant à Mme Yip.

Vous avez cinq minutes.

Jean Yip: Merci.

Disons simplement que M. Harper n'était pas en négociation avec le président Trump. Le premier ministre Carney est un pragmatique, et il peut voir que notre économie a vraiment besoin d'être diversifiée.

Je reviens maintenant au rapport. J'aimerais poser des questions à M. Jones et à Mme Xavier. Cela concerne le segment où la vérificatrice indique qu'il n'existait pas d'inventaire complet et à jour de l'équipement informatique du gouvernement — comme les ordinateurs portables, les téléphones intelligents et les serveurs — et que, bien que Services partagés Canada se soit attaqué à cela en 2017, le projet n'est pas terminé et devrait se poursuivre au moins jusqu'en 2027. Pourquoi est-ce important et pourquoi cela prend-il autant de temps?

● (1215)

Scott Jones: Je vais commencer. Merci pour cette question.

Comme je l'ai mentionné lors d'une des dernières réponses, je pense qu'il est important de souligner la complexité de l'environnement dans lequel nous évoluons, à savoir le nombre de ministères concernés. Plusieurs entités sont responsables de la gestion de leur propre inventaire. L'autre élément dont il faut tenir compte, c'est que, lorsque Services partagés a été créé, il s'agissait d'un mélange hétéroclite de technologies qui ont été rassemblées et confiées à cette nouvelle agence, avec pour seule consigne le mot d'ordre « débrouillez-vous ».

Au début, l'organisme n'a pas investi dans ses outils, puisqu'il n'y avait pas d'argent pour cela. En réalité, l'argent ne servait qu'à assurer les dépenses de fonctionnement, et nous espérions être en mesure d'y arriver. Nous avons réussi à faire des progrès notables dans des domaines tels que la cyberdéfense, avec nos collègues du Centre de la sécurité des communications. C'est pour cette raison que l'initiative Visibilité, sensibilisation et sécurité à l'égard des terminaux, ou VSST, a été remise sur les rails. Nous avons dû travailler avec le fournisseur. Nous devions nous assurer que les logiciels et les progiciels que nous avions achetés fonctionnaient de façon sécuritaire. La pandémie a retardé le processus d'approvisionnement.

S'ajoute à cela le fait qu'il s'agit d'un domaine où le marché évolue très rapidement. Nous sommes donc passés d'un processus de gestion de projet très statique et à long terme à un processus de livraison de projet très souple permettant de déployer rapidement un produit minimum viable et d'ainsi accélérer le processus. C'est pourquoi nous sommes passés de zéro déploiement à 35 000 ordinateurs de bureau à ce jour. Ce chiffre atteindra les 87 000 d'ici la fin de l'année, ce qui commence à combler le fossé. Cela dit, nous devons travailler avec plus de 100 ministères et organismes. C'est l'un des facteurs qui compliquent la situation.

Le deuxième élément, pour nous, c'est de savoir comment nous pouvons nous assurer que ces ministères ont l'information qu'il leur faut pour voir ce dont disposent leurs utilisateurs. C'est un environnement qui... Il y a très peu d'organisations dans le monde qui fonctionnent comme nous, c'est-à-dire avec tous ces silos verticaux. M. Rochon parlait des autorités, mais nous avons cet organisme horizontal qui s'occupe de l'infrastructure. Il y a par conséquent certaines choses sur lesquelles nous devons travailler avec les fournisseurs. Tous ces problèmes ont maintenant été surmontés.

Sans vouloir banaliser la chose, la tâche consiste à répéter le processus. Il faut cautionner le déploiement, entrer dans le service, faire le déploiement, passer au suivant et déployer de nouveau, et faire tout cela en fonction des priorités afin d'obtenir cette visibilité.

Caroline Xavier: Je ne sais pas si j'ai beaucoup à ajouter à ce que M. Jones a déjà dit.

Nous travaillons main dans la main. En ce qui concerne la recommandation du Bureau du vérificateur général concernant l'identification d'une nouvelle plateforme, nous travaillons en collaboration avec nos collègues du Conseil du Trésor et de Services partagés. Cependant, même sans la plateforme, nous continuerons à fournir au moins un produit minimum viable, comme l'a précisé M. Jones.

M. Rochon a parlé de l'importance de continuer à établir des relations grâce à des exercices sur table. C'est vraiment là que cela compte. En fin de compte, les systèmes dont vous disposez pour assurer le suivi physique de ces éléments importent peu si vous ne faites pas un bon travail pour maintenir ce canal de communication ouvert. Dans le contexte du rapport du Bureau du vérificateur général, c'est précisément ce sur quoi nous avons travaillé. Nous nous sommes donc améliorés et nous en avons tiré des enseignements.

Jean Yip: Quels sont les principaux obstacles qui empêchent votre organisation d'installer des capteurs de défense de cybersécurité sur tous les appareils?

Caroline Xavier: Je ne sais pas si le Conseil du Trésor souhaite répondre à cette question. Il n'y a pas d'obstacles...

Dominic Rochon: Cela renvoie à l'une des questions précédentes, à savoir si les obstacles sont d'ordre juridique ou logistique et financier. M. Jones avait répondu à cela de manière adéquate en disant qu'il y avait un peu des deux.

Il existe un obstacle dans la mesure où nous ne pouvons imposer nos règles qu'aux entités qui relèvent des annexes I et II de la Loi sur la gestion des finances publiques. L'annexe III ne relève pas de notre compétence. Par conséquent, nous ne pouvons pas obliger les sociétés d'État à utiliser les capteurs du Centre de la sécurité des télécommunications ou, en fait, à recourir aux services de Services partagés Canada. Cependant, sur une base volontaire, nous avons contacté toutes ces entités. Nous souhaitons qu'elles adoptent nos pratiques en matière de cybersécurité, car elles sont bien entendu à la fine pointe de ce qui se fait dans le monde. Et du reste, pourquoi ne le feraient-elles pas? Ainsi, petit à petit, nous avons commencé à combler cette lacune. Voilà pour ce qui est de l'aspect juridique de la question.

Sur le plan logistique et financier, comme l'a souligné M. Jones, nous devons comprendre exactement quelle est la présence sur Internet et la présence technologique de certaines de ces organisations et comment elles sont structurées. Si elles veulent ensuite que nous les protégions, que se passera-t-il si un incident survient dans l'une d'entre elles? Cela demande du temps, des efforts et des ressources. Nous devons mettre en place des mécanismes de recouvrement des coûts appropriés pour faire face à ces possibilités.

● (1220)

Le président: Merci beaucoup.

[*Français*]

Monsieur Lemire, vous avez la parole pour deux minutes et demie.

Sébastien Lemire: Merci, monsieur le président.

Madame Xavier, lors du voyage international du premier ministre et de sa délégation en Chine la semaine dernière ou il y a environ 10 jours, on avait demandé aux journalistes de ne pas apporter leur téléphone, mais plutôt de prendre un téléphone temporaire et de le jeter après pour s'assurer qu'il ne soit pas utilisé.

Quand nous, les parlementaires, voyageons, des vérifications de sécurité sont évidemment faites. Souvent, on nous prête un autre appareil pour être sûr que le pays étranger ne puisse pas accéder à nos données et à l'ensemble des informations auxquelles nous avons accès en tant que membres du Parlement.

Durant ce voyage en Chine, un accord a été conclu pour importer des véhicules électriques chinois. Je pourrais prendre mon téléphone du Parlement et me connecter au réseau Bluetooth d'un véhicule électrique chinois. Recommandez-vous de ne pas le faire? Mettrais-je à risque les données stratégiques du Parlement au profit du gouvernement chinois?

Caroline Xavier: Merci de la question.

C'est un peu difficile de répondre de façon concrète, parce que ce sont des hypothèses. Ce que je dirais en général, c'est que, comme mon…

Sébastien Lemire: C'est comme pour l'application TikTok, que le gouvernement nous a demandé d'enlever de nos téléphones. C'est une application que je n'ai jamais utilisée, mais le gouvernement m'a tout de même demandé de l'enlever. On parle aussi des téléphones de la marque Huawei, qui ont été interdits, et des réseaux sans fil. Ce n'est donc vraiment pas hypothétique.

Caroline Xavier: En effet, mais ce que j'allais ajouter, c'est que, pour les exemples que vous avez mentionnés, que ça soit TikTok ou pour une autre application, nous, au Centre canadien pour la cybersécurité, recommandons toujours de prêter attention à toutes les lois sur la vie privée du pays dans lequel les gens voyagent. C'est de ça que nous parlons.

Vous avez mentionné spécifiquement Pékin et la Chine. Cela dit, peu importe où les gens voyagent, nous conseillons de toujours prêter attention aux lois locales. Il faut se demander ce qu'elles sont, si on est à l'aise avec les lois et sur quels réseaux les données vont circuler, parce que nous n'avons pas le contrôle de tous les réseaux de télécommunications qui existent partout dans le monde.

C'est donc une question individuelle qu'un individu doit se poser quand il voyage pour s'assurer qu'il comprend les lois, les problèmes ou les défis qui existent…

Sébastien Lemire: Je vous parle ici, du sentiment qu'on a, comme élu ou citoyen, vis-à-vis des appareils qu'on utilise et qu'on connecte à d'autres sources, par exemple à un véhicule.

J'ai un véhicule électrique américain et un véhicule hybride japonais, donc je me sens moins en danger avec ces deux pays qu'avec la Chine, si j'avais un véhicule électrique chinois.

Sur le plan technologique, est-ce que les pays qui pourraient vouloir posséder mes données à des fins stratégiques peuvent le faire par l'entremise d'un appareil, par exemple, si je me connecte au réseau Bluetooth?

Caroline Xavier: Comme le disait M. Gupta plus tôt, peu importe où on se connecte, on est exposé à un risque. Le nom du pays ne change rien à ça, parce qu'on est dans un monde numérique. Dans ce dernier, sur le plan de la cybersécurité, dès qu'on est connecté à un support de télécommunications, on peut être exposé à un risque.

Cela dit, au Canada, nous travaillons très étroitement avec les compagnies de télécommunications. Nous avons une super relation avec elles, elles travaillent avec nous et elles ont une bonne compréhension des défis, peu importe le cyberacteur. Elles font le nécessaire pour essayer de protéger le plus possible les systèmes, surtout quand on utilise leur réseau.

Sébastien Lemire: J'accorde ma pleine confiance aux compagnies de télécommunications…

Le président: Je suis désolé, monsieur Lemire, mais vous aurez deux autres minutes et demie plus tard. Je vous ai laissé…

Sébastien Lemire: … mais peut-être pas aux intermédiaires.

Le président: Monsieur Lemire, il faut que je vous arrête, désolé. Vous aurez un autre tour de parole dans quelques minutes.

Monsieur Deltell, vous avez la parole pour cinq minutes.

● (1225)

Gérard Deltell: Merci beaucoup, monsieur le président.

Madame Xavier, poursuivons la conversation concernant les voitures.

Je suis un automobiliste et la plupart des gens qui nous écoutent sont automobilistes ou électromobilistes, comme on le dit maintenant. Je suis très heureux et très fier, parce que ça fait deux ans et demi que je roule en véhicule électrique. J'en suis bien content. Soit dit en passant, j'ai acheté une voiture d'occasion, c'est-à-dire à moitié prix, sans subventions et sans obligations.

Parlons maintenant des voitures électriques.

Les préoccupations soulevées par MM. Kuruc et Lemire sont pertinentes. Qu'est-ce qui va se passer? Comme on le sait, maintenant, particulièrement les voitures électriques sont d'abord des ordinateurs qui ont des roues et un moteur et qui avancent. C'est d'ailleurs un peu comme les chasseurs F— 35, qui sont des ordinateurs munis d'ailes et de bombes. D'abord et avant tout, le cœur est l'ordinateur.

Avez-vous déjà eu des menaces de cyberattaques, de non-autorisation ou quoi que ce soit concernant les voitures électriques actuelles qui sont fabriquées au Japon, en Corée du Sud, aux États-Unis ou en Europe? D'ailleurs, soit dit en passant, avant d'aller chercher des voitures en Chine, on pourrait en prendre quelques-unes en France. Elles existent.

Est-ce qu'il y a déjà eu des attaques ou des menaces de cybersécurité en lien avec les voitures électriques ou toutes les voitures, soit dit en passant, parce qu'elles sont toutes munies d'un ordinateur? Y a-t-il déjà eu des menaces d'attaques?

Caroline Xavier: Je ne peux pas faire de commentaire pour vous dire s'il y a eu des menaces spécifiques sur des véhicules électriques. Il est sûr qu'en nous basant sur tous les renseignements que nous avons et toute la recherche que nous faisons, nous savons, comme vous l'avez dit, qu'un véhicule électrique est comme un ordinateur. Nous comprenons les ordinateurs et nous savons qu'ils peuvent être vulnérables. S'ils n'ont pas une certaine quantité de couches de sécurité, leur vulnérabilité augmente.

Nous ne sommes pas un organe de réglementation. Nous allons travailler très étroitement avec Transports Canada et les secteurs qui vont mettre en place ce qui est nécessaire pour s'assurer que les véhicules électriques fonctionnent comme il faut. Nous avons préparé des publications qui parlent en général de la manière de faire attention à toutes les choses connectées et branchées, que ça soit un véhicule électrique ou un ordinateur. Nous sommes des experts en cybersécurité quand ça en vient à comprendre que des menaces vont exploiter les vulnérabilités lorsque la sécurité nécessaire n'est pas en place.

Gérard Deltell: Il y a peu près de 20 ans que les voitures ont un ordinateur. À votre connaissance, est-ce que des automobilistes ont déjà été ciblés par des cyberattaques parce que leur voiture pouvait être suivie à la trace et que des caméras de surveillance pouvaient servir à de l'espionnage? Avez-vous déjà eu connaissance de situations semblables, oui ou non?

Caroline Xavier: Je ne peux pas dire que je suis au courant et répondre à votre question de façon catégorique, c'est-à-dire par oui ou par non, parce que toutes les menaces au Canada ne sont pas automatiquement signalées au Centre canadien pour la cybersécurité. Les gens ne sont pas obligés de nous faire part de tous les incidents. Il est possible qu'un incident relié à un véhicule électrique ait eu lieu, mais ça ne veut pas dire que nous avons reçu l'information liée à cette menace. Puisque nous effectuons des recherches de façon globale et que nous restons en communication avec d'autres partenaires internationaux, nous avons une bonne idée que c'est faisable.

Monsieur Gupta, voudriez-vous ajouter autre chose?

[*Traduction*]

Rajiv Gupta: Je n'ai pas connaissance d'un incident signalé au cybercentre. C'est ainsi que nous évaluerions...

Gérard Deltell: Cela concerne-t-il les voitures?

Rajiv Gupta: Parallèlement, nous avons organisé des ateliers pour comprendre les nouvelles technologies. Tout comme les autres logiciels... Tous les logiciels comportent des vulnérabilités. Comme vous l'avez dit, c'est un ordinateur sur roues. Il y a donc des vulnérabilités.

Nous nous attendons à ce qu'elles soient ciblées. Dès qu'elles le seront, ils trouveront des vulnérabilités et, comme pour les autres logiciels, ils continueront à en trouver. Je dirais que ce n'est qu'une question de temps, et ce, quel que soit le domaine.

Nous continuerons à examiner les technologies utilisées dans les véhicules et à fournir nos conseils et nos recommandations. C'est ce que nous avons fait. Par exemple, nous l'avons fait avec des partenaires de l'industrie lors d'un atelier GeekWeek, simplement pour comprendre quelles sont ces faiblesses et comment formuler des conseils et des recommandations appropriés et veiller à ce que les Canadiens soient conscients de cela.

Nous continuerons à travailler là-dessus, mais il faut s'attendre à ce que les logiciels en couches aient des vulnérabilités et que ces dernières finissent par être exploitées, que ce soit par des cybercriminels, des États ou d'autres acteurs. En gros, comme pour les autres technologies numériques, ces vulnérabilités sont des portes ouvertes.

[*Français*]

Gérard Deltell: Merci beaucoup de ces précisions, monsieur Gupta.

Dans le monde où nous sommes actuellement, une automobile laisse des traces partout. Il y a des caméras partout, alors on est capable d'identifier une personne. On serait même capable de prendre le contrôle, c'est-à-dire qu'une puissance étrangère pourrait prendre le contrôle du véhicule. Cet impact touche tous les Canadiens dans leur vie quotidienne.

Je vous remercie.

● (1230)

Le président: Merci beaucoup, monsieur Deltell.

[*Traduction*]

Nous allons maintenant revenir à M. Osborne.

Vous avez cinq minutes.

Tom Osborne: Merci.

J'aimerais revenir à ma question précédente. J'espérais passer à une autre. J'ai parlé de la nécessité de s'attaquer aux maillons faibles.

À deux reprises, nous avons entendu parler du décret qui touche 44 ministères et de l'annexe III, les organismes étant invités à participer sur une base volontaire. Lorsque nous parlons des maillons faibles dans un domaine aussi important que la cybersécurité et la souveraineté du Canada en matière de défense nationale, je pense que ces enjeux s'inscrivent dans une certaine mesure dans ce contexte.

Quelles recommandations souhaitez-vous formuler à l'intention des membres du comité des comptes publics, pour que nous ne nous contentions plus d'une approche volontaire auprès des organismes et commissions du gouvernement? Il faut espérer qu'ils suivront vos conseils sur une base volontaire et mettront en œuvre les meilleures normes, mais ils ne sont pas tenus de le faire. Avez-vous des conseils à nous donner ou pourrions-nous recommander certaines mesures afin de garantir qu'ils respectent les pratiques exemplaires ou qu'ils soient tenus de les respecter?

Dominic Rochon: Je tiens à préciser que le problème n'est pas nouveau. Je crois qu'il a été signalé par le Comité des parlementaires sur la sécurité nationale et le renseignement il y a environ cinq ans. Nous en avons déjà discuté et nous nous sommes penchés sur la question. Si nous n'avons pas encore trouvé de solution précise pour résoudre ce problème, c'est parce qu'il est complexe, et ce pour plusieurs raisons.

Sur le plan législatif, si vous souhaitez ajouter les entités figurant à l'annexe III de façon à ce qu'elles doivent se conformer à nos politiques, les choses se compliquent pour les agents du Parlement, les sociétés d'État ou les organismes qui ne relèvent pas entièrement du gouvernement fédéral. Il est difficile de les contraindre à se plier à nos politiques. Il y a également des raisons liées à la sécurité nationale. Si nos politiques prévoient des exceptions, c'est pour de très bonnes raisons. C'est pourquoi il est parfois nécessaire de recourir à la voie de la participation volontaire.

L'autre aspect problématique, et je l'ai également mentionné, est le coût associé à ces mesures. Il est possible que certaines très petites entités gèrent leurs systèmes de manière très complexe, voire archaïque, et utilisent peut-être des systèmes anciens. Le fait d'imposer nos capteurs et technologies de cybersécurité aura un coût. Plus particulièrement, si nous activons soudainement nos capteurs au sein d'une petite entité et que nous détectons un grand nombre de problèmes, nous aurons besoin de ressources pour les résoudre. Encore une fois, tous ces éléments ont un coût important et détourneront des ressources déjà affectées aux 100 ministères et organismes que nous examinons déjà avec vigilance. Il nous faudra rediriger une partie de ces ressources vers certaines de ces petites entités pour tenter de combler certaines de ces lacunes.

Nous en discutons depuis plusieurs années déjà et nous essayons de trouver la meilleure solution. Jusqu'à présent, la meilleure solution a été de communiquer avec ces entités, ce que nous avons fait. Nous leur avons écrit. Mes collègues et moi-même... Po Tea-Duncan, en tant que dirigeante principale de la sécurité de l'information, a écrit à ces organismes, en collaboration avec le Centre de la sécurité des télécommunications. Dans certains cas, nous avons trouvé un moyen de déployer nos capteurs et de les installer à l'intérieur de la tente.

Petit à petit, nous essayons de combler ces lacunes, et c'est la meilleure approche que nous ayons trouvée jusqu'à présent.

Caroline Xavier: Pour faire suite à ce que vient de dire M. Rochon, j'ajouterais que nous avons constaté des progrès dans l'adoption des capteurs, en particulier depuis la publication du rapport du Secrétariat du Comité des parlementaires sur la sécurité nationale et le renseignement. Cette conversation pourrait également permettre aux gens de prendre conscience de l'importance de cet enjeu.

Je pense que nous avons tout mis en œuvre auprès de certaines de ces sociétés d'État pour qu'elles comprennent mieux l'importance de cet enjeu. Je dirais que nous encourageons fortement les sociétés d'État à partager leur expérience avec leurs homologues du secteur lorsqu'elles sont confrontées à un incident. Tout à coup, nous recevons également plus d'appels, car les gens commencent à en apprendre davantage et à tirer profit des pratiques des autres.

Tom Osborne: En ce qui concerne la mise en œuvre du système de gestion de l'information de sécurité et des événements dans la stratégie globale de cybersécurité des institutions fédérales, souhaitez-vous atteindre des cibles ou des étapes particulières?

● (1235)

Scott Jones: Nous mesurons plusieurs éléments. Le premier est la rentabilité. Je sais bien que dans ce domaine, on pourrait dire « vous devez dépenser tout l'argent nécessaire pour vous protéger », mais nous devons respecter un budget et utiliser chaque dollar de la manière la plus efficace possible. Nous examinons constamment cet aspect afin de nous améliorer.

Nous pouvons notamment tirer parti de notre position pour négocier de meilleurs prix grâce au volume d'achats du gouvernement du Canada. Dans certains de ces cas dont nous avons discuté, les volumes nous ont permis de réduire considérablement les coûts. Il revient beaucoup moins cher d'acheter 500 000 unités d'un produit que d'acheter une seule unité de chaque type de produit. La rentabilité est l'un des enjeux.

L'autre aspect est le maintien d'une intégration étroite avec le Centre de la sécurité des télécommunications Canada. Si je déploie quelque chose sur le marché, je veux que cela libère du temps d'analyse pour le Centre de la sécurité des télécommunications Canada, de sorte qu'il puisse se concentrer sur l'évolution de la menace. En parallèle, nous devons veiller à optimiser l'automatisation. C'est pourquoi nous évaluons le niveau d'automatisation atteint et les outils nécessaires pour accroître la productivité.

Nous ne disposons pas d'un centre d'opérations de sécurité illimité pour gérer ces éléments. En ce qui concerne l'automatisation et l'intégration, nous attendons donc de nos fournisseurs qu'ils remplissent ces obligations dans le cadre de leur contrat. Il s'agit là de tous les éléments que nous examinons pour nos mesures.

Le président: Merci.

Je crains que votre temps soit écoulé, monsieur Osborne, mais nous reviendrons vers vous plus tard.

Monsieur Rochon, permettez-moi de clarifier quelque chose: lorsque vous parlez d'entités, faites-vous principalement référence aux sociétés d'État?

Dominic Rochon: Oui, l'annexe III concerne principalement les sociétés d'État.

Le président: J'aimerais poser une question précise à ce sujet.

Souhaiteriez-vous que l'on renforce les exigences imposées aux sociétés d'État afin qu'elles suivent les directives de votre groupe?

Dominic Rochon: Personnellement, je pense que ce serait une bonne chose, oui.

Le président: Merci.

Je vais laisser les autres députés intervenir s'ils le souhaitent. Nous allons commencer notre quatrième et dernier tour. Je vais raccourcir le temps prévu afin que nous ne dépassions pas trop l'horaire. Les analystes auront peut-être quelques questions à poser à la fin. Les membres du gouvernement et de l'opposition disposeront de quatre minutes chacun.

[*Français*]

M. Lemire disposera de deux minutes.

[*Traduction*]

Monsieur Kuruc, vous allez commencer. Allez-y pour quatre minutes.

Ned Kuruc: Merci.

J'aimerais revenir sur certaines questions que j'ai posées tout à l'heure, mais je vais d'abord aborder quelques points. Ce groupe a appris que l'ancien premier ministre Stephen Harper avait négocié avec la Chine au sujet du canola. Pour ce qui est du Canola, je comprends. L'ancien premier ministre Harper n'avait pas à faire face aux cybermenaces liées à l'intelligence artificielle que nous connaissons aujourd'hui, et nous ne parlions pas de l'arrivée de 50 000 voitures électriques dans notre pays. J'aimerais revenir sur ce point. La question des véhicules électriques est un tout autre sujet.

Aujourd'hui, nous parlons de cybersécurité, et nous allons nous en tenir à ce sujet. J'ai ici un extrait de l'Évaluation des cybermenaces nationales 2025-2026. On peut y lire ceci:

> La République populaire de Chine mène des cyberopérations contre les intérêts canadiens pour servir de grands objectifs politiques et industriels, dont l'espionnage, le vol de propriété intellectuelle, l'influence malveillante et la répression transnationale. Parmi nos adversaires, la portée, la capacité et la visée du programme de cyberactivité de la RPC dans le cyberespace sont inégalées.

Je trouve préoccupant que nous posions des questions pertinentes qui intéressent les Canadiens, et que les représentants du gouvernement de l'autre côté ne le fassent pas. Il s'agit d'une menace réelle. Au bout du compte, si le premier ministre ne s'était pas présenté sur la scène internationale pour annoncer au monde entier qu'il allait travailler main dans la main avec le Parti communiste chinois, nous ne nous poserions pas ces questions aujourd'hui.

Sur ce point, j'ai une question directe à poser à la cheffe du Centre de la sécurité des télécommunications. Le Canada est-il prêt à adopter une approche ouverte à l'égard du Parti communiste chinois en matière de cybersécurité, ou devons-nous adopter une approche plus stricte ou plus robuste... ou passer à un niveau supérieur pour assurer la sécurité du Canada?

Caroline Xavier: Ce que j'aurais dit, même avant la conversation d'aujourd'hui, c'est que le Canada n'est pas à l'abri des menaces provenant d'acteurs étatiques hostiles, de cybercriminels et de cybermilitants. C'est ce qu'indique notre Évaluation des cybermenaces nationales...

Ned Kuruc: Je suis d'accord avec vous, mais compte tenu du fait que le premier ministre s'est exprimé sur la scène internationale et a pratiquement indiqué que le Parti communiste chinois était la voie à suivre, les choses ont changé. Je ne parle qu'au nom des personnes qui ont appelé mon bureau. Cette situation est préoccupante. De nombreux cas ont été signalés.

L'ancien gouvernement libéral lui-même a déclaré que nous ne pouvions pas utiliser les téléphones Huawei, etc. Le problème a été mis en évidence. Vous avez vous-même désigné la Chine comme l'un des nombreux pays concernés. Nous devrions assurément faire preuve d'une vigilance accrue compte tenu de la direction que nous prenons. Je ne demande pas de réponses concrètes. Je sais que ces événements se sont produits il y a seulement une semaine ou deux, mais vous devez réfléchir à la manière de garantir la sécurité du Canada. C'est pourquoi j'ai posé cette question.

Il s'agit là d'une voie claire pour faire des affaires avec le Parti communiste chinois, non seulement dans le domaine du canola — et peut-être que la Chine achètera notre gaz naturel liquéfié, ce que nous pouvons tous comprendre —, mais les produits chinois ou ceux du Parti communiste chinois que nous allons importer présentent de graves risques pour la cybersécurité. Les choses changent. Vous êtes l'experte. Je le reconnais, et je vous remercie, mais les appels que je reçois... Les choses ont changé depuis deux semaines.

Sommes-nous prêts à nous attaquer à ce problème? Quelles mesures allons-nous prendre pour mieux y faire face?

● (1240)

Caroline Xavier: Je pense qu'en tant qu'institution, gouvernement et pays, nous devons toujours être prêts, car les menaces auxquelles nous sommes confrontés surgissent et évoluent constamment. Une partie du travail du Centre de la sécurité des télécommunications consiste à faire face à ces menaces. Nous analysons ces renseignements et nous les exploitons au regard de ce que nous apprenons dans le domaine du renseignement étranger, ainsi que dans celui de la cyberdéfense. Le travail que j'effectue avec mes collègues du Conseil du Trésor et de Services partagés est essentiel pour garantir que les systèmes du gouvernement du Canada restent prêts à se défendre contre toute menace.

Les menaces évoluent, c'est un fait. Les faits montrent que les acteurs malveillants changent quotidiennement de stratégie et utilisent l'intelligence artificielle pour atteindre leurs objectifs. Nous le constatons aussi bien chez les cybercriminels que chez les acteurs étatiques.

Je suis fière de participer à la défense du Canada, de faire partie du portefeuille de la défense et de relever du ministre de la Défense. Dans le cadre du travail que nous accomplissons à partir de cette position et grâce aux investissements qui nous ont été accordés, nous allons évidemment poursuivre la modernisation des systèmes informatiques et continuer d'assurer la protection de nos données. Nous allons continuer de mettre en œuvre des mécanismes d'assurance de l'information et des technologies de cryptage afin de garantir la protection de toutes les données que nous hébergeons.

Le président: Merci beaucoup. Je crains que votre temps soit écoulé.

Nous allons nous tourner à nouveau vers Mme Tesser Derksen. Vous avez quatre minutes.

Kristina Tesser Derksen: Merci beaucoup, monsieur le président.

Cette conversation est très intéressante. C'est formidable.

Je tiens à souligner qu'aucun d'entre nous ne sous-estime les risques liés à la sécurité auxquels notre pays est confronté. Tous les pays sont concernés par cette évolution technologique. J'aimerais revenir sur une préoccupation que ma collègue, Mme Kusie, a soulevée au sujet de l'utilisation que j'ai faite du mot « anodines ». Je faisais référence au fait que lorsque j'ai consulté la définition du terme « événement de cybersécurité », j'ai constaté que celle-ci stipulait que « les événements ne correspondent pas nécessairement à une atteinte à la sécurité ». Il pourrait par exemple s'agir d'un utilisateur, comme moi, qui « se connecte à un système à une heure inhabituelle ».

Nous devons bien sûr envisager tous les événements comme des attaques potentielles, je le comprends, mais au final, un grand nombre d'entre eux sont anodins. Je suis heureuse que vous soyez hypervigilants, même face à ces événements anodins, et que vous veilliez à ce que nous soyons bien protégés. Je vous en remercie.

J'aimerais poursuivre dans la même veine. J'allais parler des sociétés d'État qui ne se servent pas des outils mis à leur disposition.

J'aimerais poser une question aux témoins du Bureau du vérificateur général. Comme je l'ai dit, certaines de ces sociétés d'État ont estimé que l'utilisation de ce système compromettrait leur intégrité et leur indépendance. Je décrirais cette attitude comme un état d'esprit, et j'aimerais demander au Bureau du vérificateur général s'il estime que ce type d'état d'esprit nuit, faute d'un meilleur terme, à notre capacité de nous protéger adéquatement dans le contexte de la cybersécurité.

Andrew Hayes: La meilleure réponse que je puisse donner à cette question est que, pour ce qui est de l'indépendance, très peu d'organismes sont aussi indépendants que le Bureau du vérificateur général, et nous utilisons ces outils.

En ce qui concerne les sociétés d'État, je suis tout à fait d'accord avec mes collègues en ce qui concerne la structure législative. Je tiens à souligner que la Loi sur la gestion des finances publiques prévoit d'autres options. Par exemple, la partie X de la Loi sur la gestion des finances publiques confère aux ministres le pouvoir de diriger les sociétés d'État. Il existe donc peut-être d'autres moyens d'atteindre cet objectif, mais les facteurs qui ont été avancés pour expliquer pourquoi d'autres organismes pourraient ne pas être disposés à agir sont valables. Nous devons les surmonter. Prenons un autre exemple: si vous faites appel à un prestataire externe pour vos services informatiques, il peut s'avérer coûteux de lui demander de collaborer avec des organismes gouvernementaux sur ce type de questions. Je pense que ce sont là des problèmes que le gouvernement doit résoudre.

Pour répondre à votre question sur l'état d'esprit, je pense que tous les Canadiens s'attendent à ce que le gouvernement fasse tout ce qui est en son pouvoir. Les organismes gouvernementaux feront tout leur possible pour protéger les informations et maintenir les services.

Kristina Tesser Derksen: D'accord. J'aime vos suggestions parce que — corrigez-moi si je me trompe — je n'ai pas vu de recommandations dans le rapport sur la manière dont nous pourrions inciter ces sociétés d'État à adopter ces outils.

● (1245)

Andrew Hayes: Nous n'avons pas formulé de recommandations directement dans le rapport, parce qu'il s'agit d'une question de politiques. Cependant, je pense que nous parlons en ce moment du fait qu'il est important que les organismes gouvernementaux voient clairement les menaces qui pèsent sur eux.

Mes collègues pourraient peut-être vous en dire davantage à ce sujet, mais le fait est que plus les organismes voient clairement ce qui se passe aux points d'extrémité et sur les réseaux de tous les organismes, mieux ils sont équipés pour venir en aide à tout le monde.

Kristina Tesser Derksen: D'accord. C'est excellent.

Je m'adresse de nouveau à l'équipe de la vérificatrice générale. J'ai remarqué dans le préambule de votre rapport que vous indiquez qu'« aucun financement n'[a] été accordé à une initiative visant à établir une plateforme de collaboration pour la cybersécurité et un outil de gestion des incidents ». Pouvez-vous nous en dire davantage à ce sujet?

Andrew Hayes: Je vais peut-être devoir demander à l'un de mes collègues de s'étendre un peu plus sur le sujet, mais je crois que la difficulté que l'organisation rencontrait, lorsque nous avons fourni ce rapport, c'était la nécessité de trouver du financement, ce qui n'avait pas encore été fait. Cela fait toutefois un certain temps que nous avons terminé notre rapport.

Scott Jones: Cela s'inscrivait dans le cadre de la progression du processus d'approvisionnement que j'ai mentionné précédemment. Nous sommes en train de finaliser le contrat pour le Système de gestion des événements et des incidents de sécurité, ou SGEIS. L'approvisionnement peut toujours être imprévisible et présenter des défis, mais il en est actuellement à l'étape finale, et nous sommes prêts à aller de l'avant. Les questions soulevées dans le rapport ont été gérées.

Du côté de la Visibilité, sensibilisation et sécurité de point d'extrémité, la question a été réglée, et nous en sommes maintenant à des dizaines de milliers de déploiements.

Le président: Je vous remercie. Je crains que votre temps de parole soit écoulé.

[*Français*]

Monsieur Lemire, vous avez la parole pour deux minutes.

Sébastien Lemire: Merci, monsieur le président.

Le ministre de l'Intelligence artificielle et de l'Innovation numérique, M. Solomon, a présenté un nouveau cadre sur la souveraineté numérique. Au sujet des défis et des risques, celui-ci parle des dangers liés au fait que toutes nos données soient hébergées dans d'autres pays, notamment aux États-Unis, pays où il y a des lois qui permettent aux autorités de demander l'accès aux informations détenues par des organisations à l'intérieur de leurs frontières. Il aborde également la question de la dépendance à l'égard de grandes sociétés technologiques ou d'entreprises de gestion de données.

Évidemment, ici, nous avons accès à de l'énergie renouvelable abordable et à des lieux permettant d'héberger de nombreux serveurs, mais la stratégie canadienne, visiblement, vise à nous rendre dépendants. Ça touche même nos ordinateurs. J'ai à changer le mien cette semaine, et on me dit que toutes les données seront envoyées dans le nuage.

M. Jones est peut-être le mieux placé pour répondre à ma question. En quoi la nouvelle stratégie aura-t-elle une incidence sur les choix qui seront faits par les différents ministères? On dit que le premier ministre a été tellement habile en ne nommant pas le président Trump et les États-Unis dans son fameux discours à Davos, mais on se rend hyper vulnérables à des représailles de la part des Américains. Je n'ai pas peur qu'un tank se rende à Rouyn-Noranda, mais je peux certainement avoir peur que le président Trump ordonne à Microsoft de mettre en pause tous les appareils de données qui sont reliés à Microsoft au Canada. Ça paralyserait l'ensemble de nos travaux.

Avez-vous réfléchi à ces répercussions?

Scott Jones: Oui, absolument. Nous y avons réfléchi pendant des années. Pendant les processus d'approvisionnement, nous ajoutons des clauses de sécurité, et il y a également un processus d'évaluation de sécurité, qui est fourni par le Centre de la sécurité des télécommunications, pour vérifier la protection des informations et accorder un niveau de qualification aux fournisseurs de services infonuagiques.

De plus, nous avons ajouté d'autres niveaux de sécurité, par exemple le chiffrement des courriels et d'autres communications, pour protéger l'information vraiment sensible. Nous gardons aussi les clés pour effacer ce qui est envoyé vers de grands fournisseurs dans n'importe quel pays. C'est une autre couche de protection, et c'est aussi efficace contre les cybermenaces.

Finalement, il est important d'établir un équilibre entre les capacités d'un système et les besoins du gouvernement et des utilisateurs des technologies, parce que la seule chose qui puisse être absolument sécurisée, c'est un ordinateur éteint. Ça, ça ne marche pas. Alors, on doit toujours mesurer les risques auxquels nous devons faire face.

Mes collègues veulent peut-être ajouter quelque chose.

● (1250)

Le président: Merci beaucoup.

[*Traduction*]

La prochaine intervenante est Mme Kusie, qui prendra la parole pendant quatre minutes.

Stephanie Kusie: Merci, monsieur le président.

En décembre 2022, il a été révélé que la GRC avait adjugé un contrat d'achat de matériel de radiofréquence à Sinclair Technologies, une société détenue par Hytera Communications. Hytera est une entreprise chinoise de télécommunications appartenant en partie au gouvernement chinois. Elle a été inscrite sur la liste noire de la Commission fédérale des communications des États-Unis en 2021 en tant que « risque inacceptable pour la sécurité nationale ». Le ministère de la Sécurité publique a confirmé que la GRC n'a pas demandé au CST de procéder à une évaluation des risques avant d'adjuger ce contrat.

Quelqu'un peut-il préciser si le Cabinet a indiqué aux ministères fédéraux qu'ils devaient consulter le CST avant de conclure des contrats d'achat avec des fournisseurs étrangers pour des produits utilisés par nos organismes de sécurité?

Dominic Rochon: Je vais peut-être donner mon avis à cet égard.

En raison de certaines de mes fonctions antérieures au sein du ministère de la Sécurité publique, je sais que cette question relève de la Loi sur Investissement Canada. Ce n'est pas nécessairement une question dont nous discutons dans le contexte de la protection des systèmes du gouvernement du Canada et de la cybersécurité de nos systèmes. Je crois qu'il faut plutôt faire la distinction entre les nombreuses questions qui nous ont été posées aujourd'hui. J'ai mentionné qu'il s'agissait d'un travail d'équipe, mais l'un des membres de notre équipe n'est pas présent aujourd'hui. Il s'agit du ministère de la Sécurité publique. Ce ministère est largement responsable de la cybersécurité orientée vers l'extérieur. L'équipe que vous voyez ici aujourd'hui est celle qui est chargée de sécuriser les systèmes du gouvernement fédéral.

Comme Mme Xavier l'a mentionné plus tôt, le projet de loi C-8 préconise la mise en place et l'application de mesures de cyberhygiène particulière dans quatre secteurs d'infrastructures essentielles, à savoir les transports, les finances, les télécommunications et l'énergie. Si le projet de loi est adopté, je pense que bon nombre des questions qui nous ont été posées aujourd'hui recevront des réponses claires, car des organismes de réglementation seront mis en place pour imposer des mesures de cyberhygiène dans ces industries du secteur privé.

Je m'excuse si je n'ai pas répondu précisément à votre question, mais je tenais à souligner qu'il faut faire la distinction entre ce qui se passe dans la société en général ici, au Canada, et la cybersécurité de ce milieu, qui relève de la Sécurité publique, et la protection des systèmes. Il existe évidemment des liens entre les deux, mais je tenais simplement à souligner ces distinctions.

Stephanie Kusie: Monsieur Jones, en avril 2017, il y a près de neuf ans, votre organisation a commencé à développer une application de gestion des événements et des incidents de sécurité qui devait être achevée en mars 2023. Le budget initial pour le développement de cette application s'élevait à 72,7 millions de dollars. Cependant, ce budget a été doublé en 2021 pour s'établir à plus de 144 millions de dollars. De plus, la vérificatrice générale a constaté que le produit avait été mis en veilleuse en juin 2024 dans l'attente de l'approbation d'un financement supplémentaire.

Quel est l'état d'avancement de cette application aujourd'hui? Combien de millions de dollars SPC a-t-il investis dans ce projet? De plus, le budget initial de ce projet a été largement sous-estimé. Quelle en est la raison?

Merci.

Scott Jones: Je vous remercie de votre question. Il y a plusieurs éléments à prendre en compte à cet égard. Il s'agit du projet dont je parlais. L'adjudication du contrat est prévue dans les prochains mois, et ces mois seront peu nombreux.

Deuxièmement, il s'agissait d'un domaine où la technologie évoluait très rapidement en raison de la cybersécurité. Le processus était conçu pour un processus standard d'approvisionnement de l'administration fédérale comportant des spécifications complexes, une adjudication de contrat, une livraison de produits échelonnée sur plusieurs années, puis une livraison finale. Ce type de processus ne fonctionne pas dans un environnement agile où la technologie évolue. Cette approche a été remplacée par un processus de livraison de projet beaucoup plus agile, où l'on se concentre sur des produits livrables plus petits qui se développent au fil du temps.

Troisièmement, certaines exigences ont fait grimper les coûts. Le principal facteur à l'origine de cette augmentation était l'obligation de conserver les données pendant une période beaucoup plus longue que nécessaire pour les évaluations cybernétiques essentielles. C'est un aspect auquel nous avons travaillé en collaboration avec nos collègues du CST pour déterminer ce qui est raisonnable et nécessaire. Parfois, ce qui se passe, c'est que... Les spécifications étaient trop nombreuses. C'est une façon simple de présenter les choses. Les spécifications ont été revues à la baisse afin de les remettre dans leur contexte.

Les fonds dépensés ont uniquement servi à financer les processus d'approvisionnement, car nous avons relancé ce projet afin d'éviter d'investir dans quelque chose qui était trop rigide et dont nous n'avions pas besoin, mais aussi pour disposer d'un système conforme à l'environnement cybernétique actuel, et non à celui de 2017. C'était le principal défi à relever pour relancer ce processus d'approvisionnement et le mettre en œuvre. Il est maintenant de nouveau sur la bonne voie, mais il est important de noter que, dans l'intervalle, le gouvernement du Canada a continué de disposer d'un système de gestion des événements et des incidents de sécurité. Ce système était en place avant la création du Centre canadien pour la cybersécurité, et nous continuons de le financer.

● (1255)

Le président: Je vous remercie.

C'est tout le temps dont Mme Kusie disposait.

Madame Yip, je crois comprendre que vous allez partager votre temps de parole. Je vais vous permettre de céder la parole à votre collègue en temps voulu, ou souhaitez-vous que je vous interrompe?

Jean Yip: Je vais lui céder la parole.

Le président: Fort bien. La parole est à vous pendant quatre minutes. Ensuite, j'aurai quelques questions à poser vers la fin de la séance.

Jean Yip: D'accord. Merci.

Comment la publication des lignes directrices sur la gestion des vulnérabilités contribuera-t-elle à résoudre les problèmes mentionnés dans le rapport?

Po Tea-Duncan: La gestion des vulnérabilités est un aspect important. En vertu de la politique sur la sécurité du gouvernement et de la politique sur les services et le numérique, les ministères sont tenus de rendre des comptes et sont responsables de la mise en œuvre des règles que nous établissons. Pour les aider à respecter ces exigences, le SCT offre des lignes directrices sur la gestion des vulnérabilités qui les aideront à gérer leur propre système ministériel et à distinguer et atténuer leurs vulnérabilités actuelles. Des outils tels que la Visibilité, sensibilisation et sécurité de point d'extrémité les aideront à distinguer certains de ces systèmes qui présentent des vulnérabilités. Une fois les données obtenues, vous serez en mesure de déterminer et de mettre en place les mesures de contrôle qui s'imposent, notamment en corrigeant et en comblant ces vulnérabilités et lacunes.

Cela fait partie du programme global de gestion des vulnérabilités du gouvernement du Canada, qui est mis en place dans le cadre du financement accordé au SCT dans le budget de 2024. Nous continuons de travailler avec nos collègues du Centre canadien pour la cybersécurité, ainsi qu'avec Services partagés Canada, afin d'aider les ministères à établir les priorités qui conviennent quant aux vulnérabilités qui doivent être corrigées au sein de notre écosystème.

Jean Yip: J'ai simplement une brève question à vous poser.

La nouvelle équipe violette — et cette question est destinée à M. Jones ou Rochon — aurait-elle les capacités et les ressources nécessaires pour faire face à une cyberattaque de grande ampleur et, surtout, serait-elle en mesure de réagir rapidement?

Po Tea-Duncan: L'équipe violette adopte une approche préventive en matière de mise à l'épreuve des mesures de contrôle que nous avons mis en place. Il s'agit là de mesures préventives.

En ce qui concerne les cyberattaques de grande ampleur, c'est ce qui a déjà été mis en place de concert avec les équipes du Conseil du Trésor, ainsi qu'avec le centre pour la cybernétique, qui est responsable de la réponse immédiate au sein du gouvernement du Canada, en collaboration avec Services partagés Canada, ainsi que les ministères et organismes qui jouent également un rôle dans la gestion des incidents et dans la réponse aux incidents qui touchent leurs systèmes.

Jean Yip: Merci.

Je vais maintenant céder la parole à M. Osborne.

Le président: C'était parfait, madame Yip.

Monsieur Osborne, vous disposez de deux minutes.

Tom Osborne: Merci.

Le Comité rédigera sans aucun doute un rapport et formulera peut-être des recommandations. Je sais que le Bureau du vérificateur général a déclaré que nous pouvions utiliser la partie X et demander que les ministres donnent des directives à cet égard. Tous les ministres, tous les ministères et tous les organismes ne l'ont toujours pas fait de façon uniforme. Même si, dans la plupart des cas, il peut s'agir d'une exception, lorsque nous formulons des recommandations, devrions-nous recommander des lignes directrices plus strictes en matière de cybersécurité, étant donné que nous nous penchons sur la sécurité nationale et la sécurité de nos systèmes d'information?

Dans le prolongement de cette question, si nous autorisons les organismes gouvernementaux à passer des contrats pour des services informatiques par l'intermédiaire d'agences, dont certaines peuvent même faire appel à des sous-traitants, quelles mesures devrions-nous envisager de mettre en œuvre, à titre de recommandations, afin de garantir que ces partenaires sont fiables?

Le président: Monsieur Osborne, ils pourraient déclarer que c'est à vous de le savoir...

Des voix: Oh, oh!

Le président ..., mais je vais entendre les réponses à cette question. Veuillez donc poursuivre.

Tom Osborne: Je veux connaître leurs avis à ce sujet.

Le président: Oui.

Vos opinions nous seraient utiles.

Rajiv Gupta: Je peux commencer.

En ce qui concerne les risques liés aux tiers, il est très important de les éliminer. Nous avons publié des lignes directrices en matière d'approvisionnement, afin que la cybersécurité soit intégrée dans ces approvisionnements, des lignes directrices que nous leur recommandons de suivre et qui permettent à tous de conclure des contrats. Nous les avons publiées à l'intention du gouvernement, mais aussi pour aider le Canada. Nous travaillons en étroite collaboration avec le Conseil du Trésor et Services partagés Canada afin de nous assurer qu'elles sont suivies dans le cadre de la négociation de tous nos contrats, mais nous les recommandons à tous les ordres de gouvernement et à tous les services d'approvisionnement.

Dominic Rochon: Oui, la difficulté... Je veux dire, nous parlons sans cesse des sociétés d'État, mais il y a aussi des entités parlementaires, des entités judiciaires et des organisations à gouvernance partagée. Le paysage de certaines de ces petites organisations est complexe.

Comme je l'ai indiqué précédemment, je suis personnellement favorable à un renforcement de nos pouvoirs afin que nous puissions imposer certaines des mesures d'hygiène informatique que nous imposons effectivement aux principaux ministères et organismes de l'administration publique, mais je suis conscient du fait que d'autres facteurs entrent en jeu. Nous avons essayé de résoudre ce problème en nous concentrant sur les lacunes. En nous portant à la rencontre de ces organisations, j'ai l'impression que nous avons commencé à mieux comprendre la situation et certains des défis à relever, mais j'accueillerais favorablement un rapport émanant de votre comité qui suggérerait peut-être que des pouvoirs supplémentaires nous soient conférés pour que nous puissions veiller à combler ces lacunes une fois pour toutes.

● (1300)

Le président: Je vous remercie. Le temps qui vous était imparti est écoulé.

Avant de vous laisser partir et de clore cette réunion, j'aimerais vous soumettre deux questions posées par nos analystes, auxquelles nous attendons une réponse de la part des autorités compétentes.

Premièrement, où en est l'approvisionnement du projet Visibilité, Sensibilisation et Sécurité de point d'extrémité?

Deuxièmement, le gouvernement a-t-il établi l'inventaire des actifs fédéraux liés à toutes les applications et à tous les systèmes?

Scott Jones: Je vais peut-être répondre à la première question, et ensuite, mes collègues du Conseil du Trésor pourront répondre à la deuxième.

En ce qui concerne le projet de visibilité des vulnérabilités des entreprises, le contrat a été signé, et nous en sommes maintenant à l'étape du déploiement. À ce jour, 37 000 déploiements ont été effectués, et ce chiffre va augmenter considérablement d'ici la fin de l'année civile — je n'ai toutefois pas le chiffre exact sous les yeux, et je ne voudrais pas vous citer un chiffre erroné. Par la suite, ces déploiements continueront de s'accélérer au cours du prochain exercice financier.

Dominic Rochon: Malheureusement, la réponse à la deuxième question est que nous ne disposons pas des fonds nécessaires pour donner suite à l'activité mentionnée dans cette deuxième question.

Le président: Je vous remercie.

Monsieur Jones, pourriez-vous nous communiquer le chiffre que vous ne souhaitiez pas citer? Si vous pouviez le faire parvenir au Comité dans les deux prochaines semaines, ce serait formidable. Merci beaucoup.

Monsieur Hayes, avez-vous une dernière observation à formuler? D'accord, je viens d'apercevoir votre geste... Je ne voudrais jamais être un encanteur, car le moindre geste peut déclencher une enchère.

Nous remercions nos témoins de leurs témoignages et de leur participation à l'étude du rapport intitulé « La cybersécurité des réseaux et des systèmes du gouvernement » qui fait partie des rapports de l'automne 2025 de la vérificatrice générale. Merci encore.

Nous avons légèrement dépassé le temps prévu pour la séance, alors je vais être très bref.

À l'issue de la réunion, je souhaite m'entretenir avec les membres du Sous-comité, c'est-à-dire Mme Yip, M. Lemire et Mme Kusie.

La séance est levée. Merci.