CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

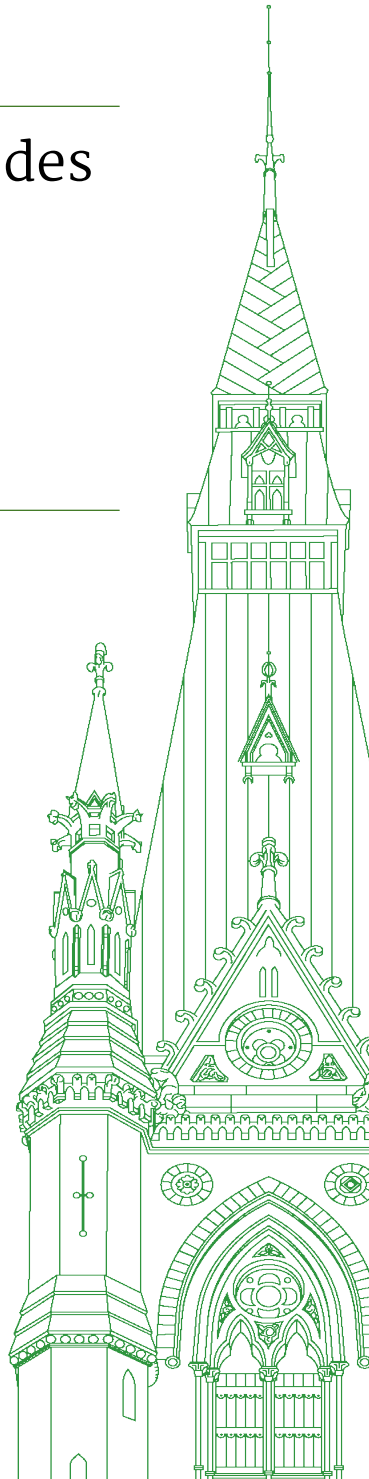
Comité permanent de la procédure et des affaires de la Chambre

TÉMOIGNAGES

NUMÉRO 119

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le jeudi 6 juin 2024



Président : M. Ben Carr

Comité permanent de la procédure et des affaires de la Chambre

Le jeudi 6 juin 2024

● (1100)

[*Traduction*]

Le président (M. Ben Carr (Winnipeg-Centre-Sud, Lib.)): Bonjour à tous.

[*Français*]

J'espère que les derniers jours ont été agréables pour vous.

[*Traduction*]

Chers collègues, nous nous réunissons à l'occasion de la 119e séance du Comité permanent de la procédure et des affaires de la Chambre.

[*Français*]

Le Comité se réunit de nouveau ce matin pour continuer son étude sur la question de privilège concernant des cyberattaques menées contre des députés.

[*Traduction*]

Chers collègues, je pense que nous connaissons tous très bien les règles concernant le son, mais je vous les rappelle très brièvement chaque fois. Veuillez vous assurer de placer votre oreillette à votre droite. Si vous avez besoin de plus d'instructions, elles sont à votre disposition.

Je vais également vous faire un rappel amical utile, je pense, pour garantir l'efficacité et la productivité du Comité, soit d'avoir un chronomètre devant vous. Si vous n'en avez pas, pas de souci, j'en ai un, mais je pense que c'est parfois utile.

Comme lors de la dernière réunion, je ne vois pas d'inconvénient, chers collègues, à reporter une partie du temps. Par exemple, s'il reste 30 secondes au premier tour et que vous ne pensez pas avoir le temps de poser une question de qualité durant ces 30 secondes, c'est correct. Remettez le temps à la présidence, et je le reporterai au tour suivant. Cela nous permet de respecter le temps imparti. Je pense que cette façon de faire est plus juste et plus productive, plutôt que de devoir se presser. C'est toujours possible de le faire.

Les hauts responsables du Centre de la sécurité des télécommunications se joignent à nous aujourd'hui pour les deux heures complètes — pendant la première, la séance sera publique, puis nous passerons à huis clos.

J'aimerais accueillir Mme Caroline Xavier, chef, CST, ainsi que M. Rajiv Gupta, dirigeant associé, du Centre canadien pour la cybersécurité.

Bienvenue à vous deux.

Vous aurez dix minutes au total pour présenter vos déclarations liminaires. Assurez-vous de poser vos questions et de formuler vos commentaires par l'entremise de la présidence.

Sur ce, je vous cède la parole.

Mme Caroline Xavier (chef, Centre de la sécurité des télécommunications): Merci, monsieur le président, de cette invitation à prendre la parole devant vous aujourd'hui.

Je m'appelle Caroline Xavier, comme on l'a mentionné. Je suis la chef du Centre de la sécurité des télécommunications, également appelé CST. Je suis accompagnée de Rajiv Gupta, dirigeant associé du Centre canadien pour la cybersécurité du CST, également appelé le Centre pour la cybersécurité.

Je souhaite commencer par donner au Comité un bref aperçu de l'évolution du paysage en évolution des menaces. Par la suite, je parlerai des activités de cybermenace qui ont été atténuées et qui visaient les parlementaires canadiens et de la façon dont le CST travaille à la protection des parlementaires et des institutions démocratiques de façon plus générale.

[*Français*]

De plus en plus, les adversaires du Canada utilisent la cybermenace pour mener des activités d'espionnage, faire avancer leurs objectifs de politique étrangère et influencer l'opinion publique canadienne à leur avantage.

Bien que nous croyions que la cybercriminalité continue d'être l'activité de cybermenace la plus susceptible de toucher les Canadiens et les organisations canadiennes, la cybermenace provenant de la Chine, principalement, mais aussi de la Russie, de l'Iran et d'autres pays, est la plus importante d'un point de vue stratégique.

[*Traduction*]

Permettez-moi d'être plus précise. La menace émanant de la RPC est presque certainement la plus importante sur le plan du volume et du perfectionnement. Les auteurs de cybermenace parrainés par la RPC continueront presque certainement de cibler les industries et les technologies au Canada afin que la Chine puisse obtenir un avantage pour ses priorités stratégiques, qu'il s'agisse de priorités politiques ou économiques ou de sécurité ou de défense.

Parallèlement, l'invasion russe de l'Ukraine en février 2022 a changé la compréhension mondiale de la façon dont les cyberactivités sont utilisées pour appuyer les opérations en temps de guerre et a démontré que les États-nations ont de plus en plus de capacité et de volonté pour utiliser la mésinformation et la désinformation afin de défendre leurs intérêts géopolitiques.

Depuis 2021, le CST a également observé que les auteurs de cybermenace parrainés par un État qui ont des liens avec la Russie et la RPC continuent de mener la plupart des activités de cybermenace cernées ciblant des élections à l'étranger. Dans la quatrième version du rapport sur les cybermenaces contre le processus démocratique, publiée en décembre 2023, nous avons décrit des exemples de cyberactivité observée à l'échelle mondiale depuis 2021. Cela comprend les attaques par déni de service distribué, ou DDoS, contre des sites Web des organismes électoraux et les modes de scrutin électronique, l'accès non autorisé aux bases de données d'inscription des électrices et électeurs afin de recueillir des renseignements personnels, et les attaques par harponnage contre le personnel électoral et les politiciennes et politiciens, notamment.

Compte tenu de l'observation de cette activité au cours des dernières années, le Centre pour la cybersécurité du CST a diffusé plus de huit alertes, quatre bulletins sur les cybermenaces et sept bulletins de cybersécurité conjoints avec des alliés, tous liés à des activités de cybermenace parrainées par l'État de la Chine ou de la Russie.

Le degré élevé de connectivité mondiale et d'intégration technologique du Canada avec ses alliés accroît son exposition à la menace. De plus, le Canada ne se trouve pas en vase clos, et les cyberactivités qui touchent les processus démocratiques de ses alliés entraîneront probablement des répercussions au Canada aussi.

En ce qui concerne l'étude du Comité, j'aimerais maintenant vous donner un aperçu du rôle du CST et de sa relation avec l'équipe des TI de la Chambre des communes.

Le CST prend son mandat et ses obligations juridiques très au sérieux. Conformément au volet cybersécurité et assurance de l'information de son mandat, le CST acquiert, utilise et analyse de l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir des conseils, du renseignement, des directives et des services pour aider à protéger l'information électronique et les infrastructures de l'information. Par conséquent, conformément à la Loi sur le CST, le CST et son Centre pour la cybersécurité échangent du renseignement et de l'information avec les fournisseurs de services et la clientèle du gouvernement, y compris les autorités compétentes au Parlement.

En juin 2022, le CST a reçu du FBI un rapport qui décrivait des courriels ciblant des personnes de partout dans le monde, y compris des personnes qui s'étaient exprimées publiquement sur les activités du Parti communiste chinois. Le rapport comportait des détails techniques et les noms de 19 parlementaires ayant été ciblés par cette activité. Toutefois, de janvier à avril 2021, plus d'un an plus tard, le Centre pour la cybersécurité avait déjà transmis des rapports aux responsables de la sécurité des TI de la Chambre des communes contenant des indicateurs techniques de compromission par un acteur habile touchant les systèmes de TI de la Chambre des communes.

À la réception de ce rapport, le CST a communiqué des renseignements précis, exploitables et techniques à propos de l'activité aux responsables de la sécurité des TI de la Chambre des communes et au Service canadien du renseignement de sécurité, ou SCRS. Grâce à cette information, le CST et la Chambre des communes ont collaboré pour déjouer la tentative de compromission de cet acteur expérimenté.

● (1105)

[*Français*]

Nous respectons le fait que la Chambre des communes et le Sénat sont indépendants et que leurs représentants sont responsables de déterminer le moment et la manière de communiquer directement avec les députés et les sénateurs. La chronologie complète des événements qui décrit les mesures prises par le Centre de la sécurité des télécommunications pour informer et aider les fonctionnaires parlementaires dans leurs efforts de détection et d'atténuation des cybermenaces a été présentée au greffier du Comité la semaine passée. Il est important de souligner que l'engagement du Centre de la sécurité des télécommunications auprès des responsables de la sécurité des technologies de l'information de la Chambre des communes est bien antérieur au rapport susmentionné du Federal Bureau of Investigation.

[*Traduction*]

En notre qualité de ressource technique centrale pour les conseils en matière de cybersécurité, nous fournissons des avis en temps quasi réel, y compris aux équipes de TI de la Chambre des communes et du Sénat, et avons aidé les responsables parlementaires de la sécurité des TI à mettre en œuvre rapidement des mesures appropriées dans leurs systèmes afin de protéger leur réseau et leurs utilisateurs contre cette menace et d'autres menaces.

Lorsqu'une cybermenace est repérée, le Centre pour la cybersécurité envoie différents types d'avis, notamment les cyberflashs, qui sont des avis urgents envoyés par courriel; des mises à jour quotidiennes sur les logiciels malveillants et les vulnérabilités dans l'espace IP d'un partenaire par l'intermédiaire du National Cyber Threat Notification Service; et des sommaires mensuels des données du NCTNS montrant comment la cybersécurité d'un abonné se classe par rapport à des pairs anonymes dans leur secteur.

Sur demande, nous fournissons des services de cyberdéfense et maintenons une ligne de communication ouverte pour atténuer les menaces possibles. Pour détecter toute cyberactivité malveillante sur les réseaux, les systèmes et les infrastructures infonuagiques du gouvernement, le Centre pour la cybersécurité fait appel à des capteurs autonomes y compris les capteurs au niveau du réseau…

● (1110)

[*Français*]

Mme Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): J'invoque le Règlement, monsieur le président.

Je suis sincèrement désolée d'interrompre la témoin, mais j'ai manqué quand même beaucoup d'éléments, parce que le rythme est trop rapide pour que l'interprète, que je salue, puisse suivre. Ça faisait deux minutes que je me disais…

Le président: D'accord, ça va. Je vais arrêter le chronomètre un moment.

[*Traduction*]

Madame Xavier, pourriez-vous essayer de ralentir la cadence un peu? Je pense que nous avons un écart dans l'interprétation, ce qui fait en sorte qu'il est un peu plus difficile pour certains députés d'entendre.

J'ai arrêté le temps. Il vous reste environ trois minutes et demie. Si vous pouviez faire de votre mieux, ce serait formidable.

Allez-y, monsieur Genuis.

[*Français*]

M. Garnett Genuis (Sherwood Park—Fort Saskatchewan, PCC): Quand ma collègue parlait en français, l'interprétation anglaise ne fonctionnait pas.

Le président: Je crois que ça fonctionne maintenant.

[*Traduction*]

Chers collègues, nous allons faire une deuxième tentative.

[*Français*]

S'il y a encore des problèmes avec l'interprétation, veuillez m'en aviser, et nous prendrons une autre petite pause, le temps de régler le problème.

[*Traduction*]

Madame Xavier, il reste trois minutes et demie.

[*Français*]

Mme Caroline Xavier: D'accord. Excusez-moi de cette interruption.

[*Traduction*]

Sur demande, nous fournissons des services de cyberdéfense et maintenons une ligne de communication ouverte pour atténuer les menaces possibles.

Pour détecter toute cyberactivité malveillante sur les réseaux, les systèmes et les infrastructures infonuagiques du gouvernement, le Centre pour la cybersécurité fait appel à des capteurs autonomes y compris les capteurs au niveau du réseau, les capteurs au niveau du nuage et les capteurs au niveau de l'hôte. Ces systèmes de défense protègent les systèmes d'importance contre 6,6 milliards de tentatives malicieuses en moyenne chaque jour

Le CST continue de surveiller les réseaux et les systèmes importants du gouvernement du Canada en ce qui a trait aux cybermenaces, et il travaille en étroite collaboration avec ses partenaires gouvernementaux, y compris les organismes de sécurité pertinents.

Nous assurons une cyberdéfense fondée sur le renseignement étranger.

[*Français*]

Enfin, j'aimerais souligner aux membres l'appui qui est mis à leur disposition. En effet, le Centre canadien pour la cybersécurité offre un service d'assistance aux parlementaires en plus d'avoir tenu des séances d'information régulières sur les cybermenaces pour les partis politiques et de leur avoir fourni un point de contact attitré au Centre pour obtenir de l'aide en matière de cybersécurité.

[*Traduction*]

Depuis 2017, le CST a publié quatre rapports non classifiés sur les cybermenaces contre le processus démocratique du Canada, et son « Évaluation des cybermenaces nationales 2023-2024 » souligne comment les activités d'influence étrangère en ligne sont devenues une nouvelle norme, alors que des adversaires cherchent à influer sur les élections et sur le discours international portant sur les événements actuels.

À l'échelle interministérielle, le Centre pour la cybersécurité du CST travaille en étroite collaboration avec Élections Canada depuis 2014 pour veiller au maintien de la sécurité de nos systèmes et notre infrastructure électoraux. Le CST continue également de travailler au sein du Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections. Les cyberincidents tels que les rançongiciels, les DDoS et les compromissions de la chaîne d'approvisionnement sont de plus en plus fréquents dans tous les secteurs d'activité, et ces incidents nuisent à notre prospérité, à notre vie privée et à notre sécurité. C'est pourquoi le projet de loi C-26 est si important. Il accorderait au gouvernement de nouveaux outils et pouvoirs qui lui permettront de renforcer les défenses, d'améliorer la sécurité dans les secteurs industriels essentiels sous réglementation fédérale et de protéger les Canadiens et les infrastructures essentielles du Canada contre les cybermenaces.

Quatre secteurs sont assujettis à la déclaration obligatoire des cyberincidents dans le projet de loi C-26: la finance, l'énergie, les télécommunications et le transport. Ceux-ci ont tous été visés en priorité en raison de leur importance pour les Canadiens et d'autres secteurs. Ce sont des facilitateurs essentiels. Le projet de loi C-26 améliorera notre capacité de nous protéger contre les menaces que nous observons aujourd'hui et les menaces auxquelles nous serons confrontés demain.

Le gouvernement fédéral a l'intention de lancer sa Stratégie nationale de cybersécurité modernisée, qui communiquera l'approche à long terme du Canada pour contrer les menaces changeantes dans le cyberespace. Au cœur de la nouvelle stratégie, il y aura un changement de paradigme vers une approche pansociétale de la cyberésilience nationale du Canada, dans le cadre duquel les entités publiques et privées et tous les ordres de gouvernement collaboreront plus étroitement pour se défendre contre les cybermenaces, y compris les menaces contre nos institutions. Le gouvernement a aussi récemment annoncé une mise à jour de sa politique de défense intitulée « Notre Nord fort et libre », qui propose d'accorder de nouveaux investissements importants au CST dans le cadre du budget de 2024.

Enfin, un aspect important de l'approche pansociétale du Canada à l'égard de notre sécurité collective consiste à adopter des pratiques exemplaires en cybersécurité, y compris des pratiques sécuritaires en matière de médias sociaux, surtout pour les personnes qui occupent des postes publics. Le Centre pour la cybersécurité a publié des directives sur les façons de vous protéger en ligne. Il propose également des ressources de cybersécurité pour les organismes électoraux, les campagnes politiques et les électeurs canadiens. J'encourage les personnes à la recherche de conseils faciles à suivre sur la cybersécurité à consulter notre site Web à l'adresse https://www.pensezcybersecurite.gc.ca/fr. Je souhaite également encourager les organisations qui ont été touchées par des cybermenaces à communiquer avec le Centre pour la cybersécurité afin qu'il puisse partager avec ses partenaires des renseignements sur les menaces pour protéger le Canada et les Canadiens en ligne.

De plus, pour faciliter le signalement des cyberincidents pour les Canadiens, le CST travaille également avec ses partenaires fédéraux pour établir une solution à guichet unique pour le signalement des cyberincidents, dans le but ultime de garantir que les Canadiens peuvent toujours trouver l'aide dont ils ont besoin. C'était une recommandation principale de la vérificatrice générale cette semaine.

En conclusion, le CST et le Centre pour la cybersécurité demeurent actifs dans leur collaboration avec leurs partenaires, y compris la Chambre des communes, afin de renforcer la cyberésilience du Canada et de protéger ses institutions démocratiques. Nous continuerons de surveiller les cybermenaces et d'échanger des renseignements sur les menaces avec nos partenaires et les intervenants, comme nous l'avons toujours fait.

● (1115)

[*Français*]

Encore une fois, je vous remercie de nous avoir invités à comparaître devant vous, aujourd'hui. Nous sommes heureux de pouvoir contribuer à cette importante discussion et de vous donner un aperçu de la façon dont le Centre de la sécurité des télécommunications et le Centre canadien pour la cybersécurité travaillent chaque jour à la protection des Canadiens et Canadiennes et de leurs institutions démocratiques.

Je vous remercie de votre attention.

Le président: Merci beaucoup, madame Xavier.

[*Traduction*]

Monsieur Genuis, vous pouvez donner le coup d'envoi à notre première ronde pour six minutes.

La parole est à vous.

M. Garnett Genuis: Merci, monsieur le président.

Pouvez-vous confirmer que le gouvernement a informé l'administration de la Chambre des communes au sujet de la cyberattaque?

Mme Caroline Xavier: Je peux confirmer que, lorsque nous avons pris connaissance en 2021 de certaines anomalies concernant de possibles cyberactivités à l'encontre de la Chambre des communes, nous avons bel et bien informé l'équipe de sécurité des TI de la Chambre des communes.

M. Garnett Genuis: Merci.

Pouvez-vous confirmer que vous lui avez dit quels parlementaires étaient visés?

Mme Caroline Xavier: Ce que je peux dire, c'est que, lorsque le FBI nous a donné les renseignements dont il disposait en juin 2022, la liste des parlementaires, nous avons effectivement communiqué cette liste de parlementaires à l'équipe de sécurité des TI de la Chambre des communes. Nous l'avons également communiquée au SCRS.

M. Garnett Genuis: Merci.

Avez-vous informé de la même façon l'administration de la Chambre des communes au sujet de la source de l'attaque?

Mme Caroline Xavier: Comme je l'ai mentionné dans la chronologie remise au greffier, nous avons exprimé clairement que, depuis janvier 2021, nous observons un acteur expérimenté mener des cyberactivités contre la Chambre des communes. Nous avons fourni 12 rapports à la Chambre des communes. Nous avons également tenu des réunions avec la Chambre des communes et le SCRS. Dans le cadre de ces diverses activités — les réunions et les rapports que nous avons fournis — nous avons pu échanger des renseignements qui allaient se révéler importants pour continuer d'atténuer la menace.

M. Garnett Genuis: Merci, madame, mais je vais répéter la question, car vous n'y avez pas répondu. La question était assez précise.

Avez-vous informé l'administration de la Chambre des communes précisément au sujet de la source de l'attaque?

Mme Caroline Xavier: Dès qu'un cyberincident survient, nous nous efforçons immédiatement d'atténuer la menace. Une fois que nous continuons de faire face à la menace, nous nous efforçons, du point de vue du CST, de mieux comprendre son origine. À mesure que nous obtenons ces renseignements, nous les communiquons aux fournisseurs de services et à ceux qui doivent savoir, surtout si cela peut servir à continuer d'atténuer la menace.

M. Garnett Genuis: Ce n'était pas une question générale. C'était une question précise sur ce que vous avez fait dans ce cas-ci.

Avez-vous informé l'administration de la Chambre des communes au sujet de la source de l'attaque?

Mme Caroline Xavier: Dans le cadre des diverses réunions que nous avons eues et des divers rapports que nous avons fournis, nous avons pu communiquer au personnel de sécurité des TI de la Chambre des communes ce qui, selon nous, était l'origine de la menace.

M. Garnett Genuis: D'accord. C'était une longue façon de dire oui, si j'ai bien compris votre réponse.

Selon votre témoignage aujourd'hui, vous avez communiqué à l'administration de la Chambre des communes la source de l'attaque, soit APT31.

Mme Caroline Xavier: Je pense qu'il serait plus approprié de discuter de certains éléments de la menace pendant la partie à huis clos de la réunion.

M. Garnett Genuis: J'ai simplement répété ce que vous avez dit dans votre réponse précédente, en guise de clarification. Il ne devrait pas être nécessaire de passer à huis clos pour que vous puissiez confirmer si ce que vous venez de dire à l'instant était juste.

Nous avez-vous dit il y a une minute que vous avez informé l'administration de la Chambre des communes qu'APT31 était la source de l'attaque? Est-ce ce que vous avez dit plus tôt, ou ai-je mal compris?

● (1120)

Mme Caroline Xavier: Ce que j'ai dit, c'est que, lorsque nous connaissons la source, ou que nous avons une compréhension générale de la source originale, nous communiquons cette information aux fournisseurs de services et aux personnes qui doivent savoir. Dans le cadre de cette pratique, nous avons échangé plus de 12 rapports avec le personnel des TI de la Chambre des communes et tenu plusieurs réunions.

Dans le cadre de ces réunions, nous avons pu communiquer des renseignements liés à l'élément d'origine.

M. Garnett Genuis: Je ne sais pas ce que vous essayez de nous dire, madame. Je ne crois pas que ce soit une question compliquée. C'est une question claire et précise. Les gens tireront des conclusions si vous éludez la question.

La question est la suivante: avez-vous, oui ou non, à un moment donné, dans une réunion, dit clairement à l'administration de la Chambre des communes que la source de l'attaque était APT31?

Mme Caroline Xavier: Comme je l'ai dit, dans le cadre des nombreuses réunions que nous avons tenues et des rapports que nous avons fournis à la Chambre des communes, nous avons communiqué ce qui, à l'époque, semblait être la source de la menace.

Nous savons maintenant — parce que nous sommes en 2024 et que nous disposons de beaucoup plus de renseignements et de connaissances collectives — qu'il s'agissait d'un acteur appelé APT31.

M. Garnett Genuis: D'accord. Avez-vous, à tout moment, informé l'administration de la Chambre des communes qu'il s'agissait d'APT31, et à quel moment était-ce?

Mme Caroline Xavier: De janvier 2021 jusqu'en… J'oublie la date exacte, car je n'ai pas la chronologie sous les yeux, mais c'était presque un an avant la période en 2022, lorsque nous avons obtenu le rapport du FBI. Nous savions dès janvier 2021 qu'APT31 était une source de préoccupation. Dans le cadre des conversations que nous avons eues avec la Chambre des communes, des exposés que nous lui avons présentés et des rapports que nous lui avons communiqués, nous avons désigné APT31 comme l'acteur potentiel à cette époque.

M. Garnett Genuis: D'accord. Vous nous dites maintenant, à la fin de ce tour, que vous avez informé la Chambre qu'il s'agissait d'APT31. Je vous demande de répondre par oui ou non.

Le président: Veuillez répondre en cinq secondes environ.

Mme Caroline Xavier: Je pense, monsieur le président, que j'ai répondu à la question.

M. Garnett Genuis: C'est donc oui, ou est-ce non?

Le président: Malheureusement, monsieur Genuis, votre temps est écoulé.

[*Français*]

Madame Fortier, vous avez la parole pour six minutes.

L'hon. Mona Fortier (Ottawa—Vanier, Lib.): Merci beaucoup, monsieur le président.

Madame Xavier et monsieur Gupta, je vous remercie d'être ici pour nous aider à faire la lumière sur cette question.

Je vais poursuivre dans la même veine. J'aimerais savoir quand vous avez découvert que la MPA 31, ou menace persistante avancée, était en cause.

Mme Caroline Xavier: Merci beaucoup de la question.

Comme je l'ai dit auparavant, dès le début de janvier 2021, nous avons constaté qu'il y avait des anomalies, des cyberactivités inquiétantes. Nous avons alors communiqué avec les analystes en cybersécurité de la Chambre des communes pour les aviser de ce qui nous inquiétait sur le plan technique. Au fur et à mesure que nous comprenions ce qui se passait, nous leur avons soumis 12 rapports, nous les avons rencontrés et nous avons aussi rencontré nos collègues du Service canadien du renseignement de sécurité, ou SCRS. Nous avons participé aux conversations, et nous avons avisé la Chambre des communes qu'un acteur d'un État-nation était en cause, et qu'il s'agissait en effet de la MPA 31.

L'hon. Mona Fortier: Est-ce que ça s'est fait à ce moment ou plus tard? C'est ce que j'essaie de comprendre.

Mme Caroline Xavier: Ça s'est fait entre le 22 janvier 2021 et le…

L'hon. Mona Fortier: Ça s'est fait avec la Chambre des communes, n'est-ce pas?

Mme Caroline Xavier: Oui, c'est exact.

L'hon. Mona Fortier: Vous avez parlé du fait que vous avez des rencontres et que vous vous échangez de l'information. Faites-vous ça quand vous remarquez quelque chose, une situation spécifique, l'activité d'un groupe? Quel genre d'information transmettez-vous à la Chambre des communes quand vous décelez une menace?

Mme Caroline Xavier: Nous transmettons énormément d'informations, autant que nous le pouvons, surtout quand elles ne sont pas classifiées. Il arrive parfois que nous déclassifiions de l'information s'il est utile de la transmettre.

Je vais demander à M. Gupta, qui était présent lors de certaines de ces conversations, de mettre un peu plus en lumière le type d'information que nous transmettons.

● (1125)

M. Rajiv Gupta (dirigeant associé, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Merci, monsieur le président.

[*Traduction*]

Lorsque l'on parle de communication de renseignements classifiés, il y a beaucoup de contexte et d'information, mais il y a souvent une ligne de démarcation, c'est-à-dire un autre ensemble d'informations que vous pouvez fournir à l'intervenant en cas d'incident ou à une autre organisation pour lui permettre de prendre des mesures immédiates pour résoudre un incident. Dans la période qui précède l'incident, nous communiquerions des renseignements situés à la ligne de démarcation: « Voici un auteur de menaces habile », ce qui, dans le domaine de la cybersécurité, signifie généralement un État-nation, et c'est très important. Cela renforce incontestablement la gravité et l'importance de l'événement.

Cependant, tout ce que nous sommes autorisés à communiquer, en raison du renseignement, ce sont les indicateurs techniques. Nous n'avions pas les adresses courriel, alors nous fournissions tous les renseignements nécessaires pour trouver les adresses courriel. C'est ce que nous avons communiqué à la Chambre des communes, et nous avons collaboré avec elle pour découvrir exactement ce qui se passait, car il y a habituellement un fil conducteur.

L'hon. Mona Fortier: Si c'est dans le cadre de votre collaboration avec la Chambre des communes que vous essayez de découvrir ce qui est arrivé, alors quel est ce rôle? La Chambre des communes va-t-elle revenir vous dire: « Voici ce que nous avons découvert? » ou devez-vous lui dire: « Trouvons quelque chose »? Comment est cette relation?

M. Rajiv Gupta: Nous avons commencé à remonter le fil conducteur en disant: « Hé, voici ce que nous savons. Trouvez vos courriels. » Nous n'avions pas les courriels. Nous avions l'outil nous permettant de rechercher des courriels. Ils allaient les chercher. C'est ce qu'ils ont fait, puis ils sont revenus avec cette information. Chaque fois que nous avons trouvé de nouveaux éléments, ils ont compris la portée de l'incident. C'est ainsi que nous collaborons avec la Chambre des communes, et nous le faisons depuis une dizaine d'années ou plus.

[*Français*]

L'hon. Mona Fortier: Pendant la période visée par cet incident, vous avez eu des échanges réguliers. La chronologie des événements que vous avez fournie aux membres du Comité indique que, le 18 février 2021, il avait été décidé que le SCRS collaborerait avec la Chambre, et que l'Équipe de gestion des événements de cybersécurité du Centre canadien pour la cybersécurité avait fourni au SCRS une liste de questions techniques pour l'aider à analyser l'activité suspecte.

Pourquoi a-t-il été décidé que le SCRS jouerait un rôle d'intermédiaire entre le Centre de la sécurité des télécommunications et la Chambre des communes?

Mme Caroline Xavier: Je vous remercie beaucoup de la question.

Nous prenons notre rôle très au sérieux. Pour nous, il est important de ne pas conserver de renseignements personnels sur des Canadiens dans les données du CST, puisque notre rôle se joue dans la sphère internationale. Quand nous comprenons que l'origine d'une menace envers le Canada vient de l'étranger, il est très naturel pour nous de passer le flambeau au SCRS, parce que ce dernier a le mandat d'agir au Canada. Nous prenons donc très au sérieux le fait de ne pas intervenir et faisons attention à ne pas gérer de renseignements personnels. La raison pour laquelle nous avons passé le flambeau au SCRS dans cette situation-ci est parce que l'incident devait être géré ici, au Canada.

L'hon. Mona Fortier: Le Centre de la sécurité des télécommunications sait-il si un suivi a été effectué auprès des parlementaires pour s'assurer qu'ils avaient été prévenus et qu'ils comprenaient les mesures à prendre, et pour répondre à leurs questions sur la menace elle-même?

Mme Caroline Xavier: Comme l'a dit mon collègue M. Gupta, lorsque nous gérons un incident impliquant une institution, nous entretenons une relation constante avec elle pour mieux comprendre la menace. Elle nous apporte des informations aussi.

Sauf dans le cas de la Chambre des communes, il arrive qu'une institution gère tout à l'interne et nous informe de l'incident seulement une fois celui-ci réglé. Il est aussi possible qu'elle ne nous en informe jamais.

Le président: Merci, madame Fortier.

Madame Gaudreau, vous avez la parole pour six minutes.

Mme Marie-Hélène Gaudreau: Je n'ai pas entendu correctement votre allocution d'ouverture, alors il se peut que je pose des questions.

Si on revient au départ, le mandat du Centre de la sécurité des télécommunications consiste à protéger les infrastructures numériques. Vos clients sont, entre autres, le gouvernement, l'administration publique, la Défense nationale et certaines entreprises que vous avez mentionnées. Est-ce exact?

Mme Caroline Xavier: Je vous remercie de votre question.

Oui, notre mandat consiste à protéger les systèmes du gouvernement et les infrastructures critiques au Canada, mais nous avons aussi un mandat international. Même si notre mandat ne consiste pas à protéger directement des individus, vous trouverez sur notre site Web de l'information sur la façon d'améliorer la cyberhygiène des individus.

Notre mandat premier est de protéger le Canada et les Canadiens, surtout les systèmes du gouvernement, les industries, les infrastructures critiques, et les secteurs de communication du gouvernement, entre autres.

● (1130)

Mme Marie-Hélène Gaudreau: D'accord. Étant donné que nous vivons un virage assez important, les députés deviennent des acteurs névralgiques. Font-ils partie de la liste des personnes auxquelles vous offrez des services?

Mme Caroline Xavier: Oui, ils en font partie. Depuis 2019, nous offrons aux parlementaires la possibilité de recevoir du soutien du Centre canadien pour la cybersécurité, surtout s'ils ont des problèmes à la suite d'incidents de cybersécurité. Ça fait aussi partie des services que nous offrons, mais il est très important que les parlementaires nous contactent s'ils veulent notre aide.

Mme Marie-Hélène Gaudreau: Pouvez-vous m'expliquer en quoi ces services consistent?

Mme Caroline Xavier: Comme je l'ai dit avant, nous faisons très attention à ne pas collecter d'information sur les Canadiens. Il est donc très important, lorsque des Canadiens ou des parlementaires communiquent avec le Centre canadien pour la cybersécurité pour obtenir du soutien, que tout se déroule de façon adéquate afin que nous puissions offrir le soutien nécessaire pour gérer l'incident sans entrer dans leur vie privée.

Mme Marie-Hélène Gaudreau: Pour ce qui est de l'information divulguée, croyez-vous que l'Administration de la Chambre des communes a suffisamment de détails pour pouvoir agir directement auprès des députés en question?

Mme Caroline Xavier: Je ne veux pas répondre pour l'Administration de la Chambre, alors il vaudrait mieux lui poser la question directement.

Cela dit, comme l'a mentionné M. Gupta, nous avons une très bonne relation avec l'Administration de la Chambre des communes. Nous collaborons avec elle depuis 2012 et la relation n'a cessé de s'améliorer. En 2016, nous avons mis en place avec elle un protocole d'entente pour nous assurer que la relation se poursuive de façon adéquate.

Mme Marie-Hélène Gaudreau: Des gens de l'Administration de la Chambre sont venus nous parler des menaces persistantes avancées, ou MPA. Ce que j'en ai compris, c'est que l'information divulguée était insuffisante. J'ai cru voir une image où on donne une information, mais c'est comme trouver une aiguille dans une botte de foin.

J'ai compris tantôt que les choses avaient beaucoup évolué en ce qui concerne le protocole et l'information pertinente en lien avec la MPA 31. Pouvez-vous me fournir davantage d'explications sur le sujet?

Mme Caroline Xavier: Je vais demander à M. Gupta de vous répondre, parce que, comme je l'ai dit, il a été très impliqué à l'époque, en 2021. Je pense qu'il pourrait vous donner une meilleure réponse.

[*Traduction*]

M. Rajiv Gupta: Je pense que, afin de comprendre les répercussions, comme je l'ai mentionné, nous avons échangé une série de rapports au cours des premières semaines qui nous aidaient à remonter le fil conducteur et à comprendre ce qui se passait. C'était en 2021, avant la vaccination contre la COVID. C'était donc très difficile de faire venir les gens dans les salles. Nous travaillions, mais tout le monde n'était pas forcément au bureau. Nous avons donc organisé une réunion classifiée pour nous assurer que nous comprenions toutes les ramifications. Nous pourrons peut-être en parler pendant la séance à huis clos, mais c'est ainsi que nous fonctionnons. Nous échangeons les renseignements que nous pouvons, puis nous essayons d'organiser des réunions classifiées pour nous assurer que l'ensemble du contexte est bien compris.

[*Français*]

Mme Marie-Hélène Gaudreau: D'accord.

Concernant le rapport du Federal Bureau of Investigation en juin 2022, j'ai une question bien simple à poser: avez-vous suffisamment de ressources humaines et de capacités techniques? Ça va à vitesse grand V, et vous avez dit à quel point les stratégies et les stratèges étaient clairement différents. Avons-nous ce qu'il faut?

Mme Caroline Xavier: Je vous remercie de cette question.

Je suis très fière de notre organisme. Nous avons des gens extraordinaires qui travaillent très fort pour les Canadiens et les Canadiennes. L'injection de fonds prévue dans le budget de 2022 nous aide à faire progresser nos activités en matière de cybersécurité et à remplir notre mandat. L'injection de fonds proposée dans le budget de 2024 nous donnerait des ressources additionnelles pour accomplir notre travail pour les Canadiens et les Canadiennes. Pour nous, il s'agit d'une marque de confiance de la part du gouvernement envers nos capacités, et nous en sommes très fiers. Nous nous engageons à répondre à la demande.

● (1135)

Mme Marie-Hélène Gaudreau: Merci beaucoup, monsieur le président.

Le président: Merci, madame Gaudreau.

[*Traduction*]

Madame Mathyssen, la parole est à vous pour six minutes.

Mme Lindsay Mathyssen (London—Fanshawe, NPD): Merci, monsieur le président.

Merci aux témoins. Je vous remercie d'être ici avec nous aujourd'hui.

Je vais peut-être me répéter un peu, mais juste pour que cela soit clair dans mon esprit également, vous avez parlé des premières communications avec la Chambre des communes lorsque vous avez pris connaissance des attaques en janvier 2021. Notre préoccupation, bien sûr, c'est qu'il y a eu une longue période, et je le comprends certainement, entre le moment où les conversations ont eu lieu, le moment où vous en avez appris davantage au fil du temps et le moment de votre signalement. C'est très bien. Je pense que l'élément essentiel ici, cependant, c'est que, à tout moment donné, rien de tout cela n'a été signalé aux députés en question. C'est ce sur quoi nous devons enquêter. Nous devons déterminer si c'est le problème.

Pourriez-vous répéter, pour ma gouverne, pourquoi c'est si important qu'il y a presque un clivage? Il y a cet espace où vous ne communiquez pas directement avec les députés une fois qu'il est déterminé que cet acteur habile existe, comme vous l'avez défini. Pourquoi cette position intermédiaire est-elle si importante? Pourquoi n'auriez-vous pas pu communiquer conjointement avec les députés concernés? Regardez-vous peut-être les avantages ou les désavantages de cette façon de faire? C'est un processus d'apprentissage constant. Je le comprends également. Comment les choses pourraient-elles changer dans l'avenir? Vous demandez-vous comment nous pouvons aller de l'avant à partir d'ici?

Mme Caroline Xavier: Merci beaucoup de poser la question.

Une chose qu'il convient de souligner, c'est que nous travaillons très fort pour informer les Canadiens et les entreprises des divers rapports que nous publions. Comme je l'ai mentionné, depuis 2017, nous avons publié trois mises à jour des « Cyberattaques contre le processus démocratique du Canada », et aussi quatre éditions de l'« Évaluation des cybermenaces nationales ». Ce sont des documents qui aident à mettre en lumière certaines des menaces que nous constatons et observons en fonction d'une foule de recherches ainsi que des observations réalisées dans les systèmes canadiens également.

Par ailleurs, nous tenons également un nombre assez important de séances d'information, et nous en avons tenu certaines avec des parlementaires, soutenues par d'autres instances comme le service et la GRC. Nous sommes très heureux de pouvoir tenir des séances d'information conjointe avec quiconque souhaite notre présence, les renseigner sur le domaine de la cybersécurité en particulier, car plus il y a de gens au courant des menaces, plus nous devenons résilients comme pays et comme personnes.

Le hic, toutefois, c'est que nous sommes très respectueux de l'indépendance de la Chambre des communes et du Sénat ainsi que du rôle que l'administration de la Chambre des communes joue pour soutenir les parlementaires. C'est pourquoi nous passons par eux, comme nous le faisons pour de nombreux autres fournisseurs de services et autres institutions avec qui nous traitons. Nous passons par eux, et nous sommes à leur service s'ils souhaitent obtenir plus de soutien de notre part. Nous serions plus qu'heureux de continuer de tenir des séances avec les parlementaires si l'administration de la Chambre des communes voulait notre aide pour organiser une séance conjointe. Nous sommes assurément disponibles pour le faire.

Soit dit en passant, le ministère de la Sécurité publique a communiqué avec le sergent d'arme, et trois séances sont actuellement prévues pour un caucus dont nous ferons partie, par exemple, avec la Sécurité publique ainsi que la GRC et le service. Vous voyez que ce sont des services que nous sommes prêts à rendre, mais nous essayons simplement de continuer d'être très respectueux des processus en place et, surtout, de l'indépendance de la Chambre des communes dans ce rôle.

Mme Lindsay Mathyssen: Je vous en suis certainement reconnaissante. Notre caucus tiendra une séance d'information la semaine prochaine, je pense. Cependant, cela concerne davantage… Ces séances d'information sont très générales et elles sont très différentes que lorsque des députés individuels sont ciblés. Encore une fois, y a-t-il un changement pour ce qui est de…? Je comprends tout à fait que l'indépendance du Parlement soit essentielle, mais c'est en fait ce dont nous parlons ici concernant la menace ou cette atteinte potentielle au privilège qui est la source d'inquiétude de ces études et de la réunion. C'est ce qui est en jeu ici également.

Pour être plus précise, y a-t-il une chose que nous ayons apprise de cette affaire et que nous avons jugée comme étant un problème? De toute évidence, les gens concernés ne le se sont pas fait dire de la manière dont il le fallait. Fait-on des changements pour s'assurer que l'atteinte au privilège ne devienne pas un enjeu futur?

● (1140)

Mme Caroline Xavier: Merci beaucoup de la question et de la précision.

Nous sommes une organisation qui se considère essentiellement comme une organisation apprenante, alors nous continuons de rechercher des moyens de nous améliorer. Cela fait partie de l'apprentissage, de pouvoir déterminer en quoi nous pouvons améliorer nos processus, en plus de tous les organes d'examen externe et des divers rapports produits concernant d'autres enjeux, comme l'ingérence étrangère.

Nous continuerons d'apprendre de cette expérience pour améliorer ces processus et travailler avec la Chambre des communes afin de trouver une meilleure voie à suivre.

En général, toutefois, lorsqu'il s'agit de repérer une personne qui pourrait être visée par un cyberincident parce que nous l'avons appris d'une source étrangère, nous transmettons généralement cette information au service, comme je l'ai mentionné plus tôt, pour la simple raison que cela devient alors une question nationale et que cela n'est pas dans nos cordes. Ce n'est pas non plus notre façon de faire. Parfois, la GRC interviendra, surtout s'il s'agit d'une affaire nécessitant l'intervention des forces de l'ordre. Dans ce cas, nous transmettons l'information à la Chambre des communes et au SCRS, afin qu'ils puissent la transmettre aux députés concernés.

Le président: Merci beaucoup, madame Mathyssen.

D'accord, mesdames et messieurs. Nous commençons notre deuxième tour.

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

M. Garnett Genuis: Merci, monsieur le président.

Je dois commencer par dire, en réponse à la série de questions avec Mme Mathyssen, que je trouve absolument ridicule de dire que l'institution gouvernementale éprouve tant de respect pour les parlementaires qu'elle leur cache des choses concernant leur propre sécurité. Ce n'est pas ainsi qu'on manifeste le respect dans les relations dont je fais partie, en cachant des choses essentielles aux gens.

Madame, lorsque le Parlement a été renseigné au sujet des aspects de cette menace, vous attendiez-vous à ce que le service des TI de la Chambre des communes informe les députés au sujet des menaces précises?

Mme Caroline Xavier: Selon notre compréhension, oui, je m'attends à ce que, si je transmets de l'information à un partenaire, ce partenaire fasse le nécessaire pour réagir au contenu de l'information fournie…

M. Garnett Genuis: Je suis désolé, madame. Vous avez vraiment usé de faux-fuyants lors de mon dernier tour. Je vais insister davantage, parce qu'éluder des questions est une affaire qui concerne les privilèges des parlementaires.

C'était une question très précise. Vous attendiez-vous à ce qu'ils renseignent les députés menacés au sujet de ces menaces?

Mme Caroline Xavier: Nous nous attendons à ce que les informations que nous transmettons soient utilisées par d'autres. Nous avons transmis une liste de noms, et nous nous attendons à ce que quelqu'un prenne des mesures en conséquence, que ce soit le SCRS ou, comme présentement, la Chambre des communes.

M. Garnett Genuis: Pardon, mais ce n'est pas ce que j'ai demandé. Ce n'est pas du tout ce que j'ai demandé. Je n'ai pas demandé si vous vous attendiez à ce que quelqu'un prenne des mesures en conséquence. Le travail de l'équipe des TI de la Chambre des communes est de protéger les systèmes de TI.

M. Chad Collins (Hamilton-Est—Stoney Creek, Lib.): J'invoque le Règlement, monsieur le président. J'aimerais entendre les réponses. Je ne pense pas qu'on a entièrement donné au témoin l'occasion de répondre.

M. Garnett Genuis: Alors, faites-le quand ce sera votre tour. S'il vous plaît, apprenez les règles du Comité, monsieur Collins.

J'ai mes cinq minutes, puis vous aurez vos cinq minutes.

M. Chad Collins: Peut-être que vous pourriez simplement faire preuve d'un peu de décence en permettant à la témoin de donner une réponse complète?

Le président: Monsieur Collins, j'entends votre rappel au Règlement.

Monsieur Genuis, quand un député invoque le Règlement, je vous demanderais de le laisser finir.

M. Chad Collins: Ce serait une très bonne chose... un peu de respect.

M. Garnett Genuis: Et vous devriez respecter les règles. J'ai mon temps de parole.

Le président: J'ai bien arrêté le temps, monsieur Genuis, alors le rappel au Règlement ne vous a pas fait perdre de temps.

Il vous reste trois minutes et dix secondes.

Je vous redonne la parole, monsieur Genuis.

M. Garnett Genuis: Merci, monsieur le président.

Si cela n'intéresse pas les députés libéraux de creuser pour obtenir des réponses, c'est leur choix, et cela ressort clairement de cette interruption.

Je m'adresse à nouveau à la témoin: j'ai posé une question très précise, que voici: vous attendiez-vous à ce que l'équipe des TI de la Chambre des communes prenne ces informations et aille en informer les parlementaires qui étaient menacés?

● (1145)

Mme Caroline Xavier: Je transmettrai l'information, et je vais demander à M. Gupta s'il aimerait répondre, puisque, comme je l'ai dit, il était présent à ce moment-là et aurait donc une meilleure compréhension de quelles étaient les attentes.

M. Garnett Genuis: Est-ce parce que vous l'ignorez? Je serais content d'écouter ce que M. Gupta a à dire, mais est-ce parce que vous ne connaissez pas la réponse à la question?

Mme Caroline Xavier: C'était parce que je n'étais pas présente personnellement. Je m'attendrais, effectivement, à ce que si je transmets de l'information à une organisation ou à la Chambre des communes, qu'elle prenne des mesures en conséquence, et qu'elle prenne l'information et la transmette...

M. Garnett Genuis: Comprenez-vous que ce n'est pas ce que je demande? Je n'ai pas demandé si une autre organisation allait prendre des mesures. J'ai demandé si on allait transmettre l'information aux parlementaires. Vous ne pouvez même pas me dire si vous vous attendiez à ce qu'on transmette l'information aux parlementaires. Voilà ce que je veux savoir: vous attendiez-vous à ce qu'on prenne ces informations et qu'on nous en informe, moi et d'autres?

Mme Caroline Xavier: Quand nous avons transmis les informations, qui comprenaient des noms, lorsque nous avons pris connaissance des noms en juin 2022, nos attentes étaient que nous allions transmettre l'information, et que des mesures seraient prises en conséquence pour atténuer les risques, donc qu'on allait intervenir.

M. Garnett Genuis: Encore une fois, vous ne répondez pas à la question. Je ne vous ai pas demandé si vous vous attendiez à ce que des mesures soient prises. Ma question est: est-ce que vous vous attendiez à ce que les parlementaires soient informés? Vous attendiez-vous à ce que le service informe les parlementaires, oui ou non?

Mme Caroline Xavier: Si une des mesures prises consistait à informer les parlementaires, alors je m'attendrais, effectivement, à ce qu'on le fasse.

M. Garnett Genuis: Était-ce l'une des mesures prises? Avez-vous recommandé que les parlementaires soient informés? Répondez par oui ou par non.

M. Rajiv Gupta: Je n'étais pas présent, lors de cette discussion. Cependant, j'ai déjà travaillé avec la Chambre des communes. Nos attentes sont fondées sur...

M. Garnett Genuis: Ma question ne concerne pas ce que vous avez fait par le passé. J'aimerais que vous répondiez par oui ou par non à une question simple. J'essaie d'obtenir une réponse durant mes cinq minutes. Je sais pour qui vous travaillez, mais cela ne vous dispense pas de l'obligation de répondre aux questions qui vous sont posées devant un comité parlementaire.

Je vous repose la question: vous attendiez-vous — et avez-vous communiqué une telle attente aux fonctionnaires de la Chambre des communes — à ce que l'information soit transmise aux parlementaires, oui ou non?

M. Rajiv Gupta: Dans notre collaboration avec la Chambre des communes, les fonctionnaires ont insisté, depuis le premier jour et durant la dizaine d'années et plus encore où nous avons travaillé avec eux, pour dire que l'indépendance de la Chambre des communes est d'une importance capitale. Ils comprennent leurs clients.

M. Garnett Genuis: Oui ou non?

M. Rajiv Gupta: Nous avons travaillé avec eux de nombreuses fois. D'après ce que je sais, après avoir travaillé avec eux dans le passé en lien avec d'autres incidents et après avoir vu ce qui a été fait, nous avons discuté de ce qui était arrivé avec eux, et ils sont partis de leur côté pour faire leur travail.

M. Garnett Genuis: Vous attendiez-vous à ce qu'ils...

M. Rajiv Gupta: D'après ce que j'ai vu dans le passé, je m'attendais à ce que nous ayons le même genre de discussion, puis que selon leur interprétation des seuils... Je ne sais pas quel seuil doit être atteint avant que le sergent d'armes de la Chambre des communes aille effectivement informer une personne...

M. Garnett Genuis: Avez-vous communiqué une attente, ou non?

M. Rajiv Gupta: Nous communiquons la menace et le contexte, pour qu'il soit compris quelle est la nature exacte de la menace...

M. Garnett Genuis: Donc, vous n'avez pas communiqué l'attente.

M. Rajiv Gupta: Une attente selon laquelle on allait informer... Nous ne leur disons pas d'aller informer... pas en disant « Vous devez aller les informer maintenant. » Nous leur disons: « C'est très important, parce que vos députés sont exposés à un risque. » Voilà le genre de choses que nous disons. Nous ne disons pas: « Allez les informer. »

Le président: Merci beaucoup, monsieur Genuis.

Vos cinq minutes sont écoulées.

La parole va à Mme Romanado pour cinq minutes.

Mme Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Merci beaucoup, monsieur le président. Par votre entreprise, j'aimerais remercier les témoins d'être avec nous aujourd'hui.

Nous avons reçu la chronologie des événements que vous nous avez envoyée. Merci beaucoup.

D'après cette chronologie et votre témoignage aujourd'hui, il semble que la communication entre le Centre pour la cybersécurité et l'équipe des TI de la Chambre des communes était pour ainsi dire un dialogue à sens unique. J'ai vu nombre d'indications selon lesquelles l'équipe des TI de la Chambre des communes ne vous a pas renvoyé de commentaires ou n'a pas fait le suivi avec le Centre, même si cela a été demandé.

Pouvez-vous confirmer que c'est ce qui est arrivé, entre le 22 janvier, lorsque vous avez commencé à détecter ces activités, et le moment où le FBI vous a transmis le rapport?

Ai-je raison?

Mme Caroline Xavier: Je vais demander à M. Gupta de répondre.

M. Rajiv Gupta: Merci beaucoup.

D'après ce que nous savons... Vous pouvez voir la chronologie; le fil des événements est bien détaillé.

Nous demandions des informations. Nous ne savons pas ce qui se passe de l'autre côté, par rapport au temps nécessaire pour accéder à cette information. Comme je l'ai dit, c'est une collaboration. Nous avons bien travaillé avec la Chambre des communes dans le passé et avons énormément de respect pour ces gens.

Je pense que, quand nous avons fini par nous réunir, nous avons échangé des informations. Nous avons échangé ces informations. Vous pouvez voir sur le fil du temps quand cela a eu lieu.

Mme Caroline Xavier: J'ajouterais que ce n'est pas anormal, pour n'importe quel incident de cybersécurité qui nous concerne, surtout quand il s'agit de renseignements critiques ou d'une entreprise du secteur privé, que l'information semble aller seulement dans un sens, parce que les gens de l'autre côté gèrent leurs propres problèmes. Ils sont dans le feu de l'action. Ce n'est pas anormal qu'il leur faille du temps pour finalement nous répondre, et possiblement ne pas nous répondre. C'est ce qui arrive parfois.

M. Rajiv Gupta: Une chose que j'aimerais ajouter est que l'auteur des menaces ayant infiltré les réseaux de la Chambre des communes utilisait des méthodes très perfectionnées. Nous avons détecté ses toutes premières actions. Les liens de suivi constituent la première étape. Ensuite vient l'étape de l'injecteur, et l'étape suivante serait le logiciel d'exploitation en tant que tel, ce qui aurait été très grave.

Nous aimerions insister sur le fait que les mesures prises par la Chambre des communes et nous-mêmes ont empêché que les réseaux de la Chambre des communes soient compromis par cet auteur de menaces très habile.

● (1150)

Mme Sherry Romanado: Vous avez mentionné le réseau de la Chambre des communes. Nous savons que, en ce qui concerne M. Genuis, son courriel personnel a aussi été ciblé. D'après ce que l'équipe des TI de la Chambre des communes nous a dit, nous savons qu'elle ne surveille évidemment pas les courriels personnels des députés.

Je tiens pour acquis que le CSTC est capable de voir, qu'il s'agisse des adresses courriel de la Chambre des communes ou d'une adresse courriel personnelle — vous n'avez pas divulgué comment vous faites ce que vous faites publiquement —, mais il semble y avoir un écart quelque part, parce que les députés ont évidemment leurs propres adresses personnelles, pour leurs activités personnelles ou partisanes. Dans ce cas-ci, il semble y avoir eu une lacune au niveau de la personne chargée d'avertir les députés que leurs courriels personnels recevaient des pourriels.

J'aimerais céder le reste de mon temps à M. Collins. Je sais qu'il avait aussi quelques questions à poser.

Merci.

M. Chad Collins: Merci, et merci aux témoins de leur présence aujourd'hui.

Vous avez mentionné l'approche fondée sur le travail d'équipe. M. Gupta a dit que vous avez une relation de travail avec vos partenaires depuis une dizaine d'années. Vous avez utilisé le mot « partenaire » plusieurs fois dans votre déclaration. C'est un environnement d'équipe. Quelqu'un a mentionné, en réponse à une des questions, un protocole d'entente.

Dans quel contexte est-ce que cela a été conclu? Est-ce que cela a un lien avec certaines des questions ou certains des enjeux qui ont été soulevés durant la réunion d'aujourd'hui, ou lors de la dernière réunion?

Mme Caroline Xavier: Quand nous devons travailler avec une entité qui se trouve au Canada en particulier, ou avec n'importe quelle entité avec qui nous allons peut-être échanger des données dont nous pourrions avoir besoin pour faire des analyses visant à mieux identifier une menace et à mieux comprendre ses origines, nous mettons souvent en place un protocole d'entente ou un instrument du même genre afin de définir très clairement comment et pourquoi les informations seront échangées.

Cela revient au fait que notre mandat est très rigoureux pour ce qui est de protéger les renseignements personnels des Canadiens et faire en sorte que ces droits ne soient pas violés. Plus précisément, lorsqu'il s'agit surtout d'une organisation qui prend peut-être en charge certains des services que nous offrons — les capteurs au niveau de l'hôte, les capteurs au niveau du réseau et les capteurs au niveau du nuage — dépendamment des services pris en charge par cette organisation, ce serait une autre raison de mettre en place un protocole d'entente. Cela vise l'échange d'informations qui a lieu ou possiblement le soutien pour une capacité de surveillance, afin que nous puissions continuer de renseigner, de tirer des leçons et de clairement définir comment les données sont gérées.

Le président: Monsieur Collins, votre temps est malheureusement écoulé, mais je vais vous donner cinq minutes de plus à la toute fin du tour.

[*Français*]

Madame Gaudreau, vous avez la parole pour deux minutes et demie.

Mme Marie-Hélène Gaudreau: Merci, monsieur le président.

Madame Xavier, j'ai trois questions à vous poser et je crois avoir suffisamment de temps.

Tantôt, j'ai été rassurée quand j'ai demandé si les services étaient suffisants, notamment en ressources humaines. J'ai été retournée d'apprendre que le 11 octobre 2023, il n'y a pas si longtemps, CBC mentionnait que le Centre de la sécurité des télécommunications était en crise. Ce n'est contre personne, on veut essayer d'être constructif. Est-ce qu'il y a eu un virage à 180 degrés pour m'annoncer aujourd'hui que vous seriez disposée à moduler advenant que l'Administration de la Chambre ou même la loi soit modifiée?

Mme Caroline Xavier: Je vous remercie de la question.

Je ne suis pas sûre de savoir à quel article de CBC vous faites référence. Cependant, je peux vous dire que, lors d'une entrevue avec Mme Bureau, si ma mémoire est bonne, nous avons parlé des ressources et des talents que le Centre de la sécurité des télécommunications recherche et dont il a besoin.

Dans cette entrevue, j'ai dit qu'il n'y avait pas que le Centre canadien pour la cybersécurité et le Centre de la sécurité des télécommunications qui étaient à la recherche de ces talents. En fait, ces talents sont très recherchés partout au Canada et dans le monde, puisque tout devient numérique.

Je pense qu'il vaut la peine de dire qu'il y a énormément d'intérêt envers le Centre de la sécurité des télécommunications. C'est la raison pour laquelle nous nous sentons très capables de répartir nos ressources selon le budget qui nous a été accordé.

Mme Marie-Hélène Gaudreau: Ça m'amène à demander comment se fait-il que nous soyons ici aujourd'hui avec mon collègue M. Genuis? De l'information a été divulguée, mais nous nous attendions à ce que les individus, dont M. Genuis, soient au courant. Nous faisons ça aujourd'hui. Qu'est-ce que nous avons manqué? Que devons-nous corriger? C'est essentiel.

Il vous reste 30 secondes pour répondre à mes questions.

● (1155)

Mme Caroline Xavier: Merci.

Comme je l'ai dit, en tant qu'organisme, nous aimons continuer à apprendre et à mieux faire les choses. Lors de votre étude, vous allez faire certaines recommandations. De là, nous allons être peut-être capables de faire mieux. Le Centre de la sécurité des télécommunications ne crée pas les politiques. En fait, on nous donne des actions à exécuter, et nous faisons de notre mieux pour le faire.

Mme Marie-Hélène Gaudreau: Merci.

Monsieur le président, j'aimerais quand même inviter le Centre de la sécurité des télécommunications à nous fournir des éléments précis, parce que vous savez de quoi vous parlez, évidemment, au fond du rapport.

Le président: Merci, madame Gaudreau. Je vous remercie aussi d'avoir joué le rôle du président en rappelant à la témoin combien de temps il vous restait.

[*Traduction*]

Madame Mathyssen, vous avez la parole pour deux minutes et demie.

Mme Lindsay Mathyssen: Merci.

J'aimerais revenir à la discussion sur le fait que l'information semblait aller seulement dans un sens, du CSTC à la Chambre des communes. Vous avez dit que c'était normal. Vous donnez de l'information à une organisation, mais vous dites que vous ne vous attendez pas à ce qu'on fasse le suivi avec vous par rapport à ces informations, ou alors, vous permettez à l'autre organisation de s'occuper de ce qui est arrivé. Vous ai-je bien compris?

Mme Caroline Xavier: Oui. Comme cela a été dit, un incident de cybersécurité constitue habituellement un moment de crise pour une organisation. Par conséquent, notre travail est de fournir du soutien. Parfois, c'est nous qui communiquons avec l'organisation pour lui dire que nous avons remarqué des activités suspectes. Parfois, l'organisation a elle-même identifié un incident de cybersécurité, alors nous l'appelons et nous lui demandons s'il y a quoi que ce soit que nous pouvons faire pour l'aider. Parfois, nous avons des communications régulières et continues dans les deux sens.

Toutefois, il arrive qu'une entreprise choisisse de faire affaire avec un fournisseur de services externe pour obtenir du soutien, et dans ce cas-là, nous assumons davantage un rôle de surveillance, et nous attendons de voir...

Une organisation ne va pas automatiquement communiquer avec nous et ne va pas nécessairement continuer de travailler avec nous. Ce n'est pas parce qu'elle ne veut pas. Parfois, surtout lorsqu'il est question de cybersécurité, nous n'encourageons pas les organisations à payer en cas d'infection par un rançongiciel, et c'est parfois une raison pour laquelle une entreprise décidera de ne pas faire affaire avec nous, parce que nous sommes une entité gouvernementale. Elle a peur de ce que cela pourrait supposer.

Même si nous ne sommes pas tous des organismes d'application de la loi — nous ne sommes pas un organisme de réglementation —, nous travaillons dur pour établir des relations de confiance, et je pense que c'est une chose que nous faisons quotidiennement. Malgré tout, je ne veux pas induire qui que ce soit en erreur en lui faisant croire que cela veut dire que nous sommes au courant de tous les cyberincidents qui surviennent dans le secteur privé, par exemple, ou dans les infrastructures essentielles.

Mme Lindsay Mathyssen: Je comprends, et je ne m'attendrais pas... il doit y avoir une certaine liberté de choix, mais est-ce que cela n'entraîne pas des risques supplémentaires pour d'éventuelles infrastructures essentielles, si vous ne faites pas de suivi?

Mme Caroline Xavier: À dire vrai, nous faisons le suivi avec ces entités. Nous continuons de les appeler et de travailler avec elles. Je ne veux pas donner à qui que ce soit l'impression que ces relations n'existent pas. Au contraire, nous avons des relations exceptionnelles avec les infrastructures essentielles, surtout le secteur de l'énergie, des télécommunications et des banques. Nous tenons régulièrement des rencontres avec ces secteurs pour discuter des menaces et pour échanger de l'information à propos des menaces qui les concernent actuellement. Ce sont d'excellentes relations, et il existe des organismes de gouvernance pour que nous puissions nous comprendre et collaborer.

Cela dit, même si nous continuons de les soutenir et d'offrir notre soutien, nous ne pouvons pas les obliger. C'est à ce chapitre, comme je l'ai dit dans ma déclaration, que le projet de loi C-26 revêt une très grande importance quant aux quatre secteurs d'infrastructures essentielles qui sont visés dans le cadre du projet de loi, parce qu'elles remplissent un rôle très important pour les Canadiens, dans l'espace des infrastructures essentielles.

Le président: Merci beaucoup, madame Mathyssen.

Monsieur Genuis, vous avez la parole pour cinq minutes.

M. Garnett Genuis: Merci, monsieur le président.

Je pose la question aux témoins: imposez-vous des conditions aux informations que vous transmettez à la Chambre des communes?

M. Rajiv Gupta: Habituellement, il y a un avertissement dans nos rapports indiquant qu'il est interdit de partager l'information sans l'autorisation explicite du CSTC. Ce serait probablement la condition. Il faudrait que je vérifie les rapports.

M. Garnett Genuis: D'accord.

Si les rapports contiennent un avertissement indiquant que l'information ne peut pas être partagée avec d'autres sans la permission du CSTC, alors comment diable aurait-on pu transmettre ces informations aux parlementaires sans la permission du CSTC?

M. Rajiv Gupta: Toute l'information leur appartient. Ce sont leurs informations, et elles leur appartiennent, sous le régime de la loi qui s'applique; par exemple, pour le reste des ministères, ce serait la Loi sur la gestion des finances publiques.

● (1200)

M. Garnett Genuis: Oui, et c'est pour ça que j'ai demandé s'il y avait des conditions.

M. Rajiv Gupta: Cela figurerait dans nos rapports, dans notre rapport explicite. Comme je l'ai dit, nous n'avions même pas les courriels, alors nous aurions transmis la clé pour y accéder. L'organisation les aurait trouvés, puis aurait eu le champ libre pour communiquer l'information.

M. Garnett Genuis: Si vous avez transmis... Je pense que ce serait important que vous nous disiez exactement quelles sont ces conditions, parce que...

M. Rajiv Gupta: Les conditions interdisent au propriétaire du système de transmettre quoi que ce soit à ses employés.

M. Garnett Genuis: Mais nous parlons tout de même d'informations que vous lui avez transmises. Le gouvernement a dit qu'il avait de l'information concernant les députés concernés par la menace, y compris l'origine de ces menaces. Vous venez de reconnaître que, dans le processus pour transmettre l'information à la Chambre des communes, vous avez probablement inclus une attente selon laquelle l'information ne serait pas transmise à d'autres sans votre consentement.

M. Rajiv Gupta: Je n'accepte pas la prémisse de ce que vous dites.

M. Garnett Genuis: J'ai simplement dit ce que vous avez dit.

Mme Caroline Xavier: Juste pour que ce soit clair, ce que mon collègue disait, c'était que...

M. Garnett Genuis: Je ne sais pas. J'aimerais entendre ce que lui-même a à dire, pour être honnête.

Que disiez-vous, monsieur? Y avait-il des conditions intégrées, ou y avait-il probablement des conditions intégrées, comme vous l'avez dit il y a une minute, selon lesquelles l'information ne serait pas transmise sans l'accord du CSTC?

M. Rajiv Gupta: Si on avait voulu transmettre de l'information précise dans le rapport, c'était toujours possible de communiquer avec nous. À l'extérieur de ce qui vient dans le rapport, ils ont accès à tous leurs systèmes de TI et à toute l'information qu'ils peuvent transmettre eux-mêmes.

M. Garnett Genuis: D'accord, dans ce cas, vous a-t-on demandé la permission de transmettre de l'information, peu importe laquelle?

M. Rajiv Gupta: Non, mais le cas échéant... c'est quelque chose que nous avons souvent fait. Nous l'avons fait souvent dans le passé, avec la Chambre des communes...

M. Garnett Genuis: Voici où le bât blesse, toutefois.

[*Français*]

Mme Marie-Hélène Gaudreau: Monsieur le président, j'invoque le Règlement: comment les interprètes peuvent-ils faire leur travail quand il y a deux conversations en même temps?

Le président: Merci, madame Gaudreau.

[*Traduction*]

Monsieur Genuis, pouvez-vous faire de votre mieux? Je vous serai reconnaissant de diriger vos questions à qui vous voulez les poser.

Je ne veux pas enlever du temps à qui que ce soit. Si des gens parlent en même temps et que cela brouille une réponse, je ne veux pas blâmer qui que ce soit, mais je pense que nous devons faire un effort pour discuter de manière fluide, afin que les interprètes puissent faire leur travail.

J'ai arrêté le temps. Il vous reste deux minutes et 20 secondes. J'espère que tous ceux qui prendront la parole donneront le temps à la personne qui pose la question ou qui y répond de dire ce qu'ils ont à dire correctement.

Merci.

M. Garnett Genuis: Voici pourquoi cette situation est bizarre. Je suis ici, en compagnie de mes collègues, M. Calkins et M. Duncan, et j'ai de l'information qui serait très importante pour la vie de M. Duncan, de l'information que je devrais probablement lui transmettre, mais je dis que je vais d'abord en parler avec M. Calkins, et je vais dire à M. Calkins de ne pas en parler à personne, y compris à M. Duncan, sans me demander la permission d'abord. Puis, deux ans plus tard, je reviens et je dis que ce n'est pas ma faute si je n'ai rien dit à M. Calkins, parce que je pensais que M. Duncan allait lui dire. La chose la plus simple aurait été pour moi de simplement informer la personne concernée, au lieu de jouer au jeu du téléphone en boucle, potentiellement en imposant des conditions qui limitent de toute façon la transmission d'informations, et potentiellement sans que toute l'information soit transmise.

Fondamentalement, la question est: pourquoi toutes ces histoires entre ceux qui détenaient l'information, c'est-à-dire le gouvernement du Canada, et les personnes qui avaient besoin de l'information, les députés qui étaient menacés et qui auraient pu prendre des mesures préventives pour se protéger? Pourquoi était-ce si difficile pour le gouvernement de simplement nous informer directement?

Mme Caroline Xavier: Comme je l'ai dit, nous prenons notre rôle très au sérieux, et nous accordons énormément d'importance à la vie privée des Canadiens. Nous accordons énormément de sérieux au rôle que nous jouons auprès des fournisseurs de services, comme la Chambre des communes. Nous sommes conscients que tout le monde a un rôle à jouer dans le processus.

Cela dit, je reconnais que nous allons tirer des leçons de cet incident et, je l'espère, une meilleure compréhension de ce que nous aurions pu faire différemment, en particulier à la lumière de l'étude que vous réaliserez.

M. Garnett Genuis: Avez-vous clairement informé la Chambre des communes que l'APT31 était l'origine de la menace? Quand le lui avez-vous dit?

Mme Caroline Xavier: Comme le montre la chronologie, nous avions détecté certaines activités depuis janvier 2021. Comme l'a expliqué mon collègue, M. Gupta, nous avons progressivement commencé à mieux comprendre la menace...

M. Garnett Genuis: Je vous ai posé une question précise, qui n'apparaît pas dans la chronologie.

Avez-vous dit à la Chambre des communes que l'APT31 était l'origine de la menace, et, le cas échéant, quand?

Mme Caroline Xavier: Je pense que nous avons répondu à cette question: nous avons effectivement dit à la Chambre des communes, dans les diverses communications que nous avons eues avec elle, que nous croyions, à ce moment-là, que la menace venait de l'APT31.

Cela étant dit, M. le député m'a demandé exactement quand cela a été fait, et je ne saurais vous dire exactement à quelle date cela est arrivé...

● (1205)

M. Garnett Genuis: Pourriez-vous nous dire le mois?

Le président: Merci beaucoup.

M. Garnett Genuis: L'année?

Le président: Excusez-moi, monsieur Genuis, mais vous avez déjà dépassé votre temps.

Monsieur Collins, vous avez la parole pour cinq minutes.

M. Chad Collins: Merci, monsieur le président.

Madame Xavier, selon le portrait que vous avez brossé aujourd'hui, je pense que vous fournissez un service à vos clients, qu'il s'agisse de clients du gouvernement ou d'ailleurs. Quand vous obtenez de l'information, vous la transmettez aux organisations ou aux ministères.

Je pourrais probablement poser comme question, disons, que c'est le genre de chose qui pourrait arriver au ministère de la Défense. Prenons par exemple notre soutien envers l'Ukraine et tous les efforts menés par la Russie contre les personnes assises autour de la table qui soutiennent encore l'Ukraine… la Russie a tenté un grand nombre d'approches pour essayer de miner notre soutien à l'égard de ce dossier.

Si cela était arrivé au ministère de la Défense, auriez-vous transmis l'information à votre client, la Défense nationale? Auriez-vous considéré qu'il s'agit de votre client, dans ce cas? Vous lui auriez fourni l'information, puis il reviendrait à la Défense nationale de décider, à l'interne, avec son propre personnel de sécurité et sa propre équipe des TI, de la marche à suivre.

Est-ce une comparaison équitable de dire que, si la même situation s'était produite dans une autre organisation, vous auriez adopté la même approche?

Mme Caroline Xavier: C'est exact. C'est exactement ainsi que nous fonctionnons.

M. Chad Collins: Vous avez dit plus tôt... vous avez dit que vous étiez « respectueux de l'indépendance ». Je pense que vous faisiez référence au personnel de la Chambre des communes. Quel niveau d'indépendance les membres du personnel ont-ils dans ce genre de cas, pour régler le problème?

La Chambre des communes a sa propre équipe de sécurité des TI. Ses représentants étaient ici, lors de notre dernière réunion, comme vous le savez, et ils ont témoigné devant nous. Ils sont responsables de ce domaine dans leur organisation. Ce n'est peut-être pas le bon terme, mais je pense que vous comprenez ce que j'essaie de dire: ils ont leurs propres rôles et responsabilités dans le travail qu'ils effectuent avec les parlementaires, dans ce genre de cas.

Pouvez-vous nous dire quel niveau d'indépendance ont les divers secteurs du gouvernement ou les intervenants externes? Où tracez-vous la limite, entre le service que vous fournissez et le fait que vous donnez de l'information à un client?

Mme Caroline Xavier: Nous fonctionnons beaucoup comme fournisseur de services, comme vous l'avez mentionné. Quand nous sommes mis au courant d'un incident ou lorsque nous détectons quelque chose en utilisant nos outils, notre intention, notre but, est de transmettre l'information autant que possible aux bonnes personnes, afin qu'elles puissent agir et atténuer la menace avant tout. Quand cela concerne un système comme le gouvernement du Canada, les sous-ministres, par exemple, sont les personnes responsables dans chacun des ministères, et, rendent ensuite des comptes à leur ministre.

Quand nous transmettons de l'information au service des TI dans une organisation gouvernementale, ce sont les gens de ce service qui vont prendre les mesures nécessaires, avec notre appui également. Ce serait, par exemple, Services partagés Canada. Tout dépend du ministère.

Cela vaut aussi pour une industrie: nous communiquons avec les organisations des TI pour leur dire que nous avons détecté quelque chose, et elles vont agir au nom de leur organisme. Souvent, il y aura des échanges, dont nous avons déjà parlé, pour qu'elles puissent recueillir plus d'informations et intervenir en conséquence.

C'est le genre de choses que nous faisons très régulièrement, parce que cela fait partie d'une initiative de préavis en matière de rançongiciel, que nous avons mis en place avec nos partenaires américains, par exemple. Plus de 500 organisations ont communiqué avec nous, à ce qu'on appelle le « niveau du responsable principal de la sécurité de l'information », afin de déjouer une attaque avant même qu'elle n'arrive, sauvant ainsi des millions de dollars.

M. Chad Collins: Mais ce cas-ci est un peu inhabituel, n'est-ce pas? Cela soulève les passions, comme vous avez pu le voir avec certaines des questions ici ce matin. Nous ne sommes pas un client habituel, je dirais. J'aimerais reparler du protocole d'entente et plus précisément de tous les aspects que l'organisation a pu examiner, avec le recul, pour voir ce qui aurait pu être mieux fait et ce qui peut être amélioré à partir de maintenant.

Le protocole d'entente vise-t-il les communications? On vous a posé des questions aujourd'hui à propos de qui aurait dû être averti et quand. Qu'est-ce qui aurait dû être fait, selon le nouveau protocole d'entente, dans la mesure où cela concerne votre travail avec le personnel de la Chambre des communes?

Mme Caroline Xavier: Je ne veux pas induire le Comité en erreur, alors je vais devoir aller vérifier, pour reconfirmer le contenu du protocole d'entente. Je ne peux pas dire que je l'ai lu avant d'arriver au Comité ce matin...

M. Chad Collins: Je pense que la question serait, désormais, qui va communiquer avec les parlementaires, si cela arrive demain?

Mme Caroline Xavier: Encore une fois, nous comptons tirer des leçons de cet incident et travailler en collaboration avec la Chambre des communes pour déterminer la meilleure marche à suivre, afin que cet incident ne se reproduise plus.

● (1210)

M. Chad Collins: Je vais céder mon temps, monsieur le président. Je le donne au suivant.

Le président: Excellent. Merci beaucoup, monsieur Collins.

Chers collègues, l'heure touche à sa fin.

Avez-vous un rappel au Règlement, monsieur Duncan?

M. Eric Duncan (Stormont—Dundas—South Glengarry, PCC): Merci, monsieur le président.

Il s'agit seulement d'une remarque, pour les réunions futures. Je sais que nous avons déjà une réunion prévue ce mardi, et que la liste des témoins a été rendue publique. À l'avenir, pourrions-nous prendre l'habitude de demander aux témoins de nous fournir leur déclaration préliminaire à l'avance, et ce, dans les deux langues officielles? Les témoins avaient beaucoup de choses à dire dans leur déclaration, et nous pouvons difficilement suivre. J'essayais de prendre des notes. Tant de choses ont été dites.

Pourrions-nous imposer une norme, à l'avenir, puisque nous savons qu'il y aura une étude? Nous savons qui sont les témoins, alors pouvons-nous nous attendre à ce qu'ils nous donnent leur déclaration au moins un jour à l'avance, s'il vous plaît?

Le président: Vous soulevez un point tout à fait juste, monsieur Duncan. Je pense que nous allons suspendre la séance. Nous n'avons pas à régler la question immédiatement. J'en prends note. Nous allons suspendre la séance. Nous pourrons discuter de la façon dont le processus pourrait être plus efficace pour les députés, les témoins et les interprètes.

Chers collègues, nous allons prendre une courte pause, puis nous commencerons la deuxième moitié de la réunion. Merci.

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