CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

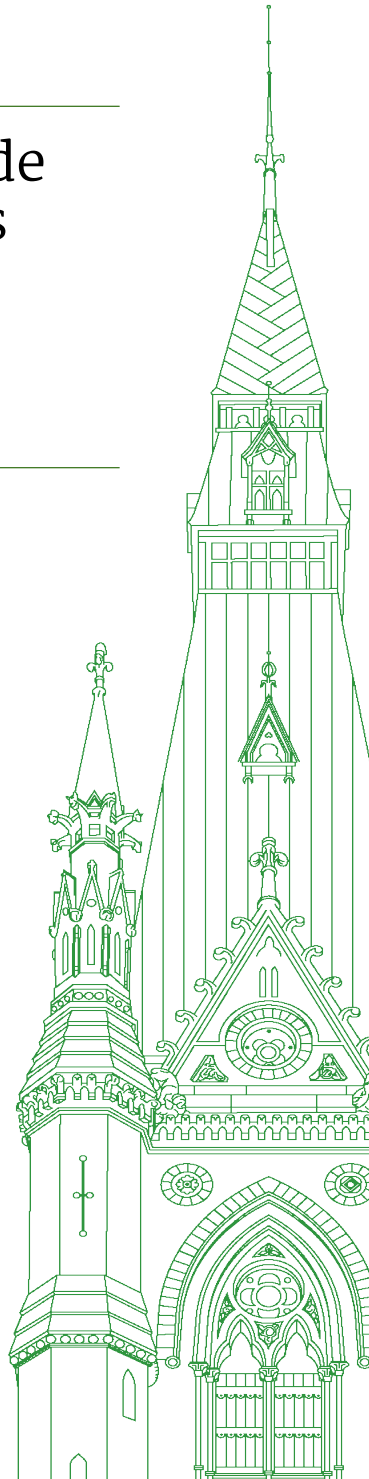
44e LÉGISLATURE, 1re SESSION

Comité permanent des transports, de l'infrastructure et des collectivités

TÉMOIGNAGES

NUMÉRO 009

Le jeudi 24 mars 2022



Président : M. Peter Schiefke

Comité permanent des transports, de l'infrastructure et des collectivités

Le jeudi 24 mars 2022

● (1530)

[*Français*]

Le président (M. Peter Schiefke (Vaudreuil—Soulanges, Lib.)): J'ouvre maintenant la séance.

Bienvenue à la réunion numéro 9 du Comité permanent des transports, de l'infrastructure et des collectivités.

La réunion d'aujourd'hui se déroule sous forme hybride, conformément à l'ordre de la Chambre adopté le jeudi 25 novembre 2021. Les membres du Comité peuvent participer en personne ou avec l'application Zoom.

Je profite de l'occasion pour rappeler à tous les participants et observateurs à cette réunion qu'il n'est pas permis de faire des captures d'écran ou de prendre des photos de leur écran.

Compte tenu de la situation actuelle de pandémie, j'encourage tous les membres du Comité et tous les témoins à suivre les recommandations des autorités sanitaires, ainsi que la directive du Bureau de régie interne du 28 janvier 2022.

[*Traduction*]

À titre de président, je veillerai de mon mieux au respect de ces mesures pendant la séance, et je remercie à l'avance les membres du Comité de leur collaboration.

Conformément à l'article 108(2) du Règlement et à la motion adoptée par le Comité le jeudi 3 mars 2022, le Comité se réunit pour étudier l'état de préparation du Canada aux menaces posées par la Russie visant les eaux, les ports et l'espace aérien du Canada.

Honorables collègues, nous recevons aujourd'hui Denis Vinette, vice-président de la Direction générale des voyageurs, de l'Agence des services frontaliers du Canada; Rajiv Gupta, dirigeant associé du Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications; et Ryan Schwartz, directeur général intérimaire de la Direction des infrastructures essentielles du Secteur de la sécurité nationale et de la cybersécurité, du ministère de la Sécurité publique et de la Protection civile.

Pendant la deuxième partie de notre séance, nous entendrons M. John de Boer, directeur principal aux Affaires gouvernementales et politiques publiques, Canada, de BlackBerry.

Je souhaite la bienvenue à tous nos témoins devant le Comité aujourd'hui.

Je céderai la parole à nos témoins pour qu'ils fassent leurs exposés.

Monsieur Denis Vinette, vous avez la parole.

M. Denis Vinette (vice-président, Direction générale des voyageurs, Agence des services frontaliers du Canada): Je vous remercie et vous souhaite un bon après-midi à tous.

[*Français*]

Bonjour, monsieur le président et membres du Comité permanent des transports, de l'infrastructure et des collectivités.

Je vous remercie de m'avoir invité à participer à la discussion aujourd'hui.

Je suis heureux d'être ici pour répondre à vos questions sur le rôle de l'Agence des services frontaliers du Canada, ou ASFC, en ce qui a trait à l'arrivée de ressortissants ukrainiens au Canada et aux sanctions à la Russie.

L'ASFC est responsable de faciliter le flux des voyages et des échanges commerciaux légitimes au Canada. Son rôle est d'évaluer le risque pour la sécurité et l'admissibilité des personnes qui viennent au Canada. Toutes les personnes, y compris les citoyens canadiens, qui cherchent à entrer au Canada doivent se présenter à l'ASFC et peuvent être soumises à un examen plus approfondi. L'admissibilité de tous les voyageurs est décidée au cas par cas et en fonction de l'information disponible au moment de l'entrée.

L'ASFC s'engage à protéger la santé et la sécurité des Canadiens et examinera, détiendra ou saisira les marchandises entrant au Canada si elles présentent un risque pour la santé, la sécurité ou la sûreté.

Au-delà du contrôle des voyageurs, l'ASFC utilise également un certain nombre de sources d'informations préalables automatisées provenant des transporteurs et des importateurs, afin de déterminer les marchandises et les moyens de transport qui pourraient constituer une menace pour le Canada.

L'Agence utilise une approche de gestion des risques pour faciliter le commerce légitime, tout en se concentrant sur les risques plus élevés ou inconnus. Cette approche consiste à contrôler les marchandises à plusieurs points du continuum commercial: dès que possible à l'étranger, en transit et à l'arrivée à la frontière canadienne.

● (1535)

[*Traduction*]

L'Agence s'efforce d'obtenir la bonne information au bon moment, afin de savoir quand, où et comment cibler ses efforts d'exécution. Les agents de ciblage de l'ASFC travaillent en collaboration avec les agents des services frontaliers qui sont formés aux techniques d'examen, d'enquête et d'interrogation. Ensemble, ils constituent les meilleurs atouts de l'Agence lorsqu'il s'agit de déterminer, de détecter et d'intercepter la contrebande à la frontière.

En ce qui concerne les sanctions commerciales, l'ASFC appuie la réponse pangouvernementale à l'invasion russe en Ukraine et aide Affaires mondiales Canada, ou AMC, à administrer la Loi sur les mesures économiques spéciales, la Loi sur les Nations Unies, la Loi sur la justice pour les victimes de la corruption d'agents étrangers, la Loi sur les licences d'exportation et d'importation et les règlements connexes à la frontière.

L'ASFC est également un partenaire actif des Centres d'opérations de la sûreté maritime et soutient Transports Canada en lui fournissant des renseignements douaniers pertinents et opportuns.

L'ASFC travaille en étroite collaboration avec la GRC pour offrir une vaste gamme de services frontaliers, le mandat de l'ASFC étant axé sur la prestation de services aux points d'entrée.

Les agents des services frontaliers examinent aussi les documents d'importation et d'exportation comme les connaissements, les factures et les certificats d'origine afin de déterminer si les marchandises ou les expéditions et les transactions font l'objet de sanctions ou de mesures de contrôle. Les expéditions qui semblent contrevenir à la loi, aux règlements ou aux sanctions sont retenues et transmises à AMC pour une évaluation plus approfondie. Sur recommandation d'AMC, l'ASFC peut procéder à une retenue ou à une saisie pour s'assurer que tous les règlements et les sanctions applicables sont mis en œuvre aux points d'entrée.

En outre, l'ASFC effectue des évaluations des risques pour les voyageurs et les marchandises qui cherchent à entrer au Canada. L'ASFC travaille avec ses partenaires du secteur du renseignement pour effectuer des contrôles de sécurité sur les ressortissants étrangers qui souhaitent entrer au pays. Les processus de contrôle et d'évaluation des risques comprennent la collecte et l'analyse d'informations provenant de diverses sources et partenaires afin de déterminer l'admissibilité et les risques.

L'Agence échange régulièrement, selon des paramètres juridiques stricts, des renseignements pertinents sur les questions de sécurité frontalière et nationale avec ses partenaires, ainsi qu'avec d'autres ministères au Canada afin d'assurer la santé et la sécurité des Canadiens.

Toutes les marchandises, tous les moyens de transport et toutes les personnes peuvent faire l'objet d'un examen approfondi. L'ASFC évalue les risques de tous les navires et de leur cargaison afin de détecter les navires et les marchandises qui présentent un risque potentiellement plus élevé.

Nos agents exercent leur jugement professionnel dans un environnement très complexe et sont bien soutenus dans leur formation pour appliquer ces mesures. Nous travaillons en étroite collaboration avec d'autres partenaires, comme Transports Canada et la GRC, pour veiller à ce que la sécurité et les sanctions soient appliquées de manière appropriée.

Je serai heureux de répondre aux questions des membres du Comité.

[*Français*]

Merci.

[*Traduction*]

Le président: Je vous remercie beaucoup, monsieur Vinette.

Nous entendrons maintenant M. Gupta.

Monsieur Gupta, vous disposez de cinq minutes pour faire votre exposé. La parole est à vous.

[*Français*]

M. Rajiv Gupta (dirigeant associé, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Bonjour.

Monsieur le président et membres du Comité, je vous remercie de m'avoir invité à comparaître devant vous aujourd'hui pour discuter de l'état de préparation du Canada en ce qui a trait à sa capacité de contrer les menaces de la Russie qui visent les eaux, les ports et l'espace aérien du Canada.

[*Traduction*]

Je m'appelle Rajiv Gupta et je suis le dirigeant associé du Centre canadien pour la cybersécurité, communément appelé Centre pour la cybersécurité, qui relève du Centre de la sécurité des télécommunications, ou CST.

Le CST, qui relève du ministre de la Défense nationale, est l'un des principaux organismes canadiens de renseignement et l'autorité technique principale en matière de cybersécurité au pays. Le Centre pour la cybersécurité est un secteur au sein du CST et un centre d'expertise unique pour toutes les questions techniques et opérationnelles en matière de cybersécurité. Nous défendons le gouvernement du Canada, diffusons nos pratiques exemplaires pour prévenir les compromissions, assurons la gestion et la coordination des incidents d'importance et travaillons à sécuriser le Canada sur le plan numérique.

Les systèmes informatiques du Canada au sein et à l'extérieur du gouvernement contiennent de l'information et des données personnelles qui sont essentielles à la prospérité, à la sécurité et à la démocratie du pays. Les systèmes informatiques canadiens sont également très importants dans le cadre des opérations liées aux infrastructures essentielles. La protection de ces systèmes s'avère donc primordiale, et je peux vous assurer que le CST et son Centre pour la cybersécurité reconnaissent cette importance.

Je ne peux pas parler de nos opérations particulières dans le cadre de cet exposé, mais je peux confirmer que nous suivons de près les activités de cybermenace associées à l'invasion russe qui a lieu actuellement en Ukraine. Nous savons que la Russie détient des cybercapacités importantes et qu'elle les a utilisées de façon irresponsable par le passé. L'attaque par le maliciel destructeur NotPetya survenue en 2017 est un exemple de ce comportement et montre les conséquences internationales que peut avoir une cyberattaque menée contre l'Ukraine.

La situation ne cesse d'évoluer et le CST continue de surveiller l'environnement de cybermenace au Canada et dans le monde, y compris les activités de cybermenace ciblant les réseaux des infrastructures essentielles, ainsi que les systèmes opérationnels et les technologies de l'information.

Nous avons mis en place sur les réseaux du gouvernement du Canada des outils pour surveiller et détecter les menaces, enquêter sur ces dernières et prendre les mesures actives nécessaires pour les neutraliser. À l'échelle du Canada, nous avons publié des bulletins non classifiés sur les menaces pour rappeler aux exploitants des infrastructures essentielles du Canada que des risques existent et qu'ils doivent prendre des mesures d'atténuation afin de protéger les infrastructures contre les activités de cybermenace connues qui sont parrainées par la Russie.

Nous encourageons d'ailleurs fortement toutes les organisations canadiennes à agir immédiatement, à faire preuve de vigilance organisationnelle accrue et à renforcer leurs mesures de cyberdéfense en ligne. Nous invitons aussi les Canadiens à consulter le site pensezcybersecurite.gc.ca et les entreprises à visiter le site cyber.gc.ca pour en apprendre plus sur les pratiques exemplaires qu'il convient d'adopter pour se protéger contre les cybermenaces.

Sachez que les rançongiciels posent un risque important pour les organisations canadiennes. Leurs conséquences peuvent être graves et comprendre l'interruption des activités, la perte permanente de données, le vol de propriété intellectuelle, des atteintes à la vie privée et à la réputation, ainsi que des coûts de reprise élevés. Nous incitons donc les organisations canadiennes à appliquer les pratiques exemplaires présentées dans le guide sur les rançongiciels publié par le Centre pour la cybersécurité.

Outre des alertes et des conseils publics, le Centre pour la cybersécurité continue de transmettre des informations importantes sur les cybermenaces à ses partenaires des infrastructures essentielles du Canada en passant par des voies de communication protégées. Il transmet entre autres des indicateurs de compromission, des conseils en matière d'atténuation des menaces et des alertes confidentielles portant sur de nouveaux maliciels et d'autres tactiques, techniques et procédures utilisées pour cibler des victimes.

Le CST communique également des renseignements importants sur les cybermenaces à des partenaires clés du gouvernement qui appuient l'Ukraine. Il continue aussi de collaborer avec le ministère de la Défense nationale et les Forces armées canadiennes dans le cadre de mesures qui favorisent la coopération sur le plan du renseignement et qui soutiennent la cybersécurité et les cyberopérations.

● (1540)

[*Français*]

Les tensions géopolitiques continuent de monter, mais sachez que le CST travaille sans relâche pour contrer les menaces étrangères et les cybermenaces qui guettent le Canada,

[*Traduction*]

et nous continuerons de le faire.

Je répondrai volontiers à vos questions.

Je vous remercie.

Le président: Je vous remercie beaucoup, monsieur Gupta.

Monsieur le directeur général intérimaire Schwartz, vous disposez de cinq minutes pour présenter votre exposé.

M. Ryan Schwartz (directeur général intérimaire, Direction des infrastructures essentielles, Secteur de la sécurité nationale et de la cybersécurité, ministère de la Sécurité publique et de la Protection civile): Bonjour, monsieur le président et honorables membres du Comité. Je suis ravi de témoigner.

Je vous remercie de m'offrir l'occasion de traiter de l'approche qu'adopte le gouvernement du Canada en matière de sécurité et de la résilience des infrastructures essentielles.

Je commencerai en effectuant un bref retour dans le temps, en 2009, quand les ministres fédéraux, provinciaux et territoriaux responsables de la gestion des situations d'urgence ont approuvé la stratégie nationale en matière d'infrastructures essentielles, laquelle établissait une approche axée sur la collaboration au chapitre de la résilience des infrastructures essentielles prévoyant la formation de partenariats, la gestion tous risques et l'échange de renseignements.

Cette stratégie montrait la voie à suivre afin de renforcer la résilience des infrastructures essentielles contre les risques existants et émergents, et établissait la classification des infrastructures essentielles du Canada dans 10 secteurs, notamment celui des transports, et des réseaux dans chacun des secteurs.

Ces réseaux sectoriels sont gérés par un ministère fédéral responsable. Par exemple, Transports Canada s'occupe du secteur des transports. Sécurité publique Canada dirige les efforts fédéraux visant à renforcer la résilience des infrastructures essentielles. Nous ajoutons de la valeur aux partenariats entre les secteurs public et privé en réunissant des acteurs au sein du forum intersectoriel national et d'autres mécanismes de mobilisation.

Sécurité publique Canada dirige également l'élaboration des politiques fédérales en matière de cybersécurité, notamment celle initialement publiée en 2010 et mise à jour en 2018. Le gouvernement s'est engagé à renouveler la cyberstratégie dans une lettre de mandat datée de décembre 2021.

C'est dans ce contexte que nous collaborons avec nos partenaires étrangers afin d'établir un ordre international fondé sur des règles dénonçant les activités malveillantes au besoin, comme le Canada l'a fait en janvier lors du prélude à l'invasion russe en Ukraine, condamnant la cyberattaque menée contre les systèmes du gouvernement ukrainien et la campagne de peur visant le peuple ukrainien.

Le gouvernement du Canada, y compris Sécurité publique Canada, prennent des mesures pour que les Canadiens, et particulièrement les propriétaires et les exploitants d'infrastructures essentielles, soient au fait des cybermenaces, y compris celles posées par des acteurs soutenus par la Russie.

Sécurité publique Canada et d'autres ministères et organismes collaborent étroitement avec des alliés et des partenaires pour établir une compréhension commune de la menace que posent les acteurs malintentionnés et pour faire en sorte que nous soyons préparés à réagir si des systèmes informatiques canadiens sont ciblés. C'est particulièrement important au regard de l'interconnectivité des infrastructures essentielles d'aujourd'hui.

Sécurité publique Canada dirige en outre des travaux menés avec des partenaires fédéraux sur les politiques de sécurité nationale, notamment pour contrer les activités hostiles d'acteurs étatiques et les menaces de nature économique à la sécurité nationale.

Pour ce qui est des programmes et des initiatives précis, Sécurité publique Canada réalise des évaluations de la résilience et des impacts, et mène des exercices et des travaux physiques et cybernétiques avec le Centre canadien pour la cybersécurité afin d'échanger des renseignements avec des partenaires de l'industrie sur les cyberrisques et les mesures d'atténuation.

Nos évaluations de l'impact sur les infrastructures essentielles appuient la prise de décisions et permettent de connaître la situation au chapitre des menaces et des risques. Elles tiennent compte de l'effet domino qui peut perturber la distribution de biens et services dans les chaînes d'approvisionnement du Canada. À cet égard, la dépendance est forte à l'égard des ports dans tous les secteurs ayant des infrastructures essentielles.

Des évaluations tous risques sont réalisées dans le cadre du Programme d'évaluation de la résilience régionale au Canada. Les gouvernements et l'industrie travaillent ainsi de manière tangible pour examiner les vulnérabilités, mettre en œuvre des mesures correctrices et améliorer la résilience. Depuis 2012, nous avons mené des centaines d'évaluations dans des infrastructures essentielles du Canada, notamment dans des réseaux de distribution d'électricité, de vastes réseaux de transport et des ports.

En juin 2020, Sécurité publique Canada, conjointement avec le Centre canadien pour la cybersécurité, a lancé l'outil canadien de cybersécurité, réagissant ainsi à l'augmentation du nombre de cyberincidents ciblant le secteur de la santé. Conçu expressément pour les propriétaires et les exploitants canadiens d'infrastructures essentielles, cet outil d'auto-évaluation virtuel prend la forme d'un bref sondage qui fait le portrait de la résilience opérationnelle et de l'état de la cybersécurité d'une organisation.

Les maliciels, et particulièrement les rançongiciels, ont frappé des infrastructures physiques comme des pipelines, des centrales électriques, des usines de traitement des eaux, des usines de fabrication, des réseaux de transport et des systèmes logistiques. Comme mon collègue l'a fait remarquer, le maliciel NotPetya a perturbé la logistique d'entreprises en 2017, ce qui a eu un effet domino dans des ports d'importance cruciale et d'autres plaques tournantes du secteur mondial des transports, et causé des milliards de dollars en dommages.

C'est avec ce genre d'incidents à l'esprit que Sécurité publique Canada a lancé une série d'exercices physiques et cybernétiques, auxquels près de 600 participants ont pris part en février et mars à l'occasion des activités de lancement. En outre, nous organisons un de nos symposiums trimestriels sur la sécurité des systèmes de contrôle industriel les 29 et 30 mars, auquel 900 personnes se sont inscrites.

Je m'en voudrais de ne pas souligner qu'il incombe aussi aux responsables des infrastructures critiques de protéger leurs actifs et leurs systèmes, notamment en adoptant des pratiques exemplaires en matière de cybersécurité et en préparant un plan de continuité des activités et de réaction aux situations d'urgence. En fait, la sécurité et la résilience des infrastructures essentielles sont une responsabilité partagée.

Dans l'avenir, Sécurité publique Canada entend collaborer étroitement avec les provinces et les territoires, le gouvernement fédéral et le secteur privé pour élaborer une stratégie et une approche nouvelles au chapitre de la résilience des infrastructures essentielles. Ces travaux sont en cours, l'objectif étant d'élaborer une stratégie et une approche avant-gardistes d'ici la fin de l'année prochaine.

Je conclurai en soulignant que nous sommes déterminés à travailler avec des partenaires pour renforcer et améliorer la sécurité et la résilience des infrastructures essentielles au Canada, notamment en contrant les cybermenaces qui ciblent nos actifs et nos systèmes les plus cruciaux.

Je vous remercie beaucoup du temps que vous m'accordez. Je répondrai avec plaisir à vos questions.

● (1545)

Le président: Merci beaucoup pour vos déclarations préliminaires, messieurs.

Aujourd'hui, c'est M. Jeneroux qui lancera la période de questions.

Monsieur Jeneroux, vous disposez de six minutes. La parole est à vous.

M. Matt Jeneroux (Edmonton Riverbend, PCC): Je vous remercie, monsieur le président.

Je remercie les témoins de prendre le temps de se joindre à nous en ce jeudi après-midi.

Monsieur Gupta, j'aimerais vous inviter à nous en dire plus sur la communication de renseignements avec le gouvernement, comme vous avez offert de le faire. Je veux comprendre le processus. En cas d'incident, communiquez-vous directement avec le ou la ministre? La communication se fait-elle par l'intermédiaire d'un contact au sein du ministère intéressé?

Je vous serais reconnaissant de nous donner plus de détails à ce sujet.

M. Rajiv Gupta: Certainement.

Je présume que vous parlez d'incidents qui surviennent au sein du gouvernement, mais je vous prie de préciser, si vous le voulez.

M. Matt Jeneroux: Oui, exactement.

M. Rajiv Gupta: Au sein du gouvernement, le Centre canadien pour la cybersécurité fait de la surveillance auprès des ministères. Nous avons divers outils de détection. Nous surveillons les réseaux, les serveurs, le nuage. Nous recueillons des renseignements et nous les analysons. Nous prenons des mesures automatisées pour défendre le gouvernement.

Il arrive que quelque chose nous échappe et qu'un incident se produise. En pareil cas, nous avons une boîte de réception partagée que tous les ministères peuvent utiliser pour nous en aviser. Sinon, c'est généralement nous qui informons les ministères qu'un incident est survenu. Ensuite, nous en évaluons la gravité.

Si nous pensons que l'incident risque d'aller au-delà du simple contrôle d'un seul ministère, nous enclenchons le processus prévu dans le PGEC GC, le Plan de gestion des événements de cybersécurité, qui relève du SCT. Divers intervenants participent à ce processus, les principaux étant la triade formée par le CCC — le Centre canadien pour la cybersécurité —, le Conseil du Trésor et Services partagés Canada. Le Plan prévoit un processus très structuré de signalisation progressive en ce qui a trait à la communication aux différents paliers et à la mobilisation des divers ministères.

● (1550)

M. Matt Jeneroux: Le processus est-il enclenché immédiatement? Un incident survient et...

M. Rajiv Gupta: Tout dépend de l'évaluation. Si l'incident est grave, le processus peut être enclenché moins d'une heure après...

M. Matt Jeneroux: C'est intéressant.

Les ministres concernés sont-ils aussi avisés de l'incident, ou la communication se fait-elle par l'intermédiaire du système de commandement, et c'est alors aux gens du ministère d'informer leur ministre?

M. Rajiv Gupta: C'est fait par l'intermédiaire du système de commandement, c'est-à-dire du PGEC GC. Le Plan précise qui doit recevoir une notification selon le niveau d'intervention et la gravité de l'incident.

M. Matt Jeneroux: La Russie a-t-elle fait des tentatives d'infiltration cybernétique visant les eaux, les ports et l'espace aérien du Canada en 2022?

M. Rajiv Gupta: Nous ne sommes au courant d'aucun incident de ce genre.

M. Matt Jeneroux: Pouvez-vous nous dire s'il y a des enquêtes en cours sur de telles tentatives?

M. Rajiv Gupta: Je ne peux pas parler au Comité de nos opérations particulières. C'est tout ce que je peux vous dire.

M. Matt Jeneroux: D'accord.

Votre organisme recommande aux organisations de signaler toute occurrence de comportement inattendu ou inhabituel sur leur réseau. Combien de signalements avez-vous reçus depuis que la Russie a envahi l'Ukraine, autrement dit au cours du dernier mois?

M. Rajiv Gupta: Je ne connais pas le chiffre exact. Nous faisons le total des signalements chaque semaine et nous les regroupons. Le Centre canadien pour la cybersécurité reçoit toutes sortes de signalements...

M. Matt Jeneroux: Le chiffre est-il dans les centaines, les milliers, les millions?

M. Rajiv Gupta: Le chiffre est probablement dans les centaines, ou il est inférieur à 100 par semaine, normalement. Nous les classons ensuite par secteur et par gravité.

Je tiens à souligner que oui, nous sommes la porte principale pour le Canada. Nous encourageons toutes les organisations d'un océan à l'autre à communiquer avec nous. Nous sommes là pour les aider. Nous tenons vraiment à ce qu'elles signalent les incidents afin que nous ayons un portrait juste de la situation. Cependant, les chiffres que je vous donne ne reflètent pas nécessairement la réalité, car nous croyons que le nombre de signalements est inférieur au nombre d'incidents.

M. Matt Jeneroux: Sur les centaines de signalements, disons, que vous recevez, quelles industries sont les plus touchées? Quels types d'organisations signalent des incidents?

M. Rajiv Gupta: Nous en recevons de tous les secteurs.

M. Matt Jeneroux: Pouvez-vous me donner des exemples?

M. Rajiv Gupta: Voulez-vous dire des exemples de secteurs et de résultats précis?

M. Matt Jeneroux: Oui, des exemples de secteurs.

M. Rajiv Gupta: Les signalements proviennent de tous les secteurs du gouvernement. Nous en recevons du secteur des finances... et aussi de tous les secteurs mentionnés par Sécurité publique...

M. Matt Jeneroux: Il faut qu'il y ait un lien avec le Canada. Sont-ils... D'où...

M. Rajiv Gupta: Oui, vous avez parfaitement raison. Nous examinons les incidents survenus au Canada et signalés par des organisations canadiennes. C'est le mandat du Centre canadien pour la cybersécurité.

M. Matt Jeneroux: Au cours du dernier mois, vous avez reçu des centaines de signalements. Est-ce plus que durant les trois dernières années ou est-ce comparable au nombre habituel?

M. Rajiv Gupta: Pour les trois dernières années, je ne pourrais pas vous le dire, mais les chiffres n'ont rien d'inhabituel. Les cybermenaces sont une réalité depuis des années, et il y en a toujours eu au Canada. Je tiens à insister sur ce fait. Nous avons publié des évaluations des cybermenaces pesant sur le Canada en 2018, en 2020... Nous faisons régulièrement face à des cybermenaces. Elles ont tendance à évoluer avec le temps.

Comme les signalements ne sont pas entre nos mains, je ne veux pas trop m'appuyer sur eux pour analyser la tendance générale, mais je peux vous dire que nous n'avons rien constaté d'anormal jusqu'à maintenant. Je pense que...

M. Matt Jeneroux: Je vais consacrer mes 30 dernières secondes — il me reste très peu de temps — à l'ASFC et à Sécurité publique.

Depuis 2015, combien d'employés ont été relevés de leurs fonctions en raison de leur participation apparente ou réelle à des activités d'ingérence étrangère? Si la réponse est zéro, combien d'enquêtes sont en cours?

M. Denis Vinette: Je peux commencer.

Je ne suis au courant d'aucun cas pareil. Il faudrait que je m'informe. Normalement, ces enquêtes sont réalisées par la GRC. La GRC serait probablement la mieux placée pour parler de toute activité s'apparentant à une menace interne qui se serait déroulée à l'ASFC et qui aurait fait l'objet d'une enquête.

Le président: Merci beaucoup, monsieur Vinette.

Monsieur Chahal, la parole est à vous. Vous disposez de six minutes.

M. George Chahal (Calgary Skyview, Lib.): Je vous remercie, monsieur le président.

D'abord, je tiens à remercier tous les témoins pour leurs exposés et leur présence.

Mes premières questions s'adressent à M. Gupta. À votre connaissance, d'où provient la majorité des cyberattaques ou des tentatives de cyberattaques visant le Canada?

● (1555)

M. Rajiv Gupta: Les cyberattaques peuvent provenir de partout dans le monde. Leur provenance apparente n'est pas nécessairement leur provenance réelle. Les auteurs de menaces tentent toujours de dissimuler d'où elles proviennent.

Dans nos évaluations des cybermenaces de 2018 et 2020, nous avons parlé des principales menaces qui pèsent sur le Canada. La première est la cybercriminalité. Les cybercriminels sont nombreux et divers; à nos yeux, ils représentent la plus grande menace. Nous avons aussi attiré l'attention sur les programmes parrainés par la Chine, la Russie, la Corée du Nord et l'Iran. D'après nous, ce sont les menaces les plus importantes auxquelles le Canada fait face.

M. George Chahal: Quels pays se défendent le mieux contre les cyberattaques? Qu'ont-ils à nous apprendre? Pouvez-vous nous donner des exemples précis?

M. Rajiv Gupta: Je ne sais pas si une évaluation sérieuse a été faite pour déterminer quels pays se défendent le mieux. Je sais que le programme de cyberdéfense du gouvernement du Canada est assez efficace. D'autres pays s'en sont servi comme modèle. Des technologies canadiennes sont utilisées ailleurs dans le monde, par exemple au Royaume-Uni, qui a déclaré publiquement avoir mis en place certains systèmes technologiques canadiens.

J'estime que nous avons un programme de bonne qualité. Nous collaborons étroitement avec nos partenaires du Groupe des cinq; nous échangeons de l'information avec eux afin de nous assurer que le Canada compte parmi les meilleurs pays au monde dans ce domaine.

M. George Chahal: Nous considérez-vous comme un chef de file mondial en matière de cyberdéfense?

M. Rajiv Gupta: À l'échelle du gouvernement du Canada, je dirais que oui.

M. George Chahal: Très bien, je vous remercie.

Monsieur Schwartz, durant votre déclaration, vous avez parlé des évaluations de la sécurité publique et des répercussions sur les réseaux de transport, les ports et les réseaux électriques. Des pirates informatiques parrainés par la Russie ont-ils déjà attaqué ou tenté d'attaquer les infrastructures de transport du Canada ou d'autres pays?

M. Ryan Schwartz: Monsieur le président, comme la question porte sur les opérations, il faudrait que je la renvoie à mon collègue du Centre canadien pour la cybersécurité, étant donné le mandat de ce centre et le type d'activités qu'il surveille.

Malheureusement, je ne suis pas en mesure de vous donner une réponse détaillée.

M. George Chahal: Pouvez-vous nous en dire plus sur les évaluations que vous avez réalisées et le travail que vous avez fait dans ces secteurs? C'est un sujet que vous avez abordé.

M. Ryan Schwartz: Certainement.

Nous avons deux programmes. J'ai mentionné le Programme d'évaluation de la résilience régionale, le PERR. Ce programme évalue la sécurité physique et la cybersécurité. Les installations des 10 secteurs d'infrastructures essentielles de toutes les régions du pays y ont accès. Comme je l'ai déjà dit, de nombreuses installations d'infrastructures essentielles ont fait l'objet d'évaluations dans le cadre de ce programme. Le PERR comprend une évaluation approfondie de la sécurité physique qui se penche sur l'approche traditionnelle de type « gardiens, barrières et armes ». Nous utilisons une série de 1 500 questions pour discuter avec les propriétaires et les exploitants d'installations d'infrastructures essentielles.

À cela s'ajoute ce qu'on appelle l'examen de la cyberrésilience du Canada. Il s'agit d'une série de questions portant sur les pratiques exemplaires et la situation en matière de cybersécurité. De plus, cette année, nous avons mis en place un nouvel outil d'analyse de la résilience de la sécurité du réseau. Cet outil se branche au réseau de l'installation pour en détecter les faiblesses et les vulnérabilités. Le Centre canadien pour la cybersécurité l'utilise aussi. Nous collaborons avec lui à cet égard.

En outre, nous effectuons des évaluations des répercussions sur les infrastructures essentielles, dans le cadre desquelles nous examinons les effets en cascade sur l'ensemble des secteurs. Je le répète, notre approche tient compte de tous les risques. En cas de séisme, d'inondation ou de tout autre type de perturbation — les barrages sont un bon exemple récent —, nous examinons la nature de la menace ou du risque. Ensuite, nous réfléchissons à l'effet domino, pour ainsi dire, de la perturbation sur les autres secteurs, aux interdépendances et, au bout du compte, à l'incidence de la perturbation sur la population canadienne et les infrastructures essentielles qui lui fournissent des services.

M. George Chahal: Je vous remercie.

Monsieur Gupta, souhaitez-vous répondre à la question? Des pirates informatiques parrainés par la Russie ont-ils déjà attaqué ou tenté d'attaquer les infrastructures de transport ou les infrastructures portuaires du Canada ou d'autres pays?

● (1600)

M. Rajiv Gupta: Je ne suis au courant d'aucun incident visant les ports.

M. George Chahal: Et les infrastructures de transport?

M. Rajiv Gupta: Les infrastructures de transport, c'est plutôt vaste. Il faudrait que je fouille ma mémoire pour me rappeler les incidents précis.

M. George Chahal: Je vous remercie.

Monsieur le président, je crois que mon temps de parole est écoulé.

Le président: Merci beaucoup, monsieur Chahal.

[*Français*]

Je donne maintenant la parole à M. Barsalou-Duval.

Vous avez six minutes.

M. Xavier Barsalou-Duval (Pierre-Boucher—Les Patriotes—Verchères, BQ): Merci, monsieur le président.

Ma première question s'adresse à M. Vinette, de l'Agence des services frontaliers du Canada.

Le gouvernement a annoncé une série de sanctions contre la Russie à la suite de l'invasion par celle-ci de l'Ukraine. Est-ce que certaines de ces sanctions ont eu une incidence sur votre travail? De quelle façon avez-vous ajusté vos façons de faire depuis?

M. Denis Vinette: Je vous remercie de cette question.

Nous vérifions toujours si des individus ou des marchandises commerciales qui arrivent au pays sont visés par les sanctions déjà en vigueur contre l'Iran, la Corée du Nord et d'autres pays. Nous tenons compte des nouvelles sanctions du ministère des Affaires étrangères qui sont venues s'ajouter aux sanctions existantes.

Nous avons transmis des directives à nos agents pour nous assurer qu'ils sont bien au fait des nouvelles sanctions imposées. Cela leur permettra de déterminer si des navires, des avions ou des marchandises arrivant au Canada y sont assujettis. Si tel était le cas, nous communiquerions avec les Affaires étrangères pour déterminer s'il faut les saisir ou leur refuser l'entrée au Canada.

Nous avons mis des mesures en place, mais l'effet immédiat n'est pas très grand, puisqu'il y a peu de marchandises, de navires ou d'autres avions qui arrivent au pays en raison des restrictions actuelles de Transports Canada.

M. Xavier Barsalou-Duval: Cette semaine, notre comité a reçu des gens de NAV CANADA et le ministre de Transports Canada au sujet, notamment, de l'interdiction de vol des avions russes dans l'espace aérien canadien.

Nous avons compris qu'il y avait eu de la confusion quant aux indications données. Il semblerait que les vols humanitaires étaient inclus, mais que ce n'était pas clair dans ce qu'avait dit Transports Canada au départ. Cela a permis à un faux vol humanitaire — du moins, qu'on prétend faux, l'enquête n'étant pas terminée — de survoler notre espace malgré l'interdiction.

De votre côté, avez-vous dû composer avec des indications imprécises? Auriez-vous besoin de plus de précisions à la suite des nouvelles mesures prises par le gouvernement?

M. Denis Vinette: Nous faisons un suivi régulier de tous les avions, camions et autres véhicules qui arrivent au pays. Nous travaillons avec les autres services de renseignement du Canada afin d'approfondir nos recherches, quand nous soupçonnons que des avions sur le point d'arriver au pays pourraient être visés par les sanctions. C'est quelque chose qui relève de Transports Canada, mais nous soutenons le ministère dans ses efforts en procédant à une vérification plus approfondie. Quand nous avons des soupçons, nous l'avisons qu'il doit faire une enquête sur l'incident en question.

M. Xavier Barsalou-Duval: Si je vous ai bien compris, vous n'avez pas eu d'indications ou de consignes qui n'étaient pas claires pour vous.

M. Denis Vinette: Vous avez bien compris. Nous travaillons très étroitement et communiquons avec les gens de ce ministère de façon quotidienne.

M. Xavier Barsalou-Duval: L'Agence a-t-elle joué un certain rôle, lorsque des gens ont dû atterrir de façon forcée à Yellowknife? Que se passe-t-il, lorsque des citoyens russes non autorisés à être sur le territoire canadien sont forcés d'y atterrir? Comment les retourne-t-on dans leur pays, puisqu'il n'y a pas de vol vers cette destination? Comment sont-ils traités? J'imagine qu'on ne les garde pas en prison pour toujours.

M. Denis Vinette: Il y a deux volets à la réponse.

Premièrement, dans ce cas-ci, il s'agissait d'un petit avion. C'était un avion commercial, mais plus petit qu'un Boeing 737. Lorsqu'on nous a informés qu'il pourrait être assujetti à des sanctions, nous avons avisé Transports Canada, qui a pris en charge le dossier de l'aéronef.

Quant aux passagers, nous avions le rôle de déterminer s'ils étaient en possession de tous les documents nécessaires pour avoir la permission d'entrer au pays. Je dois souligner qu'il n'y a pas d'interdiction d'entrée au pays visant les Russes en ce moment. Leur admissibilité est donc évaluée en fonction de leurs antécédents et des documents et des visas dont ils ont besoin. Si quelqu'un doit quitter le pays, nous nous assurons que nos agents font un suivi.

Dans un cas comme celui de Yellowknife, par exemple, les passagers qui se verraient refuser l'entrée au pays seraient redirigés vers Calgary ou Toronto, peut-être, pour quitter le pays, et nous confirmerions leur départ pour nous assurer qu'ils ont effectivement quitté le pays.

● (1605)

M. Xavier Barsalou-Duval: L'afflux de réfugiés en provenance de l'Ukraine, qui arriveront bientôt, j'espère, pourrait-il poser un défi sur le plan de l'identification des personnes et des menaces relatives à [*difficultés techniques*]?

Comment vérifiez-vous l'identité de la personne qui est devant vous?

M. Denis Vinette: Je vous remercie de votre excellente question.

Nous sommes en mesure de recevoir les Ukrainiens et les gens qui quittent leur pays pour venir ici en raison de ce qui se passe chez eux. Nos vérifications de sécurité comprennent la vérification de leurs données biométriques, dont leurs empreintes digitales, et de leurs documents. Nous faisons toutes les vérifications avant qu'ils reçoivent leur permis de séjourner au Canada. Nous faisons cela en appuyant les efforts du ministère de l'Immigration. Nous prenons donc toutes les mesures de sécurité.

Il y a toujours un risque que des gens cherchent à infiltrer un processus humanitaire de ce genre, et nous nous assurons d'avoir toutes les mesures en place pour les identifier.

Le président: Merci beaucoup, monsieur Vinette et monsieur Barsalou-Duval.

[*Traduction*]

Le prochain intervenant est M. Bachrach.

Monsieur Bachrach, vous disposez de six minutes. La parole est à vous.

M. Taylor Bachrach (Skeena—Bulkley Valley, NPD): Je vous remercie, monsieur le président.

Je remercie tous les témoins pour leurs témoignages intéressants.

Mes premières questions s'adressent à M. Gupta.

Monsieur Gupta, dans son évaluation des cybermenaces nationales de 2020, le CCC a conclu que les cyberactivités parrainées par des États représentaient la plus grande menace stratégique pour le Canada et qu'elles visaient probablement à perturber les infrastructures essentielles du pays.

Cette évaluation date d'il y a deux ans. Selon vous, est-elle encore juste aujourd'hui?

[*Difficultés techniques*]

Une voix: C'est une cyberattaque.

M. Taylor Bachrach: Est-ce ce qui est en train de se produire?

Des voix: Ha, ha!

Le président: Est-ce que tout le monde est là?

Monsieur Gupta, pouvez-vous réessayer votre microphone pour vérifier la connexion?

M. Rajiv Gupta: Oui, j'ai perdu la connexion pendant un instant. Je ne sais pas si je suis le seul.

Le président: Quelle coïncidence que c'est arrivé au milieu d'une discussion sur les menaces à la cybersécurité.

Monsieur Bachrach, je vais arrêter le chronomètre pour vous permettre de poser la question à nouveau afin que M. Gupta l'entende.

M. Taylor Bachrach: Monsieur Gupta, je ne sais pas si vous avez entendu la question. Elle concerne l'évaluation des cybermenaces nationales de 2020. Je voudrais savoir si cette évaluation est toujours juste, en particulier la constatation selon laquelle les cyberactivités parrainées par des États représentent la plus grande menace stratégique pour le Canada, surtout celles visant à perturber les infrastructures essentielles.

M. Rajiv Gupta: Je vais mentionner deux choses.

Dans notre rapport, nous avons écrit que la plus grande menace stratégique à long terme pour le Canada, ce sont les activités parrainées par des États, qui s'en prennent normalement à la prospérité économique, à la sécurité nationale et aux valeurs démocratiques. C'est quand les activités visent ces trois cibles en même temps qu'elles représentent une menace stratégique à long terme.

Dans l'évaluation des cybermenaces de 2020, nous avons également attiré l'attention sur la menace posée par les rançongiciels, en particulier les rançongiciels visant les infrastructures essentielles. Nous avons souligné que les rançongiciels risquaient d'avoir les répercussions les plus importantes sur la population canadienne. Malheureusement, depuis l'évaluation des menaces de 2020, cette prédiction s'est réalisée. Je pense qu'au cours de la dernière année, les rançongiciels sont la menace ayant eu la plus grande incidence sur la population canadienne.

Pour répondre à la question, monsieur le président, la plus grande menace stratégique à long terme demeure celle posée par les États lorsque cette menace vise à la fois la prospérité économique, la sécurité nationale et les valeurs démocratiques.

● (1610)

M. Taylor Bachrach: Je vous remercie, monsieur Gupta.

Après l'évaluation de 2020, le CCC a-t-il analysé des menaces particulières visant les infrastructures de transport maritime ou aérien? J'essaie de faire un lien avec le mandat du Comité des transports et de l'infrastructure.

Avez-vous réalisé des analyses précises de menaces particulières?

M. Rajiv Gupta: Non. Nous avons analysé différents secteurs, mais malheureusement, nous n'avons pas évalué les menaces visant précisément ces deux secteurs.

Nous avons analysé les menaces contre les technologies opérationnelles liées aux SCI. Nous trouvons cela pertinent. Le secteur des transports est une combinaison de TI et de TO. Nous nous sommes penchés sur les technologies sous-jacentes, mais nous n'avons pas évalué les menaces particulières visant les secteurs mêmes.

M. Taylor Bachrach: En mars, le président américain a publié une déclaration dans laquelle il mettait en garde contre la possibilité que la Russie mène une cyberactivité malveillante contre les États-Unis et leurs alliés, dont le Canada, bien entendu, en réponse aux coûts économiques sans précédent qu'ils ont imposés à la Russie.

Pourriez-vous décrire ou expliquer comment le contexte mondial de la cybermenace a changé depuis l'invasion de l'Ukraine par la Russie?

M. Rajiv Gupta: Bien sûr.

Pour revenir à l'évaluation de la cybermenace de 2020, nous avons mentionné que les États-nations créaient des capacités pour perturber des infrastructures essentielles. Nous savions qu'ils menaient des activités de reconnaissance dans des pays comme le Canada. Nous avons fait état dans l'évaluation de la cybermenace de 2020 qu'en l'absence d'hostilités ou de conflits, la menace serait faible.

Compte tenu de l'escalade des tensions en Ukraine et en Europe, nous avions commencé à mettre en garde le Canada le 19 janvier. C'est à ce moment-là que nous avons affiché notre premier bulletin sur l'escalade des tensions dans lequel nous exhortions les exploitants d'infrastructures essentiels à faire preuve de vigilance, à s'adapter aux tensions accrues et à mettre en œuvre certaines des recommandations que nous avions présentées pour se préparer. Nous avons réitéré ces mesures en janvier en publiant un autre bulletin.

Nous avions publié d'autres types de bulletins sur les menaces concernant les logiciels malveillants destructeurs en Ukraine et dans d'autres pays pour continuer de mettre en garde les Canadiens et de les informer de ce qui se passait exactement. Tout récemment, aux États-Unis, comme vous l'avez mentionné, M. Biden a encore une fois réitéré l'urgence de la situation. Mardi, sur notre site Web, nous avons réitéré cette mise en garde en disant que nous souscrivions à la déclaration selon laquelle les organisations canadiennes doivent faire preuve d'une vigilance accrue et que le contexte de la menace au Canada en est certainement un de vigilance et de sensibilisations accrues.

M. Taylor Bachrach: Je pense que ces points ont été abordés dans une certaine mesure dans le cadre de questions précédentes, mais d'après les renseignements disponibles, diriez-vous qu'il y a eu une hausse du nombre de tentatives de cyberattaques ciblant des infrastructures essentielles, y compris des infrastructures de transport, aux États-Unis ou dans les pays occidentaux alliés depuis l'invasion de la Russie?

M. Rajiv Gupta: À ce stade-ci, nous n'avons pas vu d'augmentation. Nous avons connaissance des cybermenaces qui ont lieu, mais ce sont des menaces que nous aurions déjà prévues.

M. Taylor Bachrach: Par ailleurs, vous avez mentionné plus tôt la cyberattaque NotPetya de 2017. Je pense que Sécurité publique nous a parlé de certaines des mesures qu'elle a prises depuis pour protéger l'infrastructure maritime et des transports du Canada.

Ma question s'adresse à vous, monsieur Gupta. Dans quelle mesure le transport maritime, au Canada plus particulièrement, est-il vulnérable à une attaque semblable à l'attaque NotPetya de 2017?

Le président: Vous avez le temps de poser une question très brève, monsieur Gupta, s'il vous plaît.

M. Rajiv Gupta: L'attaque NotPeya était attribuée à la Russie. Cela répond à une question qui a été posée plus tôt pour savoir si nous étions au courant de ces attaques.

En ce qui concerne la vulnérabilité, je laisserais le soin à mon homologue de Sécurité publique de répondre. Nous avons aidé nos collègues à concevoir l'outil, mais les évaluations, les connaissances et les renseignements recueillis ne sont pas entre nos mains au centre.

M. Ryan Schwartz: Monsieur le président, je peux fournir plus de détails dans une certaine mesure.

Nous avons travaillé sur les ports en ce qui concerne certains des outils d'évaluation de la résilience que nous avons. Nous avons réalisé des évaluations de la sécurité physique dans 14 installations au Canada. Nous n'avons effectué des évaluations de la cybersécurité que dans quatre installations. Si vous vous demandez si c'est peu, je dirais que oui. Je pense que c'est en partie attribuable au fait que les programmes que nous offrons ne sont pas obligatoires. Ce sont des programmes volontaires que Sécurité publique administre gratuitement. Nous comptons essentiellement sur les intervenants des infrastructures essentielles qui viennent nous voir pour offrir ces services.

Dans ce cas-ci, c'est un petit échantillon et nous ne pouvons pas vraiment faire de comparaisons précises sur la vulnérabilité globale.

Bien entendu, nous ne communiquons pas ces renseignements à grande échelle, sauf au propriétaire et à l'exploitant dans le cadre d'accords de confidentialité que nous signons avec eux. Nous avons des accords de non-divulgation que nous signons avec les propriétaires et les exploitants d'infrastructures essentielles et...

● (1615)

Le président: Merci beaucoup.

Je suis désolé, monsieur Schwartz. Je veux seulement m'assurer que nous accordons le même temps à tous les membres.

Chers collègues, pour ceux d'entre vous qui éprouvent des difficultés avec la connexion, je m'en excuse. Cela semble se produire dans de nombreux comités dans la Cité parlementaire à l'heure actuelle. Je vous encourage à continuer d'essayer à vous connecter.

Le prochain intervenant est M. Muys.

Monsieur Muys, vous disposez de cinq minutes. La parole est à vous.

M. Dan Muys (Flamborough—Glanbrook, PCC): Merci, monsieur le président, et merci à tous les témoins de nous accorder du temps.

Compte tenu de l'augmentation des cybermenaces graves, et certainement dans le contexte des lacunes générales dans les dépenses de défense de ce gouvernement, diriez-vous que nous ne dépensons pas suffisamment d'argent pour la cybersécurité, et plus particulièrement avec ce qui se passe dans le monde à l'heure actuelle?

M. Ryan Schwartz: Je suis désolé, monsieur le président. Est-ce une question pour Sécurité publique ou le centre pour la cybersécurité?

M. Dan Muys: Elle est pour quiconque veut y répondre. Nous commencerons peut-être avec M. Gupta.

M. Rajiv Gupta: En ce qui concerne les ressources, je pense que c'est davantage une question de politique. Pour l'instant, je voudrais souligner que la cybersécurité est une question qui concerne toute la société.

Comme on l'a mentionné plus tôt, les fournisseurs et le gouvernement ont l'obligation de fournir certains éléments de cybersécurité. C'est un équilibre. Le gouvernement doit fournir des conseils, des orientations, des outils et des renseignements pour aider les organisations à s'équiper. En même temps, les organisations doivent investir dans la mise en oeuvre des éléments fondamentaux de cybersécurité et de cyberrésilience pour se défendre.

M. Dan Muys: Quelqu'un de l'ASFC ou de Sécurité publique veut-il commenter?

M. Ryan Schwartz: D'accord.

Monsieur le président, j'ajouterais que le budget de 2019 a alloué environ 508 millions de dollars, si je ne m'abuse, pour les efforts visant à faire progresser la stratégie de cybersécurité mise à jour ou renouvelée, qui a été partagée entre un certain nombre de ministères et d'organismes pour leurs efforts respectifs en matière de cybersécurité. Je dirais également qu'il y aurait — je n'ai pas de chiffre à ce sujet — d'autres ressources qui sont appliquées ici. J'utiliserais l'exemple de mon propre groupe ici, où des efforts sont déployés pour offrir des programmes qui ne sont pas comptés ou regroupés dans le cadre de ces 508 millions de dollars.

Je vais m'en tenir là avec cette question. Merci.

M. Dan Muys: D'accord.

Diriez-vous que vous avez les ressources dont vous avez besoin à l'heure actuelle, ou en avez-vous besoin de plus?

M. Ryan Schwartz: Je suppose que la réponse est qu'il s'agit d'un secteur en pleine croissance. Je dis cela avec légèreté car l'ampleur du défi est croissante. Des investissements importants ont été réalisés.

Comme mon collègue au centre pour la cybersécurité l'a dit, la cybersécurité et la sécurité et la résilience des infrastructures essentielles sont certainement des responsabilités partagées. Je suis encouragé par le fait qu'un certain nombre d'intervenants, tant dans le secteur public que dans le secteur privé, travaillent ensemble, partagent leurs ressources et mettent en commun leurs renseignements pour résoudre ce problème.

Je pense que la nature des engagements qui ont été énoncés dans la lettre de mandat la plus récente pour que le ministre de la Sécurité publique renouvelle une stratégie indique l'intention de faire plus de travail ici, mais je ne peux pas dire si nous avons besoin de plus d'argent ou non à ce stade-ci.

M. Dan Muys: Très bien.

Pour ce qui est de l'infrastructure énergétique et des infrastructures essentielles à protéger, nous savons qu'en mai de l'année dernière, le pipeline Colonial au Texas, qui fournit la moitié de l'essence pour l'est des États-Unis, a été fermé pendant près d'une semaine en raison d'une attaque par rançongiciel. Vous avez parlé de la façon dont la menace au rançongiciel est certainement la menace qui a la plus grande incidence sur les Canadiens. Pour ce qui est de nos infrastructures essentielles en matière de transports, mais aussi de nos infrastructures énergétiques, sommes-nous prêts à faire face à une éventuelle attaque future?

● (1620)

M. Rajiv Gupta: Je peux commencer, monsieur le président.

Tout à fait, comme vous l'avez souligné, il est important de mettre en évidence le pipeline Colonial. Nous avons certainement pris cela très au sérieux, et cela correspondait à ce que nous avions prévu dans notre évaluation des cybermenaces.

En décembre, nous avons lancé une campagne contre les rançongiciels afin d'informer les Canadiens et de diffuser les renseignements, les outils et les ressources dont les organisations canadiennes ont besoin pour s'équiper.

Elle a commencé par une lettre ouverte de quatre ministres différents [*difficultés techniques*].

Le président: Je suis désolé, monsieur Gupta. Nous avons un peu de mal à vous entendre. Pourriez-vous peut-être répéter les deux ou trois dernières phrases?

M. Rajiv Gupta: D'accord.

Pour ce qui est de lutter contre les rançongiciels, nous avons lancé une campagne en décembre, qui a commencé par une lettre commune ouverte de quatre ministres différents, de même qu'un guide sur les rançongiciels et d'un bulletin sur les menaces aux rançongiciels pour contribuer à équiper les infrastructures essentielles et les Canadiens avec les outils nécessaires [*difficultés techniques*].

En outre, nous communiquons continuellement les renseignements sur les menaces liées aux rançongiciels aux différents secteurs. Vous avez mentionné l'énergie, qui est très importante et certainement dépendante des transports. Nous travaillons en étroite collaboration avec le secteur de l'énergie et nous avons mis en place deux programmes, l'un appelé Lighthouse et l'autre, Blue Flame, avec l'Association canadienne du gaz et l'industrie du gaz dans tout le Canada, afin d'échanger des renseignements sur les cybermenaces en temps quasi réel et d'aider à les protéger.

Ce sont là deux projets pilotes qui, selon nous, sont très importants pour protéger le secteur de l'énergie, et pas seulement pour les rançongiciels, mais pour les cybermenaces en général.

Le président: Merci beaucoup, monsieur Gupta.

Monsieur Muys, êtes-vous satisfait de la réponse fournie? Il y a quelques mots qui ont été coupés.

M. Dan Muys: Oui, je pense qu'il est revenu sur les lacunes dans les technologies.

Le président: Parfait. Merci.

Le prochain intervenant est M. Iacono.

Monsieur Iacono, la parole est à vous. Vous avez cinq minutes.

[*Français*]

M. Angelo Iacono (Alfred-Pellan, Lib.): Merci, monsieur le président.

Je remercie nos invités de leur présence.

Mes questions s'adressent à quiconque voudra y répondre.

Quelle est la nature de ces attaques? Sont-elles dues à des dénis de service ou s'agit-il de rançongiciels?

[*Traduction*]

M. Rajiv Gupta: Je vais commencer, monsieur le président.

En ce qui concerne la nature des attaques, nous avons décrit les rançongiciels. Les rançongiciels constituent une menace où un acteur s'introduit dans votre réseau, crypte vos données précieuses et les retient en otage jusqu'au paiement d'une rançon. Cette menace a évolué au point que les auteurs de la menace des rançongiciels prennent vos données, les cryptent parfois et menacent de vous extorquer en vous menaçant de divulguer les renseignements pour vous faire souffrir davantage et vous inciter à payer la rançon.

De toute évidence, ils sont motivés financièrement. Ils feront tout ce qu'il faut pour obtenir cet argent. Comme nous l'avons vu avec le ciblage de divers secteurs, y compris les soins de santé et autres, il y a certainement une incidence importante sur la vie, notamment. Ces auteurs de menaces sont intéressés par l'argent, et c'est à peu près tout.

Il y a différents types de menaces, évidemment. Il y a les attaques de déni de service distribué, qui sont parfois liées à des rançongiciels. Quelqu'un essaie de submerger une organisation de trafic et dit qu'il ne s'arrêtera pas tant que vous ne paierez pas une rançon. Ces attaques sont moins fréquentes que les rançongiciels traditionnels que j'ai décrits.

Il y a aussi, bien entendu, l'espionnage traditionnel et le vol de la propriété intellectuelle ou des données de l'entreprise de nature délicate, qui se traduisent par des violations de données, parce que cela vaut aussi de l'argent sur le Web caché en termes de vente de renseignements sur la santé, de données fiscales ou de renseignements financiers et de crédit, qui peuvent tous être vendus sur ces marchés pour de l'argent et, bien sûr...

[*Français*]

M. Angelo Iacono: Je vous remercie.

Monsieur Vinette, est-ce exact que la Russie fait souvent appel à des acteurs non étatiques, comme des réseaux criminels, pour mener ses attaques, afin de pouvoir mieux les nier?

● (1625)

M. Denis Vinette: Il s'agit d'une très bonne question, mais je pense que mes collègues MM. Schwartz et Gupta sont mieux placés que moi pour y répondre.

[*Traduction*]

M. Rajiv Gupta: Je peux répondre, monsieur le président.

Dans le cadre de l'évaluation des menaces aux rançongiciels, nous avons souligné les liens entre la Russie et certaines organisations criminelles en disant qu'elles étaient en mesure d'opérer avec une relative impunité dans les pays où elles ont des activités.

[*Français*]

M. Angelo Iacono: Je vous remercie.

Selon vous, quels sont les éléments vulnérables de nos propres réseaux de transport? De quoi devons-nous nous protéger?

[*Traduction*]

M. Ryan Schwartz: Je peux essayer de répondre à cette question, monsieur le président.

Du point de vue de la sécurité publique et de la résilience des infrastructures essentielles, l'une des principales vulnérabilités que nous constatons dans l'ensemble des secteurs des infrastructures essentielles est ce que j'ai appelé dans mes remarques liminaires les systèmes de contrôle industriel ou les technologies opérationnelles qui font fonctionner les centrales électriques, régulent la pression de l'eau dans les vannes ou même font fonctionner les feux de circulation. Il s'agit d'anciens systèmes qui n'étaient pas forcément destinés à être connectés à Internet, mais qui le sont désormais, compte tenu de l'Internet des objets et de la connectivité croissante dans les secteurs des infrastructures essentielles. De notre point de vue, les systèmes de contrôle industriel en général constituent une vulnérabilité clé.

Cela ne s'applique pas seulement au secteur des transports. Je dirais que cela s'applique à la santé, comme l'a mentionné mon collègue du centre pour la cybersécurité. L'incidence est due aux interdépendances. Si quelque chose se produit dans un secteur, il y aura un effet domino ou un effet d'entraînement dans d'autres secteurs. Nous sommes préoccupés par les répercussions en cascade. C'est pourquoi notre programme, avec nos collègues du centre pour la cybersécurité, se concentre sur les exercices de sécurité des systèmes de contrôle industriel. Il est également utile de se préparer à de tels événements et de faire de la planification.

En ce qui concerne le secteur de l'énergie, dans la question précédente, il y a un certain nombre d'exercices que nous menons dans le secteur privé. Ressources naturelles Canada est le ministère fédéral responsable du secteur de l'énergie et des services publics. Il y a un certain nombre d'exercices avec le Canada et les États-Unis, dont Energy Command et GridEx.

Nous nous concentrons sur ces vulnérabilités, notamment les systèmes de contrôle industriel.

[*Français*]

M. Angelo Iacono: Merci.

Le président: Merci beaucoup, monsieur Iacono.

[*Traduction*]

Merci beaucoup, monsieur Schwartz.

[*Français*]

Monsieur Barsalou-Duval, vous avez la parole pour deux minutes et demie.

Est-ce que nous avons perdu M. Barsalou-Duval?

Monsieur Barsalou-Duval, est-ce que vous nous entendez?

Puisqu'il ne répond pas, je vais donner la parole à M. Bachrach.

[*Traduction*]

Monsieur Bachrach, si vous êtes prêt à poser vos questions, je peux céder la parole à M. Barsalou-Duval après.

Monsieur Bachrach, la parole est à vous pour deux minutes et demie.

M. Taylor Bachrach: Merci, monsieur le président.

Je vais continuer mes questions pour M. Gupta, du centre pour la cybersécurité.

En 2016, Transports Canada a émis un document stratégique sur les pratiques exemplaires en matière de cybersécurité pour le secteur maritime. J'imagine que vous connaissez ce document. Je constate qu'il n'a pas été mis à jour depuis 2016. Les risques cybernétiques au cours des six dernières années ont-ils évolué dans le secteur maritime? Le cas échéant, pourquoi le document sur les pratiques exemplaires n'a-t-il pas été mis à jour?

M. Rajiv Gupta: Je tiens à préciser que ce n'est pas un produit du centre pour la cybersécurité. Je ne suis pas complètement au courant de ce qu'il en est.

Je suis certainement au courant des produits que nous publions depuis le centre pour la cybersécurité. Nous publions notre évaluation des cybermenaces et nous mettons régulièrement à jour nos conseils et orientations sur les pages Web du centre pour la cybersécurité.

La plupart de nos conseils et orientations s'appliquent à tous les secteurs. Je recommande aux gens de visiter la page cyber.gc.ca pour obtenir les renseignements les plus récents et les plus utiles.

● (1630)

M. Taylor Bachrach: Est-ce que j'ai du temps pour poser une autre question, monsieur le président?

Le président: Oui.

M. Taylor Bachrach: Je vais poser une question à notre invité de Sécurité publique.

Transports Canada a publié des propositions visant à moderniser le programme d'habilitation de sûreté en 2021. Ces propositions ajustent les exigences actuelles de base relatives aux risques pour les personnes en fonction de leur accès aux systèmes essentiels. Elles les ajustent pour inclure l'extension du contrôle de sûreté à toute personne qui participe à la circulation des expéditions maritimes.

Pensez-vous que le profil actuel des menaces de cybersécurité nécessite une expansion considérable des exigences en matière d'habilitation de sécurité?

M. Ryan Schwartz: Malheureusement, je ne suis pas en mesure de répondre à cette question. Je crois que c'est une question qu'il vaut mieux adresser à Transports Canada. Ce n'est pas un domaine qui relève de ma compétence.

M. Taylor Bachrach: D'accord.

Merci, monsieur le président.

Le président: Merci beaucoup, monsieur Schwartz et monsieur Bachrach.

[*Français*]

Monsieur Barsalou-Duval, vous avez la parole pour deux minutes et demie.

M. Xavier Barsalou-Duval: Merci, monsieur le président.

J'espère qu'on m'entend bien et qu'il n'y a pas de problème technique. Aujourd'hui, j'ai eu beaucoup de difficulté à me connecter à la réunion. Je pense que j'ai été déconnecté cinq fois de la rencontre Zoom.

Ma question s'adresse à M. Gupta. J'espère ne pas répéter ce qui a été dit, mais j'ai peut-être manqué quelques éléments qui ont été soulignés jusqu'à présent.

L'indice national de cybersécurité du Canada est de 66,23 sur 100, ce qui le place au 36e rang mondial en matière de cybersécurité. En comparaison avec l'Allemagne, qui a un indice de 90,91, ou la France, qui a un indice de 84,42, le Canada fait pâle figure, pour ne pas dire qu'il fait figure d'amateur.

J'aimerais savoir sur quoi l'on doit travailler pour augmenter cette cote. En tant que dirigeant du Centre canadien pour la cybersécurité, pourriez-vous me dire ce qui explique que notre cote soit aussi basse comparativement aux pays de référence?

[*Traduction*]

M. Rajiv Gupta: Monsieur le président, je ne suis pas familier avec l'index auquel le député fait référence, malheureusement.

[*Français*]

M. Xavier Barsalou-Duval: Cela ne vous empêche pas de parler des éléments sur lesquels on doit travailler davantage.

[*Traduction*]

M. Rajiv Gupta: Le plus important pour moi, c'est que nous commencions à mettre en œuvre les bases de la cybersécurité dans tout le pays. C'est fondamental, et cela s'applique à tous les types de menaces, qu'il s'agisse de la Russie, des rançongiciels, de la cybercriminalité ou de l'hacktivisme. Nous avons publié des conseils ou des directives de base pour que notre pays soit solide.

Évidemment, oui, j'aimerais que notre pays soit le numéro un et qu'il soit à cent pour cent là aussi, mais je pense que travailler sur ces types d'éléments de base de la cybersécurité est essentiel pour nous assurer que nous sommes prêts et résilients pour répondre à tout type de menace.

Nous avons publié des conseils et des directives pour une petite entreprise qui, je pense, sont essentiels. Il s'agit de 13 contrôles que nous pensons réalisables en termes de mise en œuvre, et nous recommandons vivement aux organisations de s'en inspirer pour mettre en œuvre ces contrôles ainsi que...

[*Français*]

M. Xavier Barsalou-Duval: Mon temps de parole est presque écoulé, mais j'aimerais vous poser une autre question.

Travaillez-vous à la mise en place ou au renforcement de la cybersécurité pour les gouvernements provinciaux ou municipaux ou vous concentrez-vous simplement sur le gouvernement fédéral?

[*Traduction*]

M. Rajiv Gupta: Nous travaillons en étroite collaboration avec nos partenaires provinciaux. J'ai récemment rencontré l'ensemble des APSI provinciaux, les agents principaux de la sécurité de l'information, au Canada. Nous travaillons bien ensemble, dans la collaboration, et nous sommes convaincus que cette collaboration permet de renforcer la cybersécurité au Canada.

Le président: Merci, monsieur Gupta.

[*Français*]

Merci beaucoup, monsieur Barsalou-Duval.

[*Traduction*]

M. Dowdall est le prochain intervenant.

Monsieur Dowdall, la parole est à vous, pour cinq minutes.

M. Terry Dowdall (Simcoe—Grey, PCC): Merci, monsieur le président.

Je tiens à remercier M. Gupta et M. Schwartz d'avoir pris le temps d'être ici aujourd'hui. Cette question s'adressera probablement à M. Gupta, mais M. Schwartz voudra peut-être faire des commentaires également.

Le 24 février 2022, lors d'un point de presse, Daniel Rogers, le sous-chef délégué du Centre de la sécurité des télécommunications, a déclaré qu'à la lumière de l'invasion de l'Ukraine par la Russie, le CST « encourage fortement toutes les organisations canadiennes à prendre des mesures immédiates et à renforcer leurs cyberdéfenses en ligne ». Bien que M. Rogers ait déclaré que le CST « n'était pas au courant de menaces précises contre des organisations canadiennes en rapport avec les événements en Ukraine et dans la région », il a souligné les « antécédents historiques de cyberattaques contre l'Ukraine et d'autres pays ». En particulier, M. Rogers a déclaré que le CST surveillait les cybermenaces « dirigées contre les réseaux d'infrastructures essentielles, notamment dans les secteurs des services financiers et de l'énergie. »

C'est particulièrement préoccupant pour les Canadiens, étant donné que beaucoup de nos renseignements personnels et financiers sont maintenant stockés dans le nuage, sur nos ordinateurs ou nos téléphones.

Je sais que certaines de ces questions ont déjà été posées, peut-être, mais avons-nous observé une recrudescence des attaques par la Russie ou la Chine depuis le début de l'invasion?

● (1635)

M. Rajiv Gupta: Le CST n'a pas constaté de hausse des attaques contre les infrastructures canadiennes au pays.

M. Terry Dowdall: Selon vous, les entreprises canadiennes des secteurs des services financiers et de l'énergie mettent-elles en place toutes les mesures de sécurité nécessaires à tous les niveaux pour contrer les cyberattaques et protéger nos renseignements personnels?

M. Rajiv Gupta: Nous maintenons un lien régulier avec ces secteurs. Nous travaillons avec ces gens et ils participent très activement à nos séances d'information. J'estime qu'ils prennent des mesures et qu'ils sont attentifs aux avis que nous diffusons, notamment quant à la nécessité d'une vigilance accrue et des efforts pour sécuriser leurs systèmes autant que possible, étant donné les hostilités dans le contexte géopolitique actuel. Les efforts de collaboration démontrent l'engagement de ces secteurs à cet égard.

M. Terry Dowdall: À titre de professionnel, comment évalueriez-vous, sur une échelle de 1 à 10 — 10 étant extrêmement sûr —, l'état de préparation actuel des secteurs canadiens des services financiers et de l'énergie contre les cyberattaques?

M. Rajiv Gupta: Il est très difficile d'attribuer une note sur une échelle de 1 à 10. J'en serais incapable. Je dirai toutefois qu'ils sont très mobilisés et qu'ils sont compétents. Nous savons qu'ils y travaillent.

Le CST n'est pas un organisme de réglementation. Par conséquent, je ne connais pas les mesures exactes qu'ils prennent pour atténuer leurs risques, mais je sais qu'ils tendent à très bien comprendre les avis et les orientations et qu'ils sont déterminés à travailler avec nous. C'est probablement tout ce que je peux dire à ce sujet.

M. Terry Dowdall: Très bien, merci.

La semaine dernière, comme vous le savez sans doute, le Congrès américain a adopté une nouvelle loi sur la cybersécurité qui oblige les entités d'infrastructures essentielles à signaler les incidents de cybersécurité importants dans les 72 heures et les paiements lors d'une attaque par rançongiciel dans les 24 heures à la Cybersecurity and Infrastructure Security Agency.

Le Canada devrait-il imiter les États-Unis?

M. Rajiv Gupta: Je peux commencer, monsieur le président.

Cela fonctionne sur une base volontaire. Évidemment, nous encourageons les entités canadiennes à nous en informer immédiatement. Nous sommes là pour les aider et nous sommes très heureux qu'ils communiquent avec nous.

Quant à la situation aux États-Unis, nous travaillerons certainement avec nos collègues et homologues américains pour apprendre comment cela fonctionne là-bas et tirer des enseignements de leur expérience.

M. Terry Dowdall: À ce moment précis, recommanderiez-vous que nous fassions preuve d'une plus grande diligence à cet égard?

M. Rajiv Gupta: Je vois plutôt cela comme une question de politique.

M. Terry Dowdall: Très bien.

M. Ryan Schwartz: Monsieur le président, permettez-moi de revenir brièvement à la question précédente, à savoir si certains secteurs sont préparés. Par rapport aux commentaires de mon collègue, j'ajouterais qu'il s'agit d'une priorité pour les associations industrielles, notamment le Forum canadien pour la résilience des infrastructures numériques et Électricité Canada, anciennement l'Association canadienne de l'électricité. Nous avons une importante collaboration avec diverses associations industrielles.

Concernant la diligence accrue et la proposition ou l'initiative américaine que vous avez mentionnée, je souligne que le budget de 2019 comprenait un investissement pour appuyer une nouvelle mesure législative visant à protéger les cybersystèmes essentiels du Canada dans quatre secteurs: finances, télécommunications, énergie et transports. Les ministères et organismes clés s'y emploient toujours. Je dirais que c'est une priorité pour nos partenaires de l'industrie, mais aussi pour le gouvernement fédéral, notamment en ce qui concerne notre travail continu pour l'établissement de politiques.

Le président: Merci beaucoup, monsieur Schwartz, et merci beaucoup, monsieur Dowdall.

La dernière intervention pour ce premier groupe revient à Mme Koutrakis.

Madame Koutrakis, vous avez cinq minutes. La parole est à vous.

[*Français*]

Mme Annie Koutrakis (Vimy, Lib.): Merci, monsieur le président, et merci à tous les témoins qui sont avec nous cet après-midi.

J'invite n'importe lequel de nos témoins à répondre à mes questions cet après-midi.

Y a-t-il des raisons de croire que des États étrangers pourraient essayer de travailler avec des groupes nationaux pour encourager le blocage d'infrastructures critiques comme les postes-frontière, comme nous l'avons vu plus tôt cette année?

● (1640)

M. Denis Vinette: Je serais heureux de répondre à la question de la députée, monsieur le président.

Je remercie la députée de la question.

En fait, nous échangeons constamment des renseignements et nous sommes toujours à l'écoute afin de savoir ce qui se passe et de détecter ce qui pourrait compromettre notre présence et la fluidité des frontières en raison de leur importance pour l'économie et pour la sécurité du Canada.

Pour répondre directement à votre question, je n'ai aucune information pour le moment qui démontre cela, mais il va sans dire que, par suite des sanctions qui ont été imposées, nous nous assurons que ces cargos, qui sont ciblés, ne passent pas à la frontière.

Sur le plan de la sécurité, nous avons des portails de détection des radiations dans nos ports maritimes pour nous assurer que les conteneurs qui arrivent d'outre-mer sont vérifiés en raison de la radiation et des produits chimiques qui pourraient s'y retrouver.

Nous sommes toujours sur nos gardes, mais je n'ai aucune information pour le moment qui démontre que des efforts sont déployés afin de bloquer les infrastructures.

Mme Annie Koutrakis: Est-ce qu'un autre témoin voudrait ajouter quelque chose?

[*Traduction*]

M. Ryan Schwartz: Monsieur le président, j'aimerais faire un commentaire, si vous le permettez.

Premièrement, par rapport à l'exemple des récents blocages de février, je n'ai pas de renseignements à ajouter à la réponse de M. Vinette. Je pense toutefois qu'il convient de se pencher sur la question des effets de la désinformation et de la mésinformation qui peuvent se propager sur les plateformes de médias sociaux et servir à susciter certaines réactions, pourrait-on dire, qui ont des conséquences négatives et perturbatrices sur les infrastructures essentielles canadiennes, notamment les infrastructures essentielles de transport.

La mésinformation et la désinformation peuvent avoir des effets déstabilisateurs considérables sur la stabilité et la fiabilité des infrastructures essentielles, mais aussi sur la cohésion sociale. Je tiens aussi à souligner ce point pour le Comité.

[*Français*]

Mme Annie Koutrakis: Je vous remercie de votre réponse.

La connaissance du domaine aérospatial et maritime du Canada est-elle suffisante pour permettre la détection de menaces envers ses installations portuaires, ses eaux et son espace aérien?

M. Denis Vinette: Je vous remercie de la question.

En fait, l'ASFC travaille en partenariat avec Transports Canada, qui est responsable de la réglementation entourant la sécurité dans les aéroports, dans nos ports maritimes et ailleurs.

Nous travaillons toujours très étroitement avec Transports Canada pour nous assurer que, dès qu'il y a des menaces ou que de l'information parvient à l'un des partenaires, celle-ci est partagée et est ensuite évaluée pour déterminer si une réponse est nécessaire. Au sein des groupes maritimes, qui surveillent nos côtes et qui constituent des équipes intégrées de l'ASFC, de la GRC, de la Garde côtière et de nos collègues militaires, nous travaillons ensemble pour avoir en tout temps un aperçu de ce qui se passe dans le domaine maritime. C'est un exemple des efforts que nous déployons pour assurer la sécurité de nos ports d'entrée quand il y a des mouvements de navires. Nous avons un effort similaire du côté aéroportuaire également.

Merci.

Mme Annie Koutrakis: Merci beaucoup.

[*Traduction*]

Ce sera ma dernière question, si j'ai le temps, monsieur le président.

Avons-nous des capacités offensives que nous pourrions utiliser en guise de représailles si la Russie tentait d'attaquer nos infrastructures essentielles?

M. Rajiv Gupta: Du point de vue du CST, nous avons [*difficultés techniques*] dans les cyberopérations défensives pour lesquelles nous avons à la fois l'autorité législative et la capacité de mener.

[*Français*]

Le président: Merci beaucoup, madame Koutrakis.

[*Traduction*]

Merci beaucoup, monsieur Gupta.

C'est là-dessus que se termine notre discussion avec le premier groupe de témoins. Au nom du Comité, je tiens à remercier tous les témoins de leur présence ici aujourd'hui.

Je vais maintenant suspendre la séance pendant cinq minutes pour permettre aux témoins de se déconnecter.

Chers collègues, lorsque nous reprendrons la séance, nous entendrons la déclaration préliminaire et le témoignage de M. John de Boer, directeur principal des affaires gouvernementales et des politiques publiques chez BlackBerry.

La séance est suspendue.

● (1640)

_____(Pause)_____

● (1650)

Le président: Nous reprenons.

Chers collègues, au cours de cette deuxième partie de la séance d'aujourd'hui, nous accueillons M. John de Boer, directeur principal des affaires gouvernementales et des politiques publiques pour le Canada, chez BlackBerry.

Monsieur de Boer, je crois savoir que vous avez préparé une déclaration. La parole est à vous, pour cinq minutes.

M. John de Boer (directeur principal, Affaires gouvernementales et politiques publiques, Canada, BlackBerry): Merci, monsieur le président.

Je suis ravi de prendre la parole devant vous et les membres du Comité aujourd'hui au nom de BlackBerry.

Depuis plus de 35 ans, BlackBerry invente et produit des solutions de sécurité fiables pour assurer la sécurité et la productivité des personnes, des gouvernements et des entreprises. Aujourd'hui, nos logiciels sont utilisés pour protéger tous les gouvernements du G7, sont intégrés à plus de 195 millions de voitures et sécurisent plus de 500 millions d'autres appareils, notamment des téléphones cellulaires, des ordinateurs portables et des systèmes dans les secteurs du transport, de l'aérospatiale et de la défense.

Aujourd'hui, en m'appuyant sur notre engagement indéfectible envers la sécurité, la sûreté et la confidentialité des données, j'aimerais parler de l'écart entre l'état de préparation en matière de cybersécurité du secteur canadien des transports et l'exposition croissante de ce secteur aux cybermenaces.

Quel que soit leur secteur d'activité, toutes les organisations risquent d'être victimes d'une cyberintrusion. Toutefois, peu d'organisations ont un même degré de risque réel de cyberattaque que les organismes du secteur des infrastructures essentielles. Comme le Comité l'a entendu plus tôt cette semaine, les attaques de rançongiciels ont augmenté de 186 % dans l'industrie du transport en Amérique du Nord entre juin 2020 et juin 2021. L'année dernière, les réseaux de transport en commun canadiens de Toronto, Montréal et Vancouver ont subi des cyberattaques. Les Canadiens sont inquiets, à juste titre. Selon le Baromètre de confiance Edelman, être victime d'une cyberattaque est maintenant la deuxième plus importante préoccupation des Canadiens après la perte d'emploi.

Actuellement, outre les obligations liées à la LPRPDE, le Canada n'a pas de réglementation pour encadrer les exploitants et propriétaires des entreprises de transport ferroviaire, aérien et de surface pour ce qui est des incidents de cybersécurité — prévention, préparation et signalement —, et encore moins pour imposer des obligations. Bien que les administrations portuaires, les installations maritimes et les services de traversiers aient l'obligation réglementaire de signaler les cyberincidents aux organismes d'application de la loi et à Transports Canada, il n'existe aucune période de déclaration spécifique ni aucune orientation sur les mesures de cybersécurité devant être mises en place.

Dans un contexte mondial et concurrentiel plus large, le Canada accuse du retard par rapport au pays du G7 sur le plan de la cybersécurité. En effet, par habitant, le Canada investit deux fois moins dans ce domaine que les États-Unis, le Royaume-Uni et la France. Les gouvernements américain et européens ont aussi mis en place une réglementation pour renforcer les exigences en matière de cybersécurité des infrastructures essentielles, notamment les systèmes de transport. À titre d'exemple, le gouvernement américain a pris des mesures importantes pour remédier aux vulnérabilités informatiques dans la foulée d'attaques successives survenues l'an dernier contre des infrastructures critiques américaines, notamment l'oléoduc de Colonial Pipeline et le métro de New York.

En mai 2021, le président Biden a pris un décret visant à améliorer la cybersécurité du pays; le décret oblige son gouvernement à moderniser ses défenses en matière de cybersécurité. En juillet 2021, le président Biden a demandé au gouvernement américain de définir des objectifs de rendement en matière de cybersécurité pour les propriétaires et exploitants d'infrastructures critiques.

En décembre 2021, la Transportation Security Administration du département de la Sécurité intérieure des États-Unis [*difficultés techniques*] tous les transporteurs ferroviaires et les exploitants de services ferroviaires voyageurs et de transport en commun ferroviaire de désigner un coordinateur de la cybersécurité, de signaler tout incident de cybersécurité au gouvernement américain dans les 24 heures, d'élaborer un plan d'intervention en cas d'incident lié à la cybersécurité et de procéder à l'analyse de la vulnérabilité de la cybersécurité.

Il y a deux semaines à peine, le président Biden a promulgué la Cyber Incident Reporting for Critical Infrastructure Act of 2022, qui oblige les entités d'infrastructures essentielles visées à signaler les incidents de cybersécurité au gouvernement dans les 72 heures et les paiements lors d'une attaque par rançongiciel dans les 24 heures.

L'Europe a des exigences semblables, exigences qu'elle étend actuellement aux systèmes de transport intelligents, par exemple les voitures connectées et les infrastructures intelligentes. Elle prévoit aussi imposer des amendes pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel, selon le montant le plus élevé, aux entités jugées non conformes.

● (1655)

Bien que le Canada se soit récemment joint au Royaume-Uni et aux États-Unis pour rappeler aux responsables des infrastructures essentielles « de prendre conscience des activités de cybermenace parrainées par l'État [...] et de se protéger contre elles », nous sommes encore loin derrière.

BlackBerry est prête à travailler avec le Comité pour renforcer la cybersécurité des systèmes de transport au Canada contre cette menace croissante et en constante évolution.

Je vous remercie du temps que vous m'avez accordé aujourd'hui. C'est avec plaisir que je répondrai à vos questions.

Le président: Merci beaucoup, monsieur de Boer.

Nous commençons les questions pour cette partie avec Mme Lantsman.

Madame Lantsman, la parole est à vous. Vous avez six minutes.

Mme Melissa Lantsman (Thornhill, PCC): Monsieur de Boer, merci de vous joindre à nous via Zoom, et merci de votre déclaration préliminaire.

Pour commencer, j'aimerais savoir si nous avons suffisamment de données au Canada. Les messages semblent contradictoires. On entend dire que nous ne savons pas ce qu'il en est, ou que nous ignorons l'ampleur de la menace dans les différents secteurs. Selon vous, collectons-nous assez de données pour évaluer correctement les menaces à la cybersécurité auxquelles nous sommes confrontés?

M. John de Boer: Quatre-vingt-dix pour cent des cyberincidents ne sont pas signalés.

En outre, comme je l'ai mentionné, les exploitants d'infrastructures essentielles ou les entités du secteur privé n'ont aucune obligation de signaler les cyberincidents.

Vous avez cerné un problème crucial. Le gouvernement canadien et de nombreuses entités n'ont tout simplement pas un portrait global de l'ampleur ou de la nature persistante de la menace. C'est un des principaux problèmes, et c'est une des raisons pour lesquelles le président Biden a imposé la déclaration obligatoire des cyberincidents pour les infrastructures essentielles.

● (1700)

Mme Melissa Lantsman: Je vous remercie de cette réponse.

Je me demande, dans ce cas, comment les gouvernements déterminent les sommes à consacrer à la cybersécurité s'ils ignorent l'ampleur de la menace.

Nous venons d'entendre M. Schwartz, un fonctionnaire du ministère de la Sécurité publique. Il a mentionné que le budget de 2019 comportait un montant de 500 millions de dollars à cette fin. Compte tenu des événements des dernières semaines au pays et du manque flagrant de financement en matière de sécurité et de défense, il a laissé entendre que c'était suffisant, en précisant toutefois, en guise de mise en garde, que les menaces augmentent.

Pouvez-vous parler brièvement de la situation du Canada sur le plan du financement consacré à la cybersécurité? Comment savons-nous combien d'argent dépenser si nous ignorons l'ampleur du problème? Pourquoi dépensons-nous beaucoup moins que nos alliés?

M. John de Boer: Le budget de l'année dernière, 2021, comportait un montant de 791 millions de dollars canadiens pour la cybersécurité, ce qui représente une légère augmentation par rapport au budget de 2019. Par habitant, comme je l'ai mentionné plus tôt, le Canada consacre 20 $ à la cybersécurité. Nous sommes loin derrière le Royaume-Uni, les États-Unis et la France, qui dépensent respectivement 52 $, 34 $ et 37 $ par habitant, en dollars canadiens.

Quant à savoir si nos dépenses sont assez élevées, la réponse courte est non. Les entreprises canadiennes ont dépensé 7 milliards de dollars en cybersécurité l'an dernier, ce qui n'est manifestement pas suffisant non plus, car selon le Bureau d'assurance du Canada, 47 % de nos petites et moyennes entreprises n'ont rien dépensé en cybersécurité l'an dernier. Donc, il serait possible d'investir beaucoup plus.

Nous devons rattraper nos alliés pour renforcer nos défenses. Une partie de la solution passe par l'obligation d'investir. Une autre, peut-être, serait que le gouvernement comble une défaillance du marché, qui considère la cybersécurité comme un coût et non une priorité. La cybersécurité doit être considérée comme une priorité au plus haut niveau.

Mme Melissa Lantsman: Dans votre déclaration préliminaire, vous avez parlé d'une augmentation de 186 % du nombre d'incidents d'une année à l'autre. Je crois que c'est le chiffre que vous avez utilisé. Je pense l'avoir mentionné plus tôt au Comité. Étant donné ce chiffre et ce que vous savez, je suis plutôt perplexe de constater que les fonctionnaires qui ont comparu plus tôt n'ont fait aucune analyse quelconque sur les transports essentiels. Je me demande s'il s'agit d'une de nos lacunes.

Quelle est votre évaluation du risque de menace étrangère, soit par la Russie, dans le cas de cette étude? Quelle est votre évaluation des menaces qu'elle pose actuellement aux infrastructures de transport essentielles?

Nous avons beaucoup entendu parler des institutions financières. Nous avons un peu entendu parler des infrastructures essentielles du secteur pétrolier. Y a-t-il moyen de savoir ce qu'il en est du secteur du transport, si cela n'a jamais fait l'objet d'une étude ou d'une évaluation?

M. John de Boer: Je me fierais à certaines évaluations provenant du gouvernement des États-Unis, qui a dit publiquement que la menace était réelle et persistante. Le président Biden a lancé une stratégie de cybersécurité maritime l'année dernière, qui documentait des lacunes importantes dans le système portuaire, de même que dans les systèmes de navires. Bon nombre de ces systèmes, qu'il s'agisse des navires, des trains ou des avions, ont été conçus pour durer 30 ans; ils sont donc désuets et n'ont pas été mis à niveau. La vulnérabilité est grande; elle est profonde, et la menace est persistante et réelle.

En octobre 2020, le département de la Justice américain a porté des accusations contre six agents du renseignement russes impliqués dans l'affaire du maliciel NotPetya qui a grandement nui au géant de l'expédition Maersk et a aussi attaqué TNT, aujourd'hui FedEx.

Les données probantes montrent que certaines des plus grandes attaques, qui ont entraîné les conséquences les plus graves, sont liées à l'État.

● (1705)

Mme Melissa Lantsman: Merci, monsieur de Boer.

Le président: Merci beaucoup, monsieur de Boer.

Merci, madame Lantsman.

Nous allons maintenant entendre M. Rogers.

Monsieur Rogers, vous disposez de six minutes; allez-y.

M. Churence Rogers (Bonavista—Burin—Trinity, Lib.): Merci, monsieur le président.

Je souhaite la bienvenue à notre invité.

Monsieur de Boer, c'est impressionnant de vous entendre parler de cybersécurité. L'année dernière seulement, à Terre-Neuve-et-Labrador, le système de santé a subi une importante attaque et a été paralysé pendant plusieurs jours, ce qui a entraîné toutes sortes de problèmes dans la province. Il y a eu des lacunes importantes. Certains dossiers médicaux étaient manquants et les professionnels des soins de santé ont dû faire face à toutes sortes de problèmes. Il a fallu beaucoup de temps et d'efforts de la part des intervenants provinciaux et fédéraux pour régler bon nombre des problèmes. Cet événement était si grave que le premier ministre et les responsables à Ottawa n'en parlaient même pas en public, pour des raisons de sécurité.

Je ne sais même pas si la situation est complètement réglée. Cela semble être le cas; il n'y a plus de discussions publiques à ce sujet.

Selon vous, comment peut-on prévenir de tels incidents pour l'avenir? On ne peut pas revenir en arrière, mais comment peut-on éviter que cela se reproduise à nouveau?

M. John de Boer: C'est une excellente question. Nous pouvons éviter ce genre de situation.

Il y a des technologies de prévention offertes sur le marché. Elles misent sur l'intelligence artificielle et l'apprentissage automatique pour prédire et prévenir les attaques. Nous allons au-delà des technologies traditionnelles, qui adoptaient ce qu'on appelle une approche fondée sur la signature, semblable à celle utilisée pour le vaccin contre la COVID-19. Il faut un patient zéro qui sert de modèle et de base pour la recherche. Aujourd'hui, la technologie permet de prévenir cela.

Ensuite, la déclaration obligatoire des cyberincidents associés aux infrastructures essentielles incitera les entités à mettre en place de meilleurs moyens de défense. Elles ne veulent pas devoir déclarer les cyberincidents, mais si elles le font, nous pourrons agir rapidement pour les contenir.

Pour aborder la vulnérabilité, les États-Unis demandent aux développeurs des logiciels intégrés aux infrastructures essentielles et aux systèmes gouvernementaux de produire ce qu'on appelle une nomenclature du logiciel ou une liste d'ingrédients, qui énumère toutes les composantes des logiciels de sorte qu'on puisse déterminer rapidement leur provenance ou leur origine, désigner les vulnérabilités et y remédier.

Dans les faits, à l'heure actuelle, les gens qui achètent les logiciels n'ont aucune idée de ce qui s'y trouve. Il n'y a aucun moyen de déterminer si l'on a appliqué les pratiques en matière de sécurité au moment de la conception du logiciel.

M. Churence Rogers: Je ne sais pas si vous aurez le temps de me répondre avant la fin de mon intervention, mais j'aimerais vous poser une autre question.

J'ai l'impression que vous avez donné beaucoup d'exemples de ce que font les États-Unis et de ce qu'ils prévoient faire. Comment décririez-vous l'état de préparation du Canada en vue de faire face à des cyberattaques contre nos réseaux de transport? Lesquels seraient les plus susceptibles d'être touchés? Les transporteurs aériens, les services maritimes ou les services ferroviaires? Comment pouvons-nous mieux nous protéger contre ces cyberattaques?

● (1710)

M. John de Boer: Malheureusement, tous les réseaux sont susceptibles d'être touchés. Ils contiennent tous de vieux systèmes de TI qui ne sont pas protégés et ont des logiciels en libre accès qui pourraient avoir des trappes. Ils dépendent des chaînes d'approvisionnement et des fournisseurs de confiance pour mettre en oeuvre des pratiques sécuritaires, mais ne les vérifient peut-être pas.

Tous les réseaux sont vulnérables. C'est pourquoi nous devons agir rapidement et demander aux exploitants des infrastructures essentielles et du transport en commun de déclarer les cyberincidents, d'élaborer des plans d'intervention en cas d'incident et de procéder à l'évaluation de la vulnérabilité de la cybersécurité. Enfin, il ne suffit pas d'avoir un plan sur papier. Il faut s'assurer que le plan soit mis en oeuvre.

M. Churence Rogers: Lorsque j'entends tous les conseils que vous nous avez donnés — et Mme Lantsman en a parlé également —, il semble que nous devions investir beaucoup plus d'argent pour être bien préparés. Est-ce exact?

M. John de Boer: BlackBerry et la Chambre de commerce du Canada ont fait une présentation budgétaire à cet égard. Nous demandons au gouvernement de doubler son investissement dans la cybersécurité. Ainsi, nos dépenses en matière de cybersécurité seraient équivalentes à celles des autres pays du G7. Donc oui, il faut dépenser plus et il faut dépenser de façon intelligente. Il y a aussi des initiatives qui ne coûtent rien et que nous pouvons prendre dès maintenant, comme la déclaration des incidents dont j'ai parlé plus tôt.

La dernière chose que j'aimerais dire, rapidement, c'est qu'il faut un leadership au sommet. Il faut désigner la cybersécurité à titre de priorité. Le président Biden parle presque quotidiennement de cybersécurité. Il faut assurer le même leadership ici.

Le président: Merci beaucoup, monsieur de Boer, et merci, monsieur Rogers.

M. Churence Rogers: Merci beaucoup.

[*Français*]

Le président: Le prochain intervenant est M. Lemire.

Monsieur Lemire, je vous souhaite la bienvenue au Comité. Vous avez la parole pour six minutes.

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

Je remercie également toute l'équipe technique.

Monsieur de Boer, en 2021, le gouvernement du Canada a choisi BlackBerry pour ses besoins en matière de productivité et de communication sécurisées ainsi que pour la gestion d'événements critiques. Comme cette affirmation laisse beaucoup de place à l'interprétation, j'aimerais connaître votre point de vue sur la question.

Quelle est la nature exacte des services de cybersécurité que BlackBerry fournit au gouvernement fédéral?

[*Traduction*]

M. John de Boer: Monsieur le président, BlackBerry offre un éventail de services, notamment des services de protection et de gestion unifiées des points d'extrémité, pour protéger les appareils mobiles. Nous offrons aussi des communications sécuritaires au gouvernement du Canada, qui sont certifiées par l'entité canadienne de cybersécurité, le Centre canadien pour la cybersécurité. L'objectif premier est la sécurisation des communications et la gestion unifiée des points d'extrémité, qui vise la sécurité des technologies mobiles.

[*Français*]

M. Sébastien Lemire: Je vous remercie.

Selon un rapport publié en 2017 par le Centre de la sécurité des télécommunications, le gouvernement fédéral subirait à lui seul, chaque année, plus de 2 500 tentatives d'intrusion informatique de la part d'acteurs étatiques étrangers.

Monsieur de Boer, êtes-vous en mesure de nous dire combien de cyberattaques, approximativement, ont eu comme cible le gouvernement fédéral depuis sa collaboration avec BlackBerry en 2021?

[*Traduction*]

M. John de Boer: C'est difficile à dire. Je n'ai pas les chiffres exacts sur le gouvernement. Encore une fois, nous nous centrons principalement sur les communications sécuritaires et sur les technologies mobiles. Nous ne surveillons pas la posture de sécurité du gouvernement du Canada.

[*Français*]

M. Sébastien Lemire: Si vous ne pouvez pas nous parler de la quantité, pouvez-vous nous parler de la qualité? Avez-vous le sentiment, depuis le début de votre mandat avec le gouvernement fédéral, que la gravité des cyberattaques ciblant les institutions canadiennes augmente?

[*Traduction*]

M. John de Boer: Je n'ai personnellement pas accès à ce type d'information sur la gravité des attaques. Je peux seulement commenter les événements qui ont fait les manchettes et ce que j'ai vu personnellement. Je ne peux malheureusement pas vous fournir une réponse précise à cette question.

● (1715)

[*Français*]

M. Sébastien Lemire: Dans votre allocution, vous avez parlé, d'une part, de la sécurité des appareils et des risques que tout le monde puisse subir des cyberattaques. D'autre part, vous avez parlé de l'obligation légale des entreprises de signaler les cyberattaques sur les infrastructures essentielles.

Seriez-vous en mesure, comme collaborateur, de nous donner de l'information sur cela? Si vous fournissez un système, c'est que vous y avez accès. Êtes-vous en mesure d'aider le gouvernement à recevoir ces données afin qu'elles soient plus transparentes?

[*Traduction*]

M. John de Boer: BlackBerry collabore régulièrement avec le gouvernement du Canada, le Centre canadien pour la cybersécurité et d'autres, que ce soit au sujet de la divulgation des vulnérabilités ou d'autres évaluations de la menace.

J'aimerais toutefois dire qu'on a beaucoup mis l'accent sur le partage des renseignements. Je crois qu'on pourrait une fois de plus reproduire ce qu'ont fait les États-Unis, avec la planification collaborative. Il s'agit d'une approche de prévention qui vise à aborder les événements qui pourraient se produire. C'est là-dessus que je me concentrerais.

Ainsi, la collaboration entre le secteur public et le secteur privé serait beaucoup plus robuste. Il y aurait une communication à deux sens et nous planifierions ensemble les événements qui risqueraient de survenir.

[*Français*]

M. Sébastien Lemire: Je crois que vous êtes à même de constater que...

Le président: Malheureusement, monsieur Lemire, je vois les lumières signalant qu'il y a un vote à la Chambre.

[*Traduction*]

Est-ce que les membres du Comité sont d'accord pour que nous poursuivions la séance ou est-ce que vous souhaitez que nous nous arrêtions ici?

Monsieur le greffier, les cloches vont sonner pendant combien de temps; le savez-vous?

Le greffier du Comité (M. Michael MacPherson): Pendant 30 minutes.

Le président: Si les membres du Comité sont d'accord, nous pourrions conclure après l'intervention de M. Lemire. Est-ce que cela vous convient?

M. Churence Rogers: C'est ce que je proposerais, monsieur le président.

Le président: Merci beaucoup, monsieur Rogers.

[*Français*]

Monsieur Lemire, vous pouvez continuer.

M. Sébastien Lemire: Merci, monsieur le président. C'est très apprécié.

Monsieur de Boer, vous êtes à même de constater que la Russie fait de la cyberintimidation et tente d'influencer l'opinion publique dans plusieurs champs d'intérêt. Nous l'avons vu lors des élections américaines, notamment. J'ai ouï dire qu'aux États-Unis, on a tenté d'influencer la perception quant à des projets comme le déploiement et la vente d'hydroélectricité dans le nord-est des États-Unis. Il y aurait eu de l'intimidation de la part de pays étrangers.

Est-ce le genre d'information que vous êtes capable de constater sur le terrain?

[*Traduction*]

M. John de Boer: BlackBerry ne gère pas nécessairement ces renseignements et n'a pas d'incidence [*difficultés techniques*]. Nous nous centrons uniquement sur le volet technique de la cybersécurité. Je ne pourrais pas commenter cet élément de la menace, malheureusement.

[*Français*]

M. Sébastien Lemire: Si des avions russes envahissaient notre espace aérien, est-ce que vous seriez capables de le savoir?

[*Traduction*]

M. John de Boer: Non, nous n'avons pas accès à ces renseignements.

[*Français*]

M. Sébastien Lemire: Parfait. Merci beaucoup.

Le président: Merci beaucoup, monsieur Lemire.

[*Traduction*]

Merci, monsieur de Boer, pour votre présence avec nous aujourd'hui et pour votre témoignage.

Voilà qui conclut les témoignages du Comité sur l'état de préparation du Canada aux menaces posées par la Russie visant les eaux, les ports et l'espace aérien du Canada.

Chers collègues, je vous remercie.

Nous allons reprendre les travaux le lundi 28 mars, à 11 heures. La séance est levée.