CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

43e LÉGISLATURE, 2e SESSION

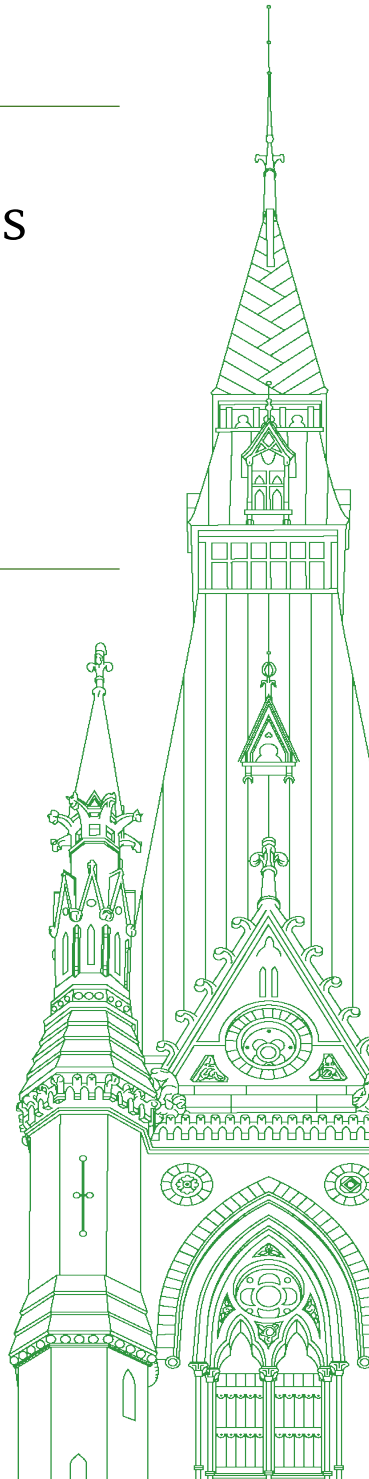
# Comité permanent des opérations gouvernementales et des prévisions budgétaires

TÉMOIGNAGES

**NUMÉRO 033**

**PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY**

Le lundi 31 mai 2021



Président : M. Robert Kitchen

# Comité permanent des opérations gouvernementales et des prévisions budgétaires

**Le lundi 31 mai 2021**

● (1535)

[*Traduction*]

**Le président (M. Robert Kitchen (Souris—Moose Mountain, PCC)):** La séance est ouverte.

Soyez les bienvenus à la 33e réunion du Comité permanent des opérations gouvernementales et des prévisions budgétaires de la Chambre des communes. Le Comité se réunit aujourd'hui de 15 h 36 à 17 h 36 pour entendre des témoins dans le cadre de son étude sur les mesures prises par le gouvernement en réponse à la pandémie de COVID-19. Nous passerons ensuite à huis clos pour discuter des travaux du Comité et examiner notre rapport sur le contrat d'équipement de sécurité offert à Nuctech.

Je profite de l'occasion pour rappeler à tous les participants qu'il est interdit de faire des captures d'écran ou de prendre des photos de son écran. Je vous rappelle aussi quelques règles à suivre pour le bon déroulement de la séance. L'interprétation de cette vidéoconférence fonctionnera pour ainsi dire comme à l'habitude. Vous avez le choix au bas de votre écran entre l'anglais et le français. Avant de prendre la parole, veuillez attendre que je vous nomme. Quand vous êtes prêts à parler, cliquez sur l'icône du microphone pour rétablir le son. Veuillez mettre votre micro en sourdine lorsque vous ne parlez pas. Pour faire un rappel au Règlement pendant la réunion, vous devez activer votre micro et dire « J'invoque le Règlement » afin d'attirer l'attention du président.

Le greffier et les analystes participent virtuellement à la séance d'aujourd'hui. Si vous avez besoin de leur parler pendant la réunion, veuillez leur envoyer un message électronique à l'adresse courriel du Comité. Vous pouvez également communiquer avec notre greffier via son téléphone cellulaire.

Pour les personnes qui se trouvent dans la salle de comité, veuillez noter que les masques sont obligatoires si vous n'êtes pas assis ou si la distanciation physique n'est pas possible.

Je vais maintenant inviter nos témoins à nous présenter leurs observations préliminaires.

Le premier à le faire sera M. Scott Jones du Centre de la sécurité des télécommunications.

**M. Scott Jones (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications):** Bonjour, monsieur le président et mesdames et messieurs les membres du Comité.

Je m'appelle Scott Jones et je suis le dirigeant principal du Centre canadien pour la cybersécurité qui relève du Centre de la sécurité des télécommunications (CST).

Sous la responsabilité du ministre de la Défense nationale, le CST est l'un des principaux organismes de sécurité et de renseignement du Canada. Il a pour mandat de fournir du renseignement étranger à l'appui des nombreuses priorités du gouvernement. Le CST est aussi la principale autorité technique du pays en matière de cybersécurité. Le Centre canadien pour la cybersécurité est un secteur au sein du CST. Notre rôle national consiste à assurer la protection du gouvernement du Canada, à diffuser nos pratiques exemplaires pour prévenir les compromissions, à assurer la gestion et la coordination des incidents d'importance et à contribuer à la sécurisation du Canada numérique.

J'ai pris la parole devant votre comité en mai dernier, soit au début de la pandémie de COVID-19, et j'aimerais profiter de l'occasion qui m'est offerte aujourd'hui pour faire le point sur l'évolution de l'environnement de cybermenaces et le travail que nous avons accompli depuis pour protéger le gouvernement du Canada, le secteur de la santé, les infrastructures essentielles de notre pays et les Canadiens contre tous les types de menaces.

La pandémie a créé un environnement incertain qui est vulnérable à l'exploitation. Le CST continue de miser sur tous les aspects de son mandat pour protéger le Canada contre les cybermenaces et éclairer les décisions du gouvernement canadien. Le CST et le Centre pour la cybersécurité travaillent de concert avec des partenaires du secteur de la cybersécurité pour protéger les Canadiens des méfaits causés par les auteurs de cybermenaces et les sites Web frauduleux.

Depuis mars 2020, le Centre pour la cybersécurité a aidé à éliminer plus de 8 000 adresses courriel et sites Web frauduleux, y compris des sites qui se faisaient passer pour des entités du gouvernement du Canada ou des portails de prise de rendez-vous de vaccination. Bien que ce travail important ait essentiellement mis l'accent sur la fraude liée à la COVID-19, nous continuons chaque jour de détecter et de supprimer de nouveaux domaines frauduleux cherchant à se faire passer pour un site du gouvernement du Canada ou d'une organisation participant aux efforts déployés pour la lutte contre la COVID-19.

Le Centre pour la cybersécurité estime que la COVID-19 pose un risque élevé pour la cybersécurité des organismes de santé canadiens qui prennent part aux activités nationales d'intervention contre la pandémie. Tout au long de la pandémie, le CST et le Centre pour la cybersécurité ont poursuivi leurs efforts en vue de sensibiliser le public aux cybermenaces qui pèsent sur les organismes de santé canadiens. Pour ce faire, ils ont adopté une approche préventive qui consiste à publier des alertes sur les menaces et à prodiguer des conseils et des consignes sur mesure à toutes les autorités de santé régionales des gouvernements provinciaux et territoriaux; aux associations et aux centres d'excellence financés par le gouvernement fédéral; aux établissements de soins; aux entreprises biopharmaceutiques et aux organismes de recherche; aux fabricants de dispositifs médicaux; et aux établissements de recherche universitaire.

Depuis le début de la pandémie, le Centre pour la cybersécurité a organisé 40 appels avec les intervenants du secteur de la santé afin de leur fournir des mises à jour régulières et adaptées concernant l'évolution du paysage de la cybermenace. Il a élargi les cadres de la communauté ainsi appuyée en faisant passer le nombre d'entités d'une poignée d'organisations avant la pandémie à plus de 150 organismes clés du secteur de la santé, en plus de travailler avec les responsables de la sécurité informatique de ces organismes sur une base régulière. En étroite collaboration avec Sécurité publique Canada, le Centre a facilité l'évaluation de la situation de cybersécurité de bon nombre de ces entités du secteur de la santé en vue de les aider à cerner leurs lacunes en la matière et à améliorer leur position de cyberdéfense et leur cyberrésilience.

Le Centre pour la cybersécurité a concentré ses efforts sur le soutien aux organismes de recherche et de développement de vaccins contre la COVID-19 dans l'ensemble du Canada. Nous collaborons avec bon nombre d'organisations de soutien à la vaccination pour offrir des services, comme la protection DNS, qui permettent de renforcer leurs capacités de cyberdéfense et de réduire considérablement leur vulnérabilité aux cyberattaques.

Pour protéger et appuyer les efforts déployés pour assurer la distribution des vaccins, le Centre pour la cybersécurité continue de collaborer avec le Groupe de travail fédéral, la chaîne d'approvisionnement en vaccins et les autorités de santé régionales dans l'ensemble du Canada afin d'accroître la sensibilisation à la cybersécurité, de rehausser le niveau de préparation aux interventions en cas d'incident et d'informer les organisations lorsque des menaces pèsent sur elles. Nous continuons de renforcer le périmètre de sécurité et le contrôle des accès dans le but de protéger le suivi des commandes de vaccins et le répertoire de données que les autorités de santé régionales s'emploient à constituer. Pour protéger les infrastructures essentielles, le CST et le Centre pour la cybersécurité restent aussi à l'affût d'informations sur les menaces qu'ils transmettent de façon proactive aux organismes canadiens, aux partenaires gouvernementaux et aux intervenants de l'industrie.

Enfin, la pandémie nous a tous rendus plus dépendants encore de l'infrastructure numérique. Plus que jamais, il est crucial que les Canadiens aient accès à la bonne information sur la façon de se protéger en ligne.

Le Centre pour la cybersécurité a mis en ligne une panoplie de conseils et d'avis pour informer les Canadiens sur la façon d'assurer leur sécurité en ligne. J'encourage les Canadiens à la recherche de conseils faciles à suivre sur la cybersécurité à consulter notre site Web: « pensezcybersécurité.ca ». D'autres publications sont offertes sur le site cyber.gc.ca à l'intention des entreprises et des grandes organisations, ou des citoyens désireux d'en savoir plus.

Le Centre de la sécurité des télécommunications s'efforce constamment d'atténuer les cybermenaces nationales et étrangères qui pèsent sur le secteur de la santé au Canada, et il continuera de le faire au cours de la présente pandémie et des années à venir.

Merci, monsieur le président.

● (1540)

**Le président:** Merci, monsieur Jones.

Nous allons maintenant entendre le représentant de Services partagés Canada.

**M. Sony Perron (premier vice-président, Services partagés Canada):** Bonjour, monsieur le président et mesdames et messieurs les membres du Comité. C'est avec plaisir que je m'adresse à vous aujourd'hui.

Je m'appelle Sony Perron et je suis premier vice-président à Services partagés Canada (SPC). Je suis accompagné de mon collègue Matt Davies, dirigeant principal adjoint de la technologie.

[*Français*]

Comme vous le savez, la ministre Murray a notamment pour mandat de diriger la transformation du gouvernement du Canada en un gouvernement plus axé sur le numérique afin d'améliorer les services offerts à la population canadienne. Pour moderniser efficacement la façon dont nous offrons des services numériques aux Canadiens et aux Canadiennes, nous investissons des ressources afin de maintenir et de développer un réseau rapide, fiable et sécurisé.

[*Traduction*]

Alors que de plus en plus de services sont offerts en ligne, il y a un risque accru de compromission des renseignements des Canadiens et du gouvernement. Il est donc essentiel que notre plan intègre des services efficaces en matière de cybersécurité d'entreprise. Nous devons accélérer les investissements afin de garder une longueur d'avance sur les auteurs de cybermenaces.

Comme vous pouvez l'imaginer, la sécurité des réseaux n'a jamais été aussi importante, alors que les Canadiens accèdent à un plus grand nombre de programmes et de services en ligne, comme la Prestation canadienne d'urgence, et que davantage de fonctionnaires travaillent à domicile.

[*Français*]

Avant la pandémie, environ 20 000 fonctionnaires accédaient à distance à un réseau au cours d'une journée de travail normale. Pour permettre aux fonctionnaires de travailler à domicile, Services partagés Canada, ou SPC, a été en mesure d'augmenter rapidement la capacité d'accès à distance protégé. Le réseau peut maintenant prendre en charge 290 000 connexions simultanément. Les fonctionnaires ont pu ainsi continuer d'offrir des services à la population canadienne pendant une période critique.

De plus, SPC a fait l'acquisition d'un ensemble d'outils de collaboration pour que les fonctionnaires fédéraux puissent continuer de travailler. Aujourd'hui, presque tous les fonctionnaires utilisent l'application Teams, qui permet de traiter de l'information jusqu'au niveau Protégé B.

[*Traduction*]

Selon nous, le nombre de personnes qui travaillent en ligne est tout simplement astronomique. Cette transition vers un milieu de travail décentralisé a été effectuée sans compromettre la sécurité informatique. Nous sommes conscients que le risque d'être la cible d'activités cybernétiques malveillantes devient de plus en plus élevé à mesure que le recours au télétravail et à des outils numériques augmente.

[*Français*]

SPC met sans cesse à jour son infrastructure de sécurité et ses logiciels pour tirer parti des mesures de sécurité les plus récentes. Nous sommes déterminés à protéger les données, les renseignements et l'infrastructure de technologies de l'information du gouvernement du Canada ainsi que les données et les renseignements personnels des Canadiens et des Canadiennes afin que ceux-ci puissent compter sur un gouvernement numérique sûr, stable et résilient.

● (1545)

[*Traduction*]

Nous collaborons avec le Centre canadien pour la cybersécurité et le Bureau du dirigeant principal de l'information du Secrétariat du Conseil du Trésor du Canada. Ils sont des partenaires essentiels de SPC aux fins de la conception et du déploiement de solutions informatiques adaptées.

En outre, nous controns chaque jour quelque deux milliards d'actions malveillantes. Il ne s'agit pas de cybermenaces purement théoriques. Ce sont de véritables menaces qui se concrétisent de façon organisée. Encore une fois, dans un tel contexte, la collaboration et la coordination avec nos partenaires sont essentielles.

[*Français*]

Les vulnérabilités de SolarWinds et de Microsoft Exchange qui ont été exploitées récemment ont mis en évidence la nécessité de pouvoir intervenir rapidement en cas de cyberincident et la nécessité de passer à de nouvelles technologies.

Nous avons récemment publié un document stratégique sur la voie à suivre pour moderniser le réseau, dans lequel nous demandons à nos partenaires de l'industrie et à différents intervenants de nous fournir leur rétroaction sur l'état futur du réseau.

[*Traduction*]

Dans ce document, nous précisons un certain nombre de priorités de Services partagés Canada, y compris la nécessité de passer à une infrastructure définie par logiciel, de tirer profit d'une technologie sans fil améliorée et d'adopter une architecture zéro confiance. Nous investissons dans nos capacités en matière de cyberdéfense et dans la migration vers une architecture zéro confiance.

[*Français*]

Le terme « zéro confiance » signifie que nous ne faisons jamais confiance et que nous faisons toujours des vérifications toujours tout avant d'accorder l'accès, et ce, grâce à un processus de surveillance continue. Cela exige d'authentifier les utilisateurs, de valider les appareils et de s'assurer que les personnes ont accès uniquement aux ressources dont elles ont besoin pour effectuer leur travail.

SPC a renforcé la sécurité générale de technologie de l'information du gouvernement du Canada grâce à des services tels que la défense multicouche, la gestion des vulnérabilités et l'intégrité de la chaîne d'approvisionnement. Notre programme intégré de cybersécurité et de sécurité de la technologie de l'information protège l'information qui soutient les autres ministères et organismes.

[*Traduction*]

Je tiens à assurer ce comité que nous surveillons constamment les cybermenaces et que nous disposons de systèmes et d'outils efficaces pour les détecter, mener des enquêtes et prendre les mesures qui s'imposent pour les neutraliser. Dans des circonstances normales de fonctionnement, aucune organisation n'est à l'abri des menaces à la sécurité informatique. Toutefois, nous vivons une période exceptionnelle. Services partagés Canada accorde et accordera toujours la priorité à la cybersécurité afin de protéger le gouvernement et la population canadienne contre les cybermenaces.

[*Français*]

Je vous remercie.

Nous serons heureux de répondre à vos questions.

**Le président:** Merci, monsieur Perron.

[*Traduction*]

Nous allons maintenant entendre le représentant du Secrétariat du Conseil du Trésor.

**M. Marc Brouillard (dirigeant principal de l'information du Canada par intérim, Secrétariat du Conseil du Trésor):** Merci, monsieur le président. Je suis ravi d'avoir l'occasion de comparaître à nouveau devant votre comité.

J'ai le plaisir d'être accompagné aujourd'hui par Aaron Snow, dirigeant principal du Service numérique canadien, ainsi que par mes collègues du Centre de la sécurité des télécommunications et de Services partagés Canada. Nous pourrons répondre aux questions des membres du Comité après mes observations liminaires.

Il serait peut-être utile d'expliquer brièvement les rôles et les responsabilités du Bureau du dirigeant principal de l'information en ce qui a trait à la cybersécurité au gouvernement du Canada. Le Bureau fournit une orientation stratégique et un leadership en matière de gestion de l'information, de technologie de l'information, de sécurité, de protection des renseignements personnels et d'accès à l'information dans l'ensemble du gouvernement du Canada.

C'est également au bénéfice de tout le gouvernement que nous fournissons du soutien et des conseils sur le renforcement des capacités, la gestion de projets et la surveillance. Les documents stratégiques du Conseil du Trésor décrivent les rôles et les responsabilités liés à la gestion de la cybersécurité du gouvernement du Canada et à la gestion ministérielle. Nous offrons l'orientation stratégique et la supervision nécessaires en nous appuyant sur la Politique sur la sécurité du gouvernement et sur la Politique sur les services et le numérique.

Nous définissons les exigences en matière de cybersécurité afin de garantir que l'information et les données, les applications, les systèmes et les réseaux du gouvernement du Canada et des ministères sont sûrs, fiables et dignes de confiance. Lorsqu'il se produit des incidents liés à la cybersécurité, le Secrétariat du Conseil du Trésor assure la coordination stratégique requise, ce qui peut comprendre la communication de directives aux ministères et organismes quant aux mesures à prendre pour minimiser l'impact à l'échelle du gouvernement du Canada.

Il s'agit là d'un travail essentiel. C'est pourquoi notre bureau travaille en étroite collaboration avec le Centre canadien pour la cybersécurité et Services partagés Canada afin de former le Comité tripartite de la sécurité de la technologie de l'information, une instance chargée d'élaborer et de maintenir une approche coordonnée et collaborative en matière de sécurité informatique dans l'ensemble du gouvernement du Canada. Il s'agit notamment de suivre l'évolution de l'environnement mondial des cybermenaces, de se tenir à l'affût des nouveaux facteurs de vulnérabilité qui pourraient avoir une incidence sur les systèmes gouvernementaux et de veiller à ce qu'il y ait une réponse coordonnée aux menaces potentielles et actives au moyen du Plan de gestion des événements de cybersécurité du gouvernement du Canada.

Et ce travail n'a fait que s'intensifier au cours des 14 derniers mois. Tout au long de la pandémie, nous avons collaboré de près avec Services partagés Canada pour soutenir les opérations gouvernementales en veillant à ce que l'infrastructure et les systèmes informatiques sécurisés continuent de permettre la prestation des services fédéraux essentiels. La collaboration virtuelle a été un élément clé pour assurer cette continuité des opérations. Pour ce faire, le gouvernement du Canada a dû s'adapter rapidement en permettant à 290 000 employés et entrepreneurs de travailler en toute sécurité à distance, ce qui représente une augmentation importante des connexions à distance par rapport aux niveaux d'avant la pandémie.

Dès les premiers jours de la pandémie, le Secrétariat du Conseil du Trésor, Services partagés Canada et le Centre pour la sécurité des télécommunications ont commencé à travailler en étroite collaboration pour répondre aux besoins en constante évolution du gouvernement du Canada. Services partagés Canada a acquis et distribué de nouveaux appareils et équipements, et a rapidement déployé de nouveaux systèmes de collaboration et de communication en nuage sécurisés, tandis que le Bureau du dirigeant principal de l'information a fourni des ressources, des conseils et des directives aux ministères, aux employés et aux entrepreneurs du gouvernement du Canada sur la façon de travailler à distance en toute sécurité. Pendant ce temps, le CSTC a multiplié les avis sur l'évolution de la situation des cybermenaces liées à la pandémie. Il s'agissait de faire en sorte que les fonctionnaires puissent continuer à servir les Canadiens tout en veillant à ce que la sécurité, la confidentialité et l'intégrité des renseignements gouvernementaux ne soient pas compromises.

Un autre exemple de collaboration est le travail du Service numérique canadien (SNC), une équipe du Secrétariat du Conseil du Trésor qui collabore avec les ministères pour les aider à surmonter les difficultés liées à la prestation des services. C'est ainsi que le SNC a mis au point GC Notification, un outil de la plateforme du gouvernement qui permet aux ministères de lancer rapidement et facilement des messages électroniques et textuels aux abonnés. Au début de la pandémie, la désinformation était prédominante. Le Service numérique canadien, Service Canada et Santé Canada ont alors mis leurs efforts en commun pour utiliser GC Notification afin de créer « Obtenir les nouvelles sur la COVID-19 », un service de courriels qui permet aux gens d'obtenir rapidement des renseignements fiables sur la pandémie. Depuis son lancement, le service a permis d'envoyer en toute sécurité plus de 5,5 millions de notifications aux abonnés.

Ainsi, la sécurité a été une priorité tout au long de la pandémie. Avec un si grand nombre de fonctionnaires travaillant à domicile, nous avons pris des mesures concrètes pour assurer en permanence la sécurité des réseaux gouvernementaux. Nous disposons de systèmes solides pour surveiller et détecter les menaces à la cybersécurité des informations qui peuvent résulter du travail à distance et pour enquêter sur ces menaces. Les mesures nécessaires, comme l'accès à distance sécurisé amélioré et d'entreprise, et les dispositifs de signature numérique ont été prises, assorties des orientations stratégiques appropriées, pour protéger les informations, tout en veillant à ce que les employés puissent continuer à fournir des services et des programmes de confiance aux Canadiens.

Nous nous sommes également efforcés de protéger le gouvernement du Canada en surveillant de façon continue les programmes importants pour les mettre à l'abri des cybermenaces, notamment en ce qui concerne les prestations liées à la COVID, comme la Prestation canadienne d'urgence. Le Centre évalue sans cesse le niveau de sécurité pour l'utilisation du nuage dans l'ensemble du gouvernement du Canada et l'efficacité des applications nuagiques, notamment pour l'Agence de la santé publique du Canada.

La pandémie de COVID-19 continue de transformer le paysage opérationnel du gouvernement, notamment pour ce qui est de la prestation de ses services. Elle nous a obligés à accélérer les efforts de transformation numérique déjà en cours, et à agir rapidement pour fournir de nouveaux services offrant un soutien direct aux Canadiens. À chaque étape du processus, la sécurité est restée au premier plan.

● (1550)

Nous demeurons déterminés à améliorer continuellement la cybersécurité au Canada en nous préparant à tous les types de cyberincidents et en protégeant les Canadiens et leurs données.

Merci, monsieur le président. Nous sommes prêts à répondre aux questions du Comité.

**Le président:** Merci, monsieur Brouillard.

Nous allons maintenant commencer le premier tour de questions.

Nous débutons par M. Paul-Hus qui dispose de six minutes.

[*Français*]

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

Bonjour, messieurs. Je vous remercie de votre présence.

Monsieur Jones, la première fois que je vous ai posé une question sur Huawei, c'était en septembre 2018, au Comité permanent de la sécurité publique et nationale. Je vous avais demandé quelle était la position du Canada au sujet de Huawei et du développement de la 5G. Évidemment, cela fait presque trois ans et l'information était moins connue, mais maintenant, nous savons très bien que nos partenaires du Groupe des cinq ont pris leur décision.

De votre côté, avez-vous remis votre rapport technique au gouvernement?

[*Traduction*]

**M. Scott Jones:** Le dossier a été soumis aux ministres. Je ne crois pas qu'il soit indiqué de ma part de vous en dire davantage à ce sujet. Je peux toutefois vous assurer que nous poursuivons nos efforts incessants avec nos partenaires dans le domaine de la cybersécurité...

[*Français*]

**M. Pierre Paul-Hus:** Monsieur Jones, je vous demande à vous, en tant que dirigeant principal du Centre canadien pour la cybersécurité, si vous avez remis un rapport. Je ne vous demande pas les résultats du rapport, je vous demande juste si vous avez remis le rapport au ministre de la Sécurité publique ou au ministre de la Défense nationale.

[*Traduction*]

**M. Scott Jones:** Monsieur le président, comme je le soulignais, nous continuons de travailler avec nos partenaires dans l'ensemble du gouvernement. Nous leur avons communiqué les renseignements à notre disposition, mais nous devons attendre... C'est le ministère de la Sécurité publique qui est responsable de l'étude et du rapport.

[*Français*]

**M. Pierre Paul-Hus:** D'accord.

J'aimerais vous poser une autre question concernant la même entreprise.

Votre organisme a-t-il été consulté au sujet du partenariat entre Huawei et Ice Wireless, une entreprise qui fait des projets de développement dans le Nord canadien?

● (1555)

[*Traduction*]

**M. Scott Jones:** Il faudrait que je fasse des vérifications pour pouvoir vous répondre.

Dans le cadre de notre programme d'examen de la sécurité, nous avons des échanges avec la majorité des fournisseurs de services de télécommunications au Canada. Nous leur parlons du déploiement de leurs services et de leurs plans, mais dans le contexte de l'environnement 4G/LTE pour l'instant. Si vous voulez de plus amples détails sur nos relations avec les différentes entreprises, je devrai faire des vérifications.

[*Français*]

**M. Pierre Paul-Hus:** Un groupe de 60 experts, dont des membres du Groupe national de coordination contre la cybercriminalité de la GRC, ont fait un plan détaillé de lutte contre les logiciels de rançon et demandent aux gouvernements du monde entier de prendre des mesures.

Est-ce que le gouvernement va accepter toutes les recommandations de ce rapport?

[*Traduction*]

**M. Scott Jones:** Si je vous ai bien compris, monsieur Paul-Hus, je crois que vous faites ici référence au rapport sur les rançongiciels.

[*Français*]

**M. Pierre Paul-Hus:** Oui.

[*Traduction*]

**M. Scott Jones:** Il ne m'apparaît pas acceptable qu'un fonctionnaire non élu parle au nom du gouvernement qui, lui, a été élu. Il va cependant de soi que nous explorons toutes les pistes envisageables pour améliorer nos moyens de défense contre les rançongiciels, une préoccupation de tout premier ordre pour le Centre canadien pour la cybersécurité.

[*Français*]

**M. Pierre Paul-Hus:** Je vous remercie.

Monsieur Perron, un rapport interne non confidentiel a été publié par le ministère de la Défense nationale concernant son évaluation du Programme de gestion de l'information et de technologie de l'information de la Défense.

Ce rapport, qui a été publié l'année dernière, critique Services partagés Canada concernant sa gestion des systèmes informatiques. Les militaires se plaignent fortement, d'une part, de ne pas être compris en ce qui concerne les opérations et, d'autre part, surtout, de ne pas avoir de services. Services partagés prenait parfois jusqu'à six mois pour répondre à des demandes du ministère de la Défense.

Qu'est-ce que vous pouvez dire là-dessus?

**M. Sony Perron:** Je vous remercie de votre question.

J'ai pris connaissance des références dans le rapport qui a été publié par le groupe de vérification de la Défense nationale. Ce rapport porte sur des actions des dernières années. Depuis, nous avons mis en place une nouvelle structure à Services partagés Canada qui nous permet d'avoir une meilleure interaction avec les ministères clients.

Nous avons maintenant un sous-ministre adjoint et une équipe qui servent exclusivement les ministères de la Défense nationale et des Anciens Combattants, ainsi que la Gendarmerie royale du Canada. Nous avons donc mis en place une nouvelle structure d'interaction, et nous essayons d'établir des plans plus intégrés.

Notamment, il y avait beaucoup de questions qui portaient sur le déploiement de services téléphoniques pour les bases militaires. Cela a été résolu. Nous avons maintenant un plan de travail mixte avec le ministère de la Défense nationale et nous avons commencé le travail. Donc, les choses s'améliorent.

**M. Pierre Paul-Hus:** C'est très bien. Avez-vous amélioré les services de fin de semaine? Un des problèmes était que personne ne répondait aux demandes les samedis et les dimanches. Y a-t-il maintenant des gens qui sont de garde et qui peuvent y répondre? Les Forces canadiennes travaillent sept jours par semaine, 24 heures par jour.

Avez-vous maintenant du personnel qui peut répondre aux demandes?

**M. Sony Perron:** Je suis désolé, mais je ne peux pas répondre à cette question précise. Chaque application, sur le réseau du gouvernement du Canada, a ses normes en matière de criticité et le temps de réponse est établi pour chacune. Pour la Défense nationale, les barèmes varient en fonction des services offerts. Il est possible que certains aient besoin d'être révisés. Cela dit, je ne suis pas en mesure de répondre à cette question. Par contre, je pourrai vous fournir la réponse par écrit, si vous le désirez.

**M. Pierre Paul-Hus:** Oui, s'il vous plaît. Nous aimerions obtenir des réponses à ce sujet.

Je vous remercie.

[*Traduction*]

**Le président:** Merci, monsieur Paul-Hus, pour vos questions et les réponses qu'elles ont suscitées.

Comme je l'ai déjà indiqué, si nos témoins souhaitent nous fournir des réponses plus détaillées après avoir fait les vérifications nécessaires, nous leur serions reconnaissants de bien vouloir transmettre le tout à notre greffier qui s'assurera de relayer l'information aux membres du Comité.

Merci.

Nous passons maintenant à M. Jowhari pour les six prochaines minutes.

**M. Majid Jowhari (Richmond Hill, Lib.):** Merci, monsieur le président.

D'abord et avant tout, je tiens à remercier tous nos témoins pour les services rendus par leurs organisations et eux-mêmes depuis toutes ces années, et plus particulièrement depuis la dernière année et demie, afin de veiller à ce que les fonctionnaires des différentes entités du gouvernement du Canada puissent travailler en toute sécurité.

Monsieur Jones, vous avez indiqué dans vos observations préliminaires que le Centre pour la cybersécurité a concentré ses efforts sur le soutien aux organismes de recherche et développement de vaccins contre la COVID-19 dans l'ensemble du Canada.

Pourriez-vous nous en dire plus long sur les mesures que vous avez prises à cette fin et sur le genre de menaces que vous avez pu détecter?

● (1600)

**M. Scott Jones:** Je suis ravi de pouvoir vous en parler. Il y a différents aspects à considérer.

D'abord et avant tout, nous sommes intervenus auprès de nombreuses organisations du secteur pour leur communiquer des conseils et des directives de base en matière de cybersécurité, mais aussi de l'information sur les menaces qui les guettent. Dès le début de la pandémie, nous avons constaté avec nos alliés que des actes malveillants commandités par des États ciblaient les chercheurs dans le domaine des vaccins. Nous avons alors dénoncé publiquement les coupables.

Nous avons ensuite conseillé les différentes organisations quant à la forme que peuvent prendre les menaces semblables et aux moyens qu'elles peuvent mettre en oeuvre pour se protéger. Nous poursuivons nos efforts auprès de ces organisations pour veiller à ce qu'elles fassent le nécessaire pour améliorer leur cybersécurité en les conseillant sur les mesures à prendre en ce sens. Dans ce contexte, nous leur transmettons les enseignements tirés de notre défense du gouvernement du Canada de telle sorte qu'elles soient prêtes à affronter n'importe quelle menace. Nous mettons aussi bien sûr à contribution notre mandat de renseignement étranger pour connaître les visées des auteurs de ces menaces afin de pouvoir tenir le secteur au courant pour que les mesures nécessaires puissent être prises avant que ces menaces se concrétisent.

**M. Majid Jowhari:** Vous avez aussi indiqué que vous collaborez avec des organisations de soutien à la vaccination. Vous avez parlé de services de protection DNS.

Pouvez-vous nous expliquer en quoi consistent exactement ces services de protection et quelles mesures votre organisation a prises dans ce contexte?

**M. Scott Jones:** C'est l'un des sujets dont j'ai traité lors d'une de mes comparutions précédentes où j'ai parlé du Bouclier canadien, un service pour lequel nous avons collaboré avec l'Autorité canadienne pour les enregistrements Internet (ACEI).

Supposons que vous recevez un courriel avec un hyperlien vers un maliciel sur lequel on vous invite à cliquer; c'est de la cybercriminalité. Si vous cliquez sur le lien en question, le service de protection DNS va faire en sorte qu'il ne pourra pas s'ouvrir. Vous n'irez pas plus loin. C'est de cette façon que vous êtes protégés. On vous empêche de commettre une erreur en cliquant sur le lien.

Nous avons travaillé en partenariat avec l'ACEI pour offrir le même service aux entités commerciales, et aux organisations de soutien à la vaccination dans le cas qui nous intéresse. Nous l'avons fait en raison de la menace qui pèse sur ces organisations depuis le début de la pandémie. Nous avons fait le nécessaire pour leur offrir le même service.

Nous nous sommes inspirés de tout ce que nous avons appris en assurant la protection du gouvernement du Canada et en bloquant différents sites. Nous sommes à l'origine de pas moins de sept milliards d'actions par jour pour défendre le gouvernement. Nous veillons à communiquer toute l'information pertinente à ce sujet à l'ACEI, notre partenaire dans ce dossier, afin que toutes ces organisations puissent bénéficier de la même protection.

**M. Majid Jowhari:** Je comprends aussi que notre gouvernement a récemment revu son plan stratégique des opérations numériques. J'aimerais connaître les réflexions des trois témoins à ce sujet. Pourriez-vous commencer par nous expliquer en quoi consiste un plan stratégique des opérations et comment chacun de vos ministères y contribue?

Nous pourrions probablement commencer par M. Jones.

**M. Marc Brouillard:** Monsieur le président, c'est mon bureau qui publie le Plan stratégique des opérations numériques. Si vous êtes d'accord, j'aimerais commencer, après quoi je suis certain que les autres témoins pourront ajouter leur grain de sel.

**M. Majid Jowhari:** Très bien. Procédons ainsi si c'est mieux.

**M. Marc Brouillard:** Merci.

Le Plan stratégique des opérations numériques est un document mis à jour chaque année. Il se veut un plan de gestion intégré trisannuel régissant les services, l'information, les données et la cybersécurité. Le PSON actuel a été mis à jour pour tenir compte de l'accélération de la transformation numérique.

Ce plan repose sur quatre piliers. Le premier consiste à moderniser la façon dont nous remplaçons, bâtissons et gérons nos grands systèmes de TI, pour corriger les failles dont nous avons hérité, ce qu'on appelle la dette technique au sein de nos organisations. Le deuxième consiste à fournir des services aux gens où et quand ils en ont besoin, en mettant l'accent sur les services à offrir aux Canadiens. Le troisième consiste à favoriser une approche pangouvernementale des opérations numériques, selon une perspective d'entreprise, pour éviter le dédoublement des efforts. Le quatrième concerne la transformation de nos méthodes de travail, nous voulons comprendre les nouvelles façons de travailler, d'assurer la gouvernance, de fournir des ressources; ce sont des éléments essentiels pour relever le défi.

Je m'arrêterai là et laisserai les autres témoins vous répondre, s'ils le souhaitent.

**M. Sony Perron:** Monsieur le président, pour Services partagés Canada, ce plan est essentiel puisqu'il est l'architecture et l'orientation qui guident tous les ministères offrant des services à la clientèle dans le déploiement de leurs programmes, pour tout ce qui concerne la gestion de leur architecture obsolète et l'aide que nous pouvons leur offrir, la modernisation de leur infrastructure et l'aide que nous pouvons leur offrir, de même que leur transformation organisationnelle et l'aide que nous pouvons leur offrir. Tous les signaux envoyés dans ce plan sont essentiels pour guider SPC dans l'accomplissement de son mandat.

Ce plan influence le ministère client qui nous demande de l'aide pour mettre en oeuvre son propre programme en matière de TI, il lui sert de cadre général. Nous sommes prêts à l'appuyer, ce qui sous-entend d'offrir un soutien à la migration de la charge de travail. Il favorise également une plus grande connexion au nuage, un accès sécurisé à l'infonuagique. Il incite les ministères à participer activement à des solutions d'entreprise pour éviter les doublons technologiques au profit d'une approche d'entreprise susceptible de servir à tous les ministères. C'est un pilier essentiel de notre programme.

● (1605)

**M. Majid Jowhari:** Merci. Je pense que je n'ai plus de temps.

**Le président:** Comme les représentants des deux autres ministères ont pu répondre à la question, si vous souhaitez nous répondre brièvement, monsieur Jones, nous vous en serons reconnaissants. Merci.

**M. Scott Jones:** Merci, monsieur le président.

Rapidement, je pense que le Plan stratégique des opérations numériques nous permet de veiller à ce que la sécurité soit un enjeu central du début à la fin, à ce qu'on y réfléchisse bien dès le début, puis à ce qu'on fixe des priorités en conséquence. Le fait est que nous avons un nombre limité d'experts en matière de sécurité, donc cela nous permet de les affecter aux priorités les plus importantes de l'ensemble du gouvernement du Canada pour l'aider à atteindre ses objectifs. Ces deux éléments sont essentiels.

**M. Majid Jowhari:** Merci, monsieur le président.

**Le président:** Merci.

Je donnerai maintenant la parole à Mme Vignola pour six minutes.

[*Français*]

**Mme Julie Vignola (Beauport—Limoilou, BQ):** Je vous remercie, monsieur le président.

Ma question s'adresse à M. Jones.

L'offre de services aux Canadiens a-t-elle été interrompue à cause de cyberévénements malveillants?

[*Traduction*]

**M. Scott Jones:** Nous devons composer avec toutes sortes de cyberactivités tous les jours. Comme je l'ai mentionné il y a quelques minutes, nous intervenons entre deux milliards et huit milliards de fois par jour, en moyenne environ sept milliards de fois, parce qu'il y a toujours beaucoup de cyberactivités qui ciblent le gouvernement, mais à ma connaissance...

[*Français*]

**Mme Julie Vignola:** Je sais qu'il y a beaucoup de cyberattaques. Toutefois, est-ce que certains événements ont empêché l'offre de services aux Canadiens?

[*Traduction*]

**M. Scott Jones:** Je laisserais probablement mon collègue, M. Brouillard, vous répondre du point de vue du Conseil du Trésor, mais à ma connaissance, de mon point de vue, nous gérons bien la situation. Il n'y a pas eu d'interruption de services en raison de cyberattaques à l'encontre du gouvernement du Canada. Il y a des cyberincidents qui nous ont poussés à agir, mais aucune cyberattaque n'a véritablement réussi à paralyser les services.

[*Français*]

**Mme Julie Vignola:** D'accord, merci.

Nous savons tous que les données personnelles de dizaines de milliers, voire de centaines de milliers de personnes ont été volées. Elles ont reçu des relevés de revenus pour des salaires qu'elles n'ont jamais gagnés.

Quelles sont les causes de ces vols de données? Quelles solutions sont mises en place?

● (1610)

**M. Marc Brouillard:** Je peux répondre à cela.

Vous faites allusion à l'attaque de bourrage de justificatifs qui a eu lieu l'été dernier. L'identité de certains Canadiens a été volée par d'autres sources. Nous ne savons pas quelles sont précisément ces sources, mais nous savons que d'autres événements ont affecté l'économie canadienne.

Ces renseignements se retrouvent souvent sur ce qu'on appelle le Web caché, qui est en quelque sorte le côté criminel d'Internet. Les criminels s'emparent de l'identité des gens ou de n'importe quels renseignements qu'ils peuvent recueillir et tentent de les utiliser dans les systèmes fédéraux. Lorsque nous avons constaté que des systèmes faisaient l'objet de nombreuses attaques visant l'identité des personnes, nous avons pris la décision de fermer le service, et ce, par souci de prévention. Nous voulions nous assurer qu'il n'y aurait pas d'attaques plus importantes. Par la suite, l'Agence du revenu du Canada a vérifié les transactions. Dans tous les cas où c'était suspect, on a communiqué avec les citoyens ou la situation a été renversée.

**Mme Julie Vignola:** D'accord, je vous remercie.

Les logiciels qui sont très souvent utilisés sont ceux qui sont le plus fréquemment visés par des cyberattaques. C'est le cas pour la suite Office et pour tout ce qui touche à Microsoft.

L'utilisation de logiciels comme ceux de Microsoft n'expose-t-elle pas davantage le gouvernement à des cyberattaques, étant donné que c'est cette compagnie qui est majoritairement visée?

**M. Marc Brouillard:** Je vais laisser mon collègue M. Jones répondre à cette question.

[*Traduction*]

**M. Scott Jones:** Je vous remercie de cette question.

Il y a un certain nombre de choses à prendre en considération. Oui, ce sont les logiciels les plus utilisés, donc évidemment, ce sont les logiciels les plus fréquemment visés par les acteurs malveillants. Cependant, ce sont également ceux que les chercheurs en matière de sécurité connaissent le mieux.

Je dois mentionner la stratégie du gouvernement du Canada pour bien gérer des choses comme les rustines et les mises à jour de logiciels. C'est l'un des avantages que nous confère Services partagés Canada. Nous constatons une nette amélioration quand SPC est le ministère responsable de répondre rapidement aux alertes. Dans les cas les plus graves, quelques minutes à peine après que nous l'ayons avisé, SPC commençait à déployer des rustines pour que nous soyons prêts à réagir; c'est quelque chose.

Chaque logiciel a ses vulnérabilités. Tout dépend ensuite de la rapidité avec laquelle on peut réagir pour atténuer ou réduire le risque auquel s'expose une organisation. Aucun logiciel n'est invulnérable, malheureusement.

[*Français*]

**Mme Julie Vignola:** Au cours des derniers mois, les Russes se sont amusés à plusieurs reprises à attaquer les systèmes des États-Unis, notamment un logiciel du fournisseur américain SolarWinds. Ces gens ont réussi à infiltrer le Département de la sécurité intérieure des États-Unis et le Département du Trésor.

De telles attaques ont-elles eu lieu au Canada? Le cas échéant, quelles ont été les cibles de ces attaques et comment y a-t-on fait face?

**M. Marc Brouillard:** Certaines entreprises faisant partie du réseau du gouvernement du Canada utilisaient le logiciel de SolarWinds, mais à cause de notre infrastructure, de la capacité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada, on a pu déterminer ce qui se passait et constater que notre infrastructure ne faisait l'objet d'aucune attaque. On a cerné les points vulnérables et on s'est employé à résoudre le problème. À ce que je sache — mon collègue M. Jones pourra le confirmer —, nous n'avons vécu en aucun cas ce qu'ont vécu les États-Unis.

**Mme Julie Vignola:** Je vous remercie.

[*Traduction*]

**Le président:** Merci.

Je donnerai maintenant six minutes à M. Green.

**M. Matthew Green (Hamilton-Centre, NPD):** Merci.

Je serai heureux de poursuivre dans la foulée de ces questions. Par votre intermédiaire, monsieur le président, je m'adresse à M. Jones. Pour que tout le monde comprenne bien, je crois que mon amie du Bloc faisait allusion aux quelque 50 000 incidents malicieux repérés à l'encontre de l'ARC. Est-ce le genre de chose qui pousserait le Centre de la sécurité des télécommunications à intervenir ou reviendrait-il plutôt à l'ARC d'effectuer l'analyse en profondeur?

**M. Scott Jones:** Monsieur le président, je pense que c'est une excellente question.

La menace, ici, vient du bourrage d'identifiants ou du vol de renseignements, au moyen de renseignements déjà volés sur tant d'entre nous lors de diverses atteintes à la sécurité des données; ces renseignements sont ensuite réutilisés contre le gouvernement.

Habituellement, il faut se demander quelle forme prend l'attaque contre l'application pour commettre les fraudes. Cet aspect relève du ministère. Les fonctionnaires savent à quoi ressemble l'activité normale, donc ils sont à l'affût de tout ce qui peut sembler anormal, mais évidemment, nous travaillerons avec eux.

Nous travaillons en étroite collaboration avec l'ARC à cet égard, comme avec tout ministère offrant le même genre de service, mais du strict point de vue de la cybersécurité, ce genre d'activité pourrait, de l'extérieur, avoir l'air normal. Le pirate a le nom d'utilisateur et le mot de passe de la personne, de sorte que l'activité semble tout à fait légitime. Nous sommes là pour veiller à ce qu'il n'y ait pas de brèche entre les ministères, donc nous surveillons ce qui se passe de l'extérieur, alors que les gens du ministère restent à l'affût de toute activité frauduleuse de l'intérieur.

**M. Matthew Green:** Nous avons beaucoup entendu parler de la prévalence de la fraude au titre de la PCU, puis nous entendons M. Brouillard nous dire qu'environ 50 000 identités circulent dans le Web caché. Y a-t-il déjà quoi que ce soit qui nous porte à croire que les renseignements ainsi obtenus ont pu être utilisés pour présenter des demandes frauduleuses au titre de la PCU?

● (1615)

**M. Scott Jones:** Monsieur le président, je pense que je vais laisser mon collègue...

**M. Matthew Green:** Monsieur le président, avant que M. Jones ne cède la parole à son collègue, j'aimerais lui demander si ce genre de chose serait de son ressort.

**M. Scott Jones:** Ce sont vraiment deux choses différentes, monsieur le président. Je pense qu'il y a beaucoup d'atteintes à la protection des données qui ont lieu. Le commissaire à la protection de la vie privée du Canada a dit, dans notre évaluation des cybermenaces nationales, où nous abordons justement la question, que 28 millions de Canadiens se sont fait voler des renseignements personnels l'an dernier. Ces renseignements sont ensuite réutilisés pour cibler le gouvernement du Canada. Ainsi, une personne peut réutiliser des mots de passe pour se connecter.

Ce ne sont pas des renseignements qui ont été volés au gouvernement. Ils ont été volés ailleurs, mais les gens les réutilisent. Nos questions de sécurité sont souvent les mêmes. Quelle est votre couleur préférée? Quelle école avez-vous fréquentée? C'est le genre de renseignement que ces criminels volent, et comme les mots de passe sont une chose horrible et que nous en avons tous beaucoup trop, nous avons tendance à les réutiliser. Beaucoup de Canadiens les réutilisent, donc les pirates ont pu en réutiliser certains. C'est le propre du bourrage d'identifiants. Dans ce cas, ce sont des renseignements obtenus au moyen d'atteintes à la protection des données ailleurs qui sont réutilisés contre le gouvernement du Canada. Mais peut-être M. Brouillard pourrait-il...

**M. Matthew Green:** Je vous pose la question en toute déférence, parce que ce n'est pas tous les jours que nous recevons un représentant du Centre de la sécurité des télécommunications. C'est pourquoi j'essaie de profiter au maximum de notre échange, parce que je ne sais pas quand vous reviendrez.

Est-ce un scénario possible? Je vous pose la question pour m'instruire moi-même. Se pourrait-il que des renseignements obtenus par l'exploitation des vulnérabilités de l'ARC aient été utilisés pour présenter des demandes frauduleuses au titre de la PCU? Peut-être que je simplifie à outrance ou que je confonds les choses.

J'aimerais beaucoup vous entendre à ce sujet, monsieur Jones.

**M. Scott Jones:** Cela me semble assez peu probable, honnêtement, parce que ce n'est pas ce que nous avons observé. Nous avons vu des Canadiens se faire usurper leur identité pour cela, des pirates ont utilisé leurs renseignements personnels légitimes pour se connecter en leur nom. C'est principalement ce que je peux vous répondre à ce sujet, mais M. Brouillard pourra peut-être vous en dire davantage.

**M. Matthew Green:** Je comprends. Quand j'entends que l'information pourrait circuler dans le Web caché, j'ai une vision assez sombre de ce que cela pourrait donner et de la façon dont le crime organisé, classique ou non, et d'autres entités pourraient utiliser ces renseignements pour frauder le gouvernement. Je me demande seulement si nos propres vulnérabilités peuvent avoir joué un quelconque rôle dans la situation.

J'ai une question complémentaire à poser à M. Jones par votre intermédiaire, monsieur le président.

J'entends souvent parler, dans différentes réunions de comités sur les comptes publics et ailleurs, de l'obsolescence de certaines technologies. Est-ce une chose sur laquelle se penche le Centre de la sécurité des télécommunications? Serait-il de votre ressort d'examiner les vulnérabilités systémiques du gouvernement, puis d'informer les ministères concernés de vos constats, qui n'auraient qu'à trier l'information pertinente dans leurs efforts pour repérer nos plus grandes failles en matière de sécurité?

**M. Scott Jones:** C'est une excellente question, et vous vous trouvez devant le bon groupe de personnes pour y répondre. Nous représentons les trois entités chargées d'évaluer comment nous assurer de la robustesse du gouvernement. M. Brouillard est notre chef d'orchestre, en sa qualité de dirigeant principal de l'information du gouvernement. Donc oui, la réponse à votre question, c'est que parfois, l'obsolescence nous avantage. Parfois, il y a des technologies si vieilles qu'elles ne sont plus…

**M. Matthew Green:** Comme la disquette. Il n'y aura pas d'espionnage sur nos disquettes.

**M. Scott Jones:** Certaines technologies sont si vieilles qu'elles ne sont pas accessibles par Internet. Dans la plupart des cas, toutefois, c'est là où intervient Services partagés Canada, avec sa stratégie du périmètre, pour accroître la sécurité et intégrer divers outils de sécurité pour nous conférer le niveau de protection voulue… Nous prenons très au sérieux la nécessité de protéger l'information.

Quand nous modernisons nos systèmes et déployons le Plan stratégique des opérations numériques, nous nous assurons d'instaurer un degré de sécurité élevé dès le départ. Le fait est qu'il y a tellement d'atteintes à la protection des données — je parle ici de tout ce qui se passe à l'extérieur du gouvernement du Canada — qu'il y a déjà énormément de renseignements accessibles sur chaque citoyen, sur chacun d'entre nous, sur le Web.

Je peux vous dire que j'ai moi-même déjà été victime de vols de données, quand il y a eu l'attaque contre Yahoo…

**M. Matthew Green:** Ouf. Ils n'ont pas choisi la bonne personne.

**M. Scott Jones:** C'est la réalité.

**M. Matthew Green:** Oui, malheureusement.

**Le président:** Merci, monsieur Green.

Merci, monsieur Jones.

C'est ici que se termine le premier tour. Nous commencerons le deuxième.

C'est M. McCauley qui disposera des cinq premières minutes.

**M. Kelly McCauley (Edmonton-Ouest, PCC):** J'ai bien aimé la série de questions de M. Green.

Je remercie les témoins d'être parmi nous aujourd'hui.

Le rapport annuel révisé du Comité des parlementaires sur la sécurité nationale et le renseignement est apparu sur nos bureaux il y a quelques jours. J'ai quelques questions à vous poser à ce sujet.

On peut y lire que la Chine et la Russie sont les principaux acteurs malicieux dont il faut nous méfier. Cela concerne-t-il l'espionnage industriel, les attaques contre le gouvernement, les attaques contre nos systèmes logistiques, nos services publics ou d'autres choses? Pouvez-vous nous informer davantage à ce sujet?

● (1620)

**M. Scott Jones:** Monsieur le président, j'aimerais vous renvoyer à l'évaluation des cybermenaces nationales que nous avons publiée en novembre 2020. Nous avons inscrit quatre États à la liste des principales menaces contre le Canada, soit la Chine, la Russie, la Corée du Nord et l'Iran. Nous avons mentionné que le vol de propriété intellectuelle était l'un des grands éléments à surveiller, mais il y a également l'infrastructure essentielle.

Je tiens toutefois vraiment à souligner que nous avons écrit qu'en l'absence d'hostilités internationales, il nous semble extrêmement peu probable qu'un État s'attaque délibérément à notre infrastructure essentielle. Je tiens à insister sur ce point parce que…

**M. Kelly McCauley:** Qu'entendez-vous par infrastructure essentielle? Vous dites faire ce constat en l'absence d'actes de guerre. Nous avons pourtant vu l'attaque contre Colonial il y a quelques semaines à peine. Ne pourrions-nous pas craindre la même chose contre nous?

**M. Scott Jones:** Oui, tout à fait. En fait, c'est ce que j'ai dit au journaliste du *National Post*. Le problème, c'est que quand un rançongiciel est déployé contre une victime comme un fournisseur d'infrastructure essentielle, compte tenu de l'intégration des technologies, l'entreprise doit, pour se défendre, mettre toute sa technologie hors ligne. Elle s'isole et se ferme pour prendre des mesures de protection.

C'est ce que le public a vu dans l'attaque contre Colonial. L'entreprise a transféré toute l'exploitation de ses oléoducs hors ligne pour pouvoir reprendre la maîtrise de son infrastructure. Nous soulignons justement dans notre évaluation des cybermenaces nationales qu'il faut prendre ce genre de choses très au sérieux. Les rançongiciels sont la principale menace à laquelle sont exposés le Canada et les Canadiens. Ils menacent notre infrastructure essentielle exactement pour les raisons que nous venons d'évoquer. Nous espérions tous, dans le domaine de la cybersécurité, ne jamais voir d'attaque comme celle qui a été perpétrée contre Colonial, mais ce n'est que la première d'une longue liste.

**M. Kelly McCauley:** Qui serait responsable de surveiller ce genre de chose? On dit toujours que c'est une responsabilité énorme. Bien sûr, il y a les aéroports, les oléoducs, les services publics. De manière générale, qui en a la responsabilité, pour qu'une situation telle que celle que nous avons vue chez Colonial ne se reproduise plus, pour qu'il n'y ait pas d'attaque contre un aéroport ou ce genre de chose? Est-ce que cela relève de différents ordres de gouvernement?

**M. Scott Jones:** Cela varie. Nous travaillons avec tous les ordres de gouvernement, de même qu'avec les fournisseurs d'infrastructure essentielle. Nous nous assurons de leur fournir toute l'information pertinente. Nous essayons de tisser des relations avec chaque entreprise. En général, les gens sont très réceptifs à notre démarche. Ils se soucient tous autant que nous de la sécurité.

Cependant, de manière générale, l'environnement des TI est fragile du point de vue de la cybersécurité, de sorte qu'il faut prévoir de multiples mécanismes de défense. Cela nous amène à travailler ensemble. C'est une responsabilité partagée, cela ne dépend pas que du gouvernement fédéral, puisqu'en définitive, c'est le propriétaire ou l'exploitant de l'infrastructure qui est l'ultime responsable. C'est le propriétaire du réseau, le propriétaire de l'infrastructure. C'est lui qui prend les décisions en matière d'investissement. Nous nous efforçons de faire en sorte qu'il soit le mieux renseigné possible, après quoi nous travaillons ensemble pour réagir aux menaces le plus tôt possible. C'est une responsabilité commune.

**M. Kelly McCauley:** Qu'en est-il des sociétés d'État? Sont-elles traitées exactement comme les ministères?

**M. Scott Jones:** Non, monsieur le président. Les sociétés d'État ont un statut unique. Nous sommes en mesure de leur offrir la même qualité de service qu'à toutes les organisations fédérales. Cependant, en raison de leur structure, leurs dirigeants ont tendance à avoir plus de souplesse quant aux décisions à prendre en matière de cybersécurité, un peu comme dans le secteur privé, mais nous travaillons avec beaucoup de sociétés d'État.

**M. Kelly McCauley:** Oui, cela vient évidemment de beaucoup de décisions prises il y a longtemps déjà, avant que ce genre de problème n'existe. Est-ce une chose qu'il faudrait repenser? Certes, les sociétés d'État fonctionnent de manière indépendante, mais pour une chose comme la cybersécurité, faudrait-il repenser leur structure et les assujettir au CTC?

**M. Scott Jones:** Eh bien, comme je le disais, nous sommes en mesure de leur offrir toute la gamme de services que nous offrons aux autres organisations fédérales. Le gouvernement fédéral est de loin notre principal client, mais nos services sont optionnels pour les sociétés d'État. Chacune fait ses propres choix. Nous leur avons toutes offert de travailler avec nous, comme nous offrons nos services à tous les ministères.

● (1625)

**M. Kelly McCauley:** Merci.

**Le président:** Merci, monsieur McCauley.

Nous passons maintenant à M. Kusmierczyk, pour cinq minutes.

**M. Irek Kusmierczyk (Windsor—Tecumseh, Lib.):** Merci, monsieur le président.

Chaque année, le dirigeant principal de l'information remet des prix communautaires. En 2020, Services partagés Canada a reçu le prix d'excellence en matière de diversité et d'inclusion pour le Programme d'accessibilité, d'adaptation et de technologie informatique adaptée, ou AATIA. J'ai été ravi de voir que le budget de 2021 accordait un montant supplémentaire de trois millions de dollars pour cet important programme. Encore une fois, je suis enchanté par le travail que fait Services partagés Canada pour l'accessibilité et l'inclusion des personnes handicapées, alors bravo à l'équipe.

En cette Semaine nationale de l'accessibilité, existe-t-il des problèmes particuliers en ce qui a trait à la cybersécurité et à l'inclusion des personnes handicapées? En d'autres termes, comment rendre la cybersécurité accessible?

Je suppose que cette question s'adresse à M. Perron ou à M. Davies.

**M. Sony Perron:** Monsieur le président, c'est une question intéressante dans le sens où, bien que nous soyons très concentrés sur la sécurité et la cybersécurité, nous devons nous assurer que nos employés et les Canadiens ont accès aux services et aux systèmes que nous mettons en place. Outre la sécurité, l'accessibilité est toujours l'une de nos préoccupations.

À Services partagés Canada, nous avons une équipe, qui s'appelle l'équipe du Programme d'accessibilité, d'adaptation et de technologie informatique adaptée. Elle conseille les ministères sur les applications et les solutions qui sont à leur disposition pour assurer l'accessibilité par défaut de toute chose qui peut être lancée, qu'il s'agisse d'une application ou d'un nouveau processus. Des efforts sont aussi faits pour veiller à ce que tout ce qui est en place depuis un certain temps soit également examiné et ajusté à cet égard. Nous observons les normes en matière d'accessibilité. Nous avons cette capacité, et c'est très important.

Le lien avec la sécurité, c'est que lorsque nous mettons en œuvre de nouvelles mesures, nous devons nous assurer que nous les testons du point de vue de l'accessibilité afin d'éviter qu'elles ne deviennent un obstacle pour ceux qui ont légitimement besoin de ces applications et de ces systèmes pour faire leur travail ou se prévaloir de leurs services. Il est essentiel que nous maintenions ce focus.

Il y a deux autres aspects à ce programme. L'un consiste à permettre aux employés de recevoir une évaluation de ce dont ils pourraient avoir besoin pour fonctionner pleinement sur le lieu de travail. On veille en cela à assurer l'égalité des moyens. L'autre consiste à fournir des conseils. L'année dernière, nous avons ajouté une dimension qui manquait à ce programme, à savoir que les nouveaux employés ou les employés temporaires qui arrivent bénéficient également de ce que nous appelons la bibliothèque de prêt. Il s'agit de s'assurer qu'au début de leur emploi au gouvernement fédéral en tant qu'employeur de choix, nous leur fournissons les outils et les mesures d'adaptation susceptibles de les aider à participer pleinement au travail, qu'il s'agisse de technologies, de moniteurs, d'appareils particuliers ou d'applications prévues à cette fin. Ce programme est d'une importance cruciale.

Merci de l'avoir mentionné. C'est très important, surtout cette semaine.

**M. Irek Kusmierczyk:** C'est exactement cela. J'apprécie le fait que chaque fois que nous cherchons à proposer des mesures de cybersécurité, nous les considérions sous l'angle de l'accessibilité afin d'éviter de créer de nouveaux obstacles pour nos employés fédéraux.

Selon le plan stratégique des opérations numériques, le gouvernement fédéral est en voie de lancer le programme UnGC, qui permettra aux particuliers et aux entreprises d'utiliser une seule identité et un seul mot de passe pour accéder aux services du gouvernement fédéral par l'intermédiaire d'un guichet unique sur Canada.ca. Il s'agit aussi de faciliter les choses pour les gens.

Quel est l'état d'avancement des travaux effectués pour la plateforme UnGC? Quels problèmes pourraient se mettre en travers de la concrétisation de cette vision?

**M. Marc Brouillard:** Le principe derrière UnGC, c'est que nous ne voulons pas que les Canadiens aient à essayer de comprendre et de décoder toute la machinerie bureaucratique gouvernementale qui se cache derrière. Nous voulons en outre faire en sorte que tous les services offerts aux Canadiens soient vraiment accessibles à partir d'un seul guichet. Voilà ce qu'est Canada.ca. Pour passer à l'étape suivante, pour passer à un environnement axé sur les services, la base est l'identité numérique. Nous voulons permettre aux Canadiens d'utiliser l'identité de confiance de leur choix pour accéder aux services sur Canada.ca et pour passer d'un service à l'autre sans à-coups.

Nous avons récemment lancé un projet pilote avec Emploi et Développement social Canada, appelé le Programme de modernisation du versement des prestations, pour permettre l'accès à un système d'ouverture de session — Sign In Canada — qui permettra aux Canadiens d'accéder de façon transparente aux prestations offertes par ce ministère. Les usagers n'auront qu'à se brancher une fois pour accéder à plusieurs services.

Nous faisons cela dans une optique d'entreprise, de sorte qu'une fois ce travail achevé, le système pourra être réutilisé par d'autres ministères et organismes. Ultimement, tous les services du gouvernement du Canada seront disponibles par le truchement d'une capacité d'identification unique. C'est ce que nous appelons le « UnGC ».

Merci.

● (1630)

**M. Irek Kusmierczyk:** Cette simplification ou cette rationalisation des services présente-t-elle des risques ou des problèmes supplémentaires sur le plan de la cybersécurité?

**M. Marc Brouillard:** Dans le cadre du modèle actuel, si tous les services étaient accessibles à partir d'un seul justificatif d'identité et que ce dernier était compromis, il y aurait évidemment un risque accru. Pour résoudre ce problème, nous faisons en sorte que l'accès n'est pas seulement lié à un justificatif, mais aussi à une véritable identité numérique, quelque chose qui est vérifiable et hautement sécurisé. Par exemple, vous devriez être en mesure de fournir l'accès à votre identité provinciale, plus peut-être fournir un mot de passe ou une autre forme d'identification. Plusieurs actions seront nécessaires pour cautionner l'accès. Nous appelons cela l'authentification multifactorielle. C'est ce qui rendra ce service plus sûr.

**Le président:** Merci, monsieur Kusmierczyk.

Nous passons maintenant à Mme Vignola pour deux minutes et demie.

[*Français*]

**Mme Julie Vignola:** Merci beaucoup.

Ma question s'adressera à M. Jones ou à M. Brouillard. Ils se partagent la tâche.

Monsieur Brouillard, la semaine dernière, on a parlé un peu à la blague des systèmes désuets en les comparant à nos vieux systèmes DOS. Blague à part, quels sont les plus grands risques et les principales menaces causées par la désuétude de nos systèmes? La vérificatrice générale a parlé de points de rupture causés par la désuétude.

Est-on rendu à ce point de rupture? Quelles pourraient en être les conséquences pour les citoyens? D'où viennent les menaces exactement? Est-ce que ce sont des menaces internes ou est-ce que ce sont des menaces à l'international? Si c'est à l'international, quel pays nous attaque?

**M. Marc Brouillard:** Je vais répondre à la question le premier.

Je vais expliquer la différence entre la dette technique et les risques liés aux systèmes existants.

Premièrement, plus les systèmes sont âgés, plus cela coûte cher de les maintenir. C'est comme si on achetait une voiture et qu'on ne mettait pas d'huile dans le moteur: tôt ou tard, il faudrait remplacer le moteur.

Deuxièmement, plus les systèmes vieillissent, plus les cyberrisques augmentent parce que les systèmes sont exposés pendant beaucoup plus longtemps aux cyberattaquants.

Je donne la parole à M. Jones afin qu'il explique ce risque.

[*Traduction*]

**M. Scott Jones:** Merci.

J'aimerais ajouter deux ou trois choses. La première, c'est que si le système est connecté à Internet, il doit être maintenu à jour. C'est à cet égard que diffère le branchement de l'environnement traditionnel. C'est là qu'un environnement moderne change la menace.

Cela étant dit, en général, l'origine des menaces n'a pas d'importance pour un cyberdéfenseur. Nous regardons à quoi pourrait ressembler l'activité malveillante, quelle que soit sa provenance, car nous ne faisons pas de distinction sur ce plan. Ensuite, s'il y a une menace, elle est traitée par les autorités compétentes qui enquêtent sur ce type d'activités. Dans la plupart des cas, s'il s'agissait d'une activité de nature criminelle, cette autorité serait la GRC.

En ce qui concerne l'environnement informatique, nous avons parlé de différentes mesures, et elles font partie de nos 10 meilleures. L'une des plus importantes est de maintenir les systèmes à jour et de s'assurer qu'ils sont continuellement améliorés. C'est un domaine où nous devrons nous appliquer relativement à la prochaine génération de technologies. La sécurité devra être intégrée dès le départ. La sécurité n'est pas quelque chose que l'on boulonne autour des systèmes; elle est intégrée tout au long du processus. Lorsque M. Brouillard parlait du processus d'identité numérique, la sécurité était pensée dès le départ, avant qu'un seul morceau de code ne soit écrit ou qu'une simple application ne soit achetée. C'est ce que nous devons faire à l'avenir.

**Le président:** Merci, monsieur Jones et madame Vignola.

Nous allons maintenant passer à M. Green pour deux minutes et demie.

**M. Matthew Green:** Merci.

Le 25 mai 2020, M. Glover a déclaré au Comité qu'au cours des 10 premières semaines de la pandémie, il n'y avait pas eu d'incidents constituant une atteinte à la sécurité des données. Cependant, au cours de la même période, des incidents ont été interceptés tous les jours, mais aucun d'eux n'a porté à conséquence.

Comment la situation a-t-elle évolué depuis mai de l'année dernière? Y a-t-il eu des incidents préjudiciables pour les données?

Je crois que cette question s'adresse au dirigeant principal de l'information, M. Brouillard.

● (1635)

**M. Marc Brouillard:** Monsieur le président, à ma connaissance, il n'y a pas eu d'atteintes importantes aux données liées à la cyberactivité depuis le début de la pandémie. Il y a cette injection forcée de justificatifs d'identité de l'été dernier, qui, comme l'a dit M. Jones, n'était pas une violation de nos systèmes. C'était plutôt des gens qui accédaient au système avec des justificatifs frauduleux. Cela devient en fait une question de fraude et non de cybersécurité.

Certains autres problèmes dont nous avons parlé aujourd'hui — SolarWinds, la vulnérabilité de Microsoft Exchange, certaines vulnérabilités de tiers — ont été corrigés. Ils ont été corrigés, mais il n'y a pas eu d'atteintes significatives à la sécurité des données.

**M. Matthew Green:** Y a-t-il eu des interceptions qui ont porté à conséquence? Dans l'affirmative, combien et quand?

**M. Marc Brouillard:** Je suis désolé. Pouvez-vous définir « interception », comme dans...

**M. Matthew Green:** Eh bien, M. Glover a dit que des incidents étaient interceptés tous les jours, mais qu'aucun n'avait eu de conséquences. Je crois comprendre ce que cela signifie, mais je ne veux pas...

**M. Marc Brouillard:** En ce qui concerne les aspects techniques, peut-être que M. Perron ou M. Jones aimerait intervenir.

**M. Matthew Green:** S'agit-il d'une opération de type « déni de service »?

**M. Marc Brouillard:** Qu'ils les arrêtent, oui.

**M. Sony Perron:** Je peux peut-être ajouter qu'au cours des 10 premières semaines de la pandémie, le système a eu des difficultés à s'adapter à l'accès à distance et qu'il n'y avait pas assez de connexions. Lorsque nous sommes arrivés à la fin du mois de mai et au mois de juin de l'année dernière, la capacité de l'accès à distance sécurisé avait été augmentée, et ces interceptions avaient donc cessé.

Vous avez peut-être remarqué qu'au moment où M. Glover parlait, nous parlions aussi de la situation où nous demandions aux employés de n'utiliser le système qu'à certaines heures de la journée. Nous avons réglé ce problème pendant l'été en augmentant la capacité de l'accès à distance sécurisé.

J'insiste sur les mots « accès à distance sécurisé ». L'idée n'est pas de donner un accès. Il s'agit de donner un accès à distance sécurisé, c'est-à-dire de permettre à nos employés de travailler depuis leur domicile sans que cela ne fasse augmenter les risques pour le réseau et les activités du gouvernement. Aujourd'hui, nous sommes en mesure de fournir 290 000 connexions simultanées, et nous avons répondu à toutes les demandes d'augmentation de capacité des ministères.

En ce qui concerne ces situations qui avaient cours dans les premières semaines de la pandémie, avec un travail acharné et une collaboration entre les parties, nous avons pu mettre en place des solutions qui ont permis à des centaines de milliers d'employés fédéraux de travailler de la maison.

**Le président:** Merci, monsieur Perron et monsieur Green.

Nous allons maintenant passer à Mme Harder, pour cinq minutes.

**Mme Rachael Harder (Lethbridge, PCC):** Monsieur Perron, ma question s'adresse à vous.

Services partagés Canada est responsable de tout l'approvisionnement en matière de TI. Nous parlons de courriels, de téléphone, de centres de données informatiques pour l'ensemble du gouvernement du Canada. Compte tenu de votre rôle, pouvez-vous dire au Comité s'il existe ou non une interdiction d'acheter de la technologie Huawei pour quelque ministère que ce soit au sein du gouvernement du Canada?

**M. Sony Perron:** Monsieur le président, il y a un processus qui s'appelle le processus d'intégrité de la chaîne d'approvisionnement qui est géré par le Centre de la sécurité des télécommunications. Services partagés Canada soumet à cet organisme les activités d'approvisionnement auprès des fournisseurs ou les nouveaux produits envisagés afin qu'il en fasse l'examen du point de vue de la sécurité et qu'il formule des conseils appropriés en la matière. Avant que Services partagés Canada ne prenne une décision, ce n'est pas seulement le produit ou le service qui doit être examiné, mais aussi la façon dont le service est construit et fourni.

Sur ce point, si vous êtes d'accord, monsieur le président, nous allons demander à M. Jones d'expliquer en quoi consistent ces évaluations.

**Mme Rachael Harder:** Permettez-moi d'intervenir une seconde.

Je ne veux pas un résumé global du processus d'évaluation. Je cherche en fait une réponse assez simple. Je veux savoir s'il est interdit au gouvernement du Canada de se procurer de la technologie Huawei pour assurer la prestation de services gouvernementaux, quels qu'ils soient.

**M. Sony Perron:** D'accord. Je vais essayer d'être un peu plus clair.

Nous n'avons pas de technologie Huawei en service sur notre réseau à l'heure actuelle. Si un fournisseur proposait d'avoir recours à cette technologie, cela ferait partie de l'ensemble qui serait examiné dans le cadre du processus d'intégrité de la chaîne d'approvisionnement et, en vertu de ce processus, le Centre de la sécurité des télécommunications serait appelé à donner son avis.

À l'heure actuelle, nous n'avons pas acheté... nous n'utilisons pas la technologie Huawei sur le réseau du gouvernement du Canada.

**Mme Rachael Harder:** Je comprends que vous ne fassiez pas cela en ce moment, mais y a-t-il une politique en place pour nous protéger contre toute acquisition future de la technologie Huawei?

**M. Sony Perron:** En ce qui concerne les politiques, lorsque nous acquérons des services ou des technologies, nous passons par le processus d'intégrité de la chaîne d'approvisionnement. Nous demandons l'avis du Centre de la sécurité des télécommunications avant d'aller de l'avant. Il existe un processus intégré pour évaluer l'intégrité de la chaîne d'approvisionnement et pour s'assurer que nous prenons les meilleures décisions pour soutenir les opérations gouvernementales et les services destinés aux Canadiens. C'est ce que l'on appelle le processus d'intégrité de la chaîne d'approvisionnement.

● (1640)

**Mme Rachael Harder:** Ce que j'entends de votre part, c'est que Services partagés Canada serait ouvert à la possibilité de se procurer de la technologie Huawei. Est-ce bien cela?

**M. Sony Perron:** Ce que je veux dire, c'est que chaque fois que nous achetons de nouveaux produits ou de nouveaux appareils, nous suivons le processus d'intégrité de la chaîne d'approvisionnement qui a été mis en place pour évaluer ces transactions.

**Mme Rachael Harder:** Cette chaîne d'approvisionnement dont vous parlez, cette intégrité, il n'y a rien là-dedans qui empêcherait la mise en service de la technologie Huawei ici au Canada.

**M. Sony Perron:** Monsieur le président, pour répondre à la question de la députée, ce processus est géré par le Centre de la sécurité des télécommunications, alors je pense que M. Jones serait mieux placé que moi pour en décrire les étapes et le déroulement.

**Mme Rachael Harder:** Je vais permettre à M. Jones de nous dire de quoi il retourne.

**M. Scott Jones:** Dans le cadre des contrôles de l'intégrité de la chaîne d'approvisionnement, nous vérifions un certain nombre de choses — le type d'équipement, la vulnérabilité, le contrôle et l'influence de la propriété étrangère, et bien d'autres aspects. Ensuite, nous déterminons une cote de risque. Si la cote de risque est trop élevée, le ministère — dans ce cas-ci Services partagés Canada — prendra la décision d'accepter ou de rejeter le produit. En cas de rejet, le ministère se chargera de trouver un autre type de produit. Comme nous procédons produit par produit, nous examinons toujours la situation dès le départ afin de respecter les règles relatives aux accords commerciaux, etc. et de donner les meilleurs conseils possible à Services partagés Canada.

L'objectif pour nous est de nous assurer que nous fournissons une évaluation complète et détaillée du risque de la chaîne d'approvisionnement afin que les ministères puissent prendre leurs décisions.

**Mme Rachael Harder:** Merci.

Pour répondre à ma question précise, en ce qui concerne Huawei, nous avons des preuves concrètes d'espionnage, d'infiltration et d'ingérence systématique de la Chine dans les entreprises canadiennes et au sein du gouvernement fédéral. Cela semble être un risque assez élevé pour ce qui est de l'évaluation des risques dont vous parlez, qui comprend la propriété étrangère, et puis, bien sûr, le risque que ce type de technologie poserait aux Canadiens et à l'État.

Est-ce que Huawei fait l'objet de discussions? Les cinq du Groupe des cinq ont tous interdit la technologie Huawei ou ont établi des protocoles très rigoureux quant à son utilisation. Le Canada va-t-il dans cette direction? Tenez-vous compte de cela? Cela va-t-il faire partie de la politique à venir?

**M. Scott Jones:** Comme l'a dit M. Perron, le gouvernement du Canada n'utilise aucune technologie Huawei sur ses réseaux. Nous soumettons nos achats d'équipement, tout équipement acheté, à notre processus d'intégrité de la chaîne d'approvisionnement.

**Mme Rachael Harder:** Je suis désolée. Cela ne répond pas à ma question. Est-ce qu'un processus est en train d'être mis en place pour protéger les Canadiens et l'État des risques qui pèsent sur les renseignements sensibles qui sont dans nos systèmes de données? Y a-t-il une initiative mise en place pour s'assurer que la technologie Huawei ne soit pas utilisée dans des projets futurs?

**M. Scott Jones:** Le processus d'intégrité de la chaîne d'approvisionnement est là pour garantir que toutes les décisions prises le sont pour assurer la sécurité des renseignements des Canadiens et des réseaux canadiens et des réseaux du gouvernement du Canada, c'est-à-dire de Services partagés Canada dans le cas qui nous occupe.

**Le président:** Merci, madame Harder.

Nous allons maintenant passer à M. Drouin, pour cinq minutes.

**M. Francis Drouin (Glengarry—Prescott—Russell, Lib.):** Merci, monsieur le président.

Je tiens à remercier les témoins qui ont comparu devant le Comité.

J'aimerais revenir sur l'intégrité de la chaîne d'approvisionnement. Monsieur Perron, depuis combien de temps cette intégrité de la chaîne d'approvisionnement est-elle en place?

**M. Sony Perron:** Vous me posez une question qui demande des connaissances historiques. Je ne suis pas à Services partagés Canada depuis assez longtemps pour répondre à cette question et vous donner une date.

Je pense que M. Jones ou M. Brouillard pourra sans doute nous donner la date où ce processus a été créé.

**M. Marc Brouillard:** À moins que M. Jones ne connaisse la date exacte, je crois qu'il faudra vous revenir là-dessus. Je sais que cela existe depuis de nombreuses années. Je suis ici depuis 2016, mais je ne pourrais pas vous donner de date exacte.

**M. Francis Drouin:** D'accord.

Monsieur Jones, c'est à vous.

**M. Scott Jones:** Le programme officiel coïncide avec la mise en place initiale de Services partagés Canada, mais la prestation de conseils sur l'intégrité de la chaîne d'approvisionnement a débuté bien avant cela, dans les années qui ont précédé cette mise en place et avant mon implication dans la cybersécurité, il y a 14 ou 15 ans.

Le programme officiel a vraiment commencé avec Services partagés Canada. Idem pour la présence d'un point central pour le travail qui se fait en matière d'approvisionnement et sur ces grands projets.

● (1645)

**M. Francis Drouin:** D'accord.

Je veux juste m'assurer de bien comprendre. N'importe quelle entreprise — et peu importe qu'il s'agisse de Huawei ou de qui que ce soit d'autre — peut participer à un marché. Sauf qu'une fois que ce qu'elle offre est passé par le processus d'intégrité de la chaîne d'approvisionnement, on peut revenir à elle et lui dire: « Désolé, mais votre sécurité ne passe pas la rampe, donc vous ne pouvez pas participer. » Est-ce là l'objectif?

**M. Sony Perron:** Exactement. Il s'agit aussi de nous assurer que nous ne regardons pas seulement la surface. Le processus fait un examen en profondeur. Qu'est-ce qui se cache derrière? Qu'est-ce qui se cache derrière sur le plan technologique?

Parfois, nous achetons des services. Ces fournisseurs de services auront leurs propres technologies et leurs propres infrastructures. Celles-ci doivent être transparentes. Les renseignements à cet égard sont fournis au Centre de la sécurité des télécommunications par les soumissionnaires au moyen du processus, et c'est le centre qui en fait l'évaluation. Nous nous appuyons sur cet avis pour prendre une décision définitive en matière d'approvisionnement.

**M. Francis Drouin:** D'accord.

Une entreprise canadienne pourrait sembler sécuritaire a priori et tout ce qu'on voudra, mais il se peut que ses propres fournisseurs soient à risque ou qu'ils utilisent des technologies compromettantes. C'est là tout l'intérêt du processus d'intégrité de la chaîne d'approvisionnement.

**M. Sony Perron:** C'est l'assurance que Services partagés Canada recherche à travers ce processus. Il s'agit de s'assurer que ceux qui ont l'expertise et les connaissances vont suivre le processus et effectuer ce genre d'évaluation, évaluation pour laquelle notre équipe technique n'a peut-être pas le savoir-faire voulu. Le Canada est chanceux à cet égard; nous avons ce centre avec des ressources spécialisées qui concentre 100 % de son énergie sur cette question. Il nous donne l'assurance que nous faisons le meilleur choix du point de vue de la sécurité.

**M. Francis Drouin:** Formidable. Merci.

Je vais changer de sujet.

De toute évidence, certains Canadiens ont ressenti l'impact de la fermeture de leurs comptes gouvernementaux auprès de l'ARC. Quelqu'un peut-il m'expliquer ce qui s'est passé et pourquoi le gouvernement a pris la précaution de fermer ces comptes? Quelle est la meilleure façon pour les Canadiens d'empêcher que cela se produise?

**M. Marc Brouillard:** Je peux répondre à la première partie de cette question, monsieur le président.

L'ARC a utilisé de manière proactive différentes méthodes et des tiers pour rechercher des signaux indiquant que certains comptes potentiellement compromis avaient été repérés. Encore une fois, il peut s'agir de revenir aux capacités où il y a eu des compromissions antérieures ou des listes connues d'identités suspectes. Tout ce qu'ils font, c'est désactiver les comptes. Ils contactent les utilisateurs et leur disent qu'ils ont peut-être été compromis et que cela a pu faire partie d'un autre événement susceptible d'avoir une incidence sur d'autres comptes comme leurs comptes bancaires, leurs comptes Facebook et d'autres choses de ce genre. Il s'agit d'un conseil proactif aux Canadiens pour les inciter à faire attention à leur cyberhygiène et les inviter à prendre les mesures qui s'imposent.

Pour ce qui est des comptes de l'ARC, il existe un processus qui permet de rétablir les comptes des usagers. Ils ne perdent pas leurs comptes de façon permanente. Ils doivent simplement réinitialiser leur mot de passe et rétablir leur identité.

Je laisse à M. Jones le soin d'évoquer les autres mesures de cyberhygiène que les Canadiens devraient prendre pour se protéger de façon générale lorsque cela se produit ou simplement en temps normal.

**M. Scott Jones:** Monsieur le président, je vais rapidement donner des précisions sur ce que les Canadiens peuvent faire.

La première chose est la suivante: n'utilisez pas les mêmes mots de passe sur les comptes auxquels vous tenez vraiment. En fait, ne réutilisez jamais vos mots de passe. Nous recommandons aux Canadiens d'utiliser des gestionnaires de mots de passe, qui génèrent automatiquement des mots de passe aléatoires et compliqués.

Mais pour les choses auxquelles vous tenez vraiment, utilisez des mots de passe uniques. Activez l'authentification multifactorielle. Cela signifie qu'il faut demander à l'hôte de vous envoyer un message texte lorsque vous vous branchez, qu'il faut se brancher depuis un appareil de confiance ou qu'il faut avoir de ces jetons durs pour se brancher, bien que peu de gens se servent de ces jetons parce qu'ils sont difficiles à utiliser. Quoi qu'il en soit, vous devriez activer quelque chose pour qu'il y ait une vérification.

Les questions de sécurité ne constituent pas une authentification multifactorielle. Ces renseignements ont déjà fait l'objet de vols, alors ne comptez pas sur cela comme deuxième facteur. Quand nous parlons de facteurs... C'est quelque chose que vous connaissez: votre mot de passe. C'est quelque chose que vous êtes: dans le monde physique, une empreinte digitale ou une photo ou quelque chose du genre. C'est quelque chose que vous avez. C'est là que nous parlons de la réception d'un SMS sur votre téléphone qui vous donne un code que vous devrez utiliser dans les prochaines minutes pour vous brancher, etc. C'est ce que l'on entend par « authentification multifactorielle ».

En activant ces éléments, vous devenez déjà une cible beaucoup plus difficile. Ce sont des choses simples que vous pouvez faire. J'encourage tous les Canadiens à changer les mots de passe des choses qui leur tiennent à cœur, des choses dont la compromission pourrait leur nuire en tant que citoyen. Choisissez un mot de passe difficile. Mieux encore, choisissez une phrase de passe si cela est autorisé. Prenez quelque chose que vous serez le seul à connaître, dont vous seul pourrez vous souvenir. Si vous devez l'écrire, enfermez-le quelque part et cachez-le. Ne le collez pas sous votre clavier. C'est le premier endroit où l'on regardera.

● (1650)

**M. Francis Drouin:** Formidable. Merci.

C'est tout, monsieur le président?

**Le président:** Oui, monsieur Drouin. Je vous remercie beaucoup.

Nous avons entendu d'excellentes questions et d'excellentes réponses. Je regarde l'heure en ne perdant pas de vue que nous allons bientôt devoir passer à huis clos. Si nous entamons la prochaine série de questions, cela nous amènera bien au-delà de ce point.

Je me souviendrai de ne plus mettre mon mot de passe sous mon clavier. Je vous remercie du conseil.

Cela dit, j'aimerais remercier les témoins d'avoir été là aujourd'hui, tous les cinq — bien que M. Jones, M. Perron et M. Brouillard aient répondu à toutes les questions. Nous vous en sommes reconnaissants. Vous avez indiqué que vous auriez peut-être à faire des recherches pour répondre à certaines des questions qui vous ont été posées. Si vous pouviez envoyer ces réponses au greffier, nous vous en serions grandement reconnaissants.

Nous allons maintenant mettre fin à la partie publique de cette séance et passer à huis clos. Lorsque je suspendrai la réunion, le personnel technique mettra fin à ce segment dans Zoom. Cela signifie que les membres devront se débrancher et réintégrer la séance en utilisant le code d'accès que le greffier leur a envoyé.

Je vais maintenant suspendre la réunion. Nous nous retrouverons dans quelques minutes.

[*La séance se poursuit à huis clos.*]