CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

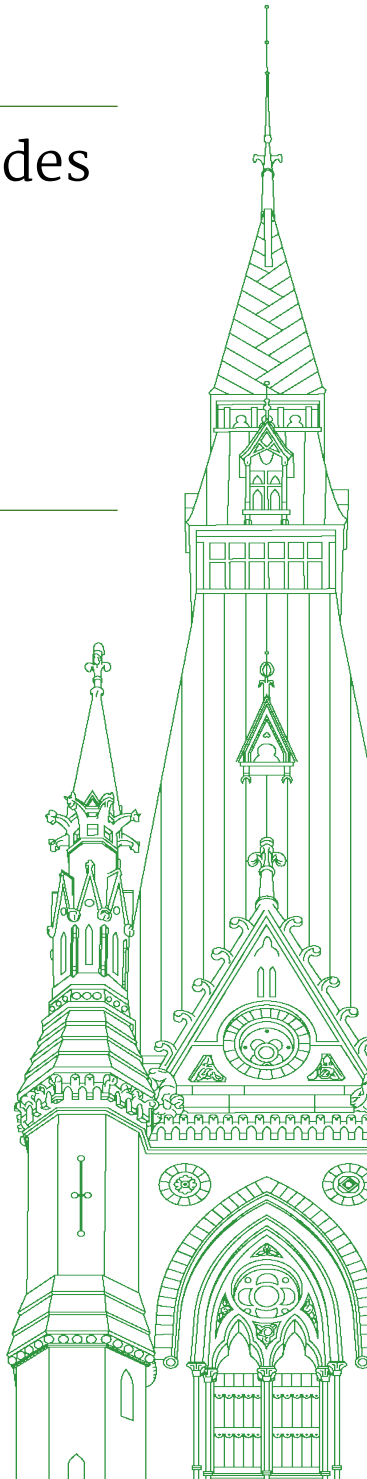
Comité permanent de la procédure et des affaires de la Chambre

TÉMOIGNAGES

NUMÉRO 118

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le mardi 4 juin 2024



Président : M. Ben Carr

Comité permanent de la procédure et des affaires de la Chambre

Le mardi 4 juin 2024

● (1100)

[*Traduction*]

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

[*Français*]

J'espère que tout le monde a passé une belle fin de semaine dans sa circonscription.

Collègues, je vous souhaite la bienvenue à la 118e réunion du Comité permanent de la procédure et des affaires de la Chambre.

Aujourd'hui, le Comité se réunit pour discuter de la question de privilège concernant des cyberattaques menées contre des députés.

[*Traduction*]

Chers collègues, nous sommes tous au courant des nouvelles règles sur les dispositifs audio. Veuillez les placer sur les autocollants fournis devant vous sur la table, à votre gauche ou à votre droite, lorsqu'ils ne sont pas utilisés.

Je remarque que nous accueillons un certain nombre de membres non permanents. Je souhaite la bienvenue aux remplaçants qui sont là.

Chers collègues, nous avons eu quelques séances très productives. Nous avons traité de questions délicates et difficiles, ce qui n'a pas empêché d'avoir des échanges respectueux. Nous avons pu maintenir un bon dialogue entre ceux qui posent des questions et les témoins. J'espère que nous pourrons continuer dans cet esprit.

[*Français*]

Ce matin, nous recevons plusieurs témoins.

[*Traduction*]

Les témoins ne nous sont pas étrangers. Ils ont comparu il n'y a pas si longtemps.

Je souhaite la bienvenue à Eric Janse, greffier de la Chambre des communes, à Stéphan Aubé, administrateur en chef, à Michel Bédard, légiste et conseiller parlementaire, à Patrick McDonell, sergent d'armes et dirigeant de la sécurité institutionnelle, à Jeffrey LeBlanc, sous-greffier à la procédure; et à Benoit Dicaire, dirigeant principal de l'information par intérim, Services numériques et biens immobiliers.

Monsieur Janse, vous et vos collègues avez 10 minutes pour commencer la séance. Après vos interventions, nous passerons à la première série de questions.

[*Français*]

Monsieur Janse, vous avez la parole.

[*Traduction*]

M. Eric Janse (greffier de la Chambre des communes): Merci beaucoup, monsieur le président. C'est un plaisir de comparaître de nouveau devant le Comité, cette fois-ci pour aborder un sujet différent de celui de la semaine dernière et avec des témoins un peu différents.

Nous comparaissons pour discuter de la présomption d'atteinte au privilège découlant des cyberattaques menées contre des députés par une entité étrangère appelée Advanced Persistent Threat 31, qui aurait le soutien de la République populaire de Chine. Nous espérons que notre témoignage aidera le Comité dans l'étude de cette importante question.

Dans sa décision du 8 mai 2024, le Président a séparé la question de privilège en deux parties distinctes. La première concernait le fait que les députés n'ont pas été informés de la cyberattaque, tandis que la deuxième concernait la cyberattaque elle-même.

Dans sa décision, le Président a noté que, depuis l'attaque, les processus et les protocoles concernant le besoin d'aviser les députés avaient évolué. Le Président a notamment fait référence à la directive de mai 2023 de l'ancien ministre de la Sécurité publique concernant les menaces à la sécurité du Canada visant le Parlement et les parlementaires. Il a aussi mentionné une recommandation faite par le Comité dans son 63e rapport, selon laquelle les députés devraient être avisés par le SCRS des menaces d'ingérence étrangère qui les visent.

Dans la deuxième partie de sa décision, qui concerne la cyberattaque elle-même, le Président a estimé qu'il s'agissait d'une tentative d'ingérence dans le travail des parlementaires et a jugé que la question de privilège se posait de prime abord.

● (1105)

[*Français*]

Pour en arriver à cette conclusion, le Président s'est référé à la question de privilège fondée de prime abord qui a été soulevée par le député de Wellington-Halton Hills. Celui-ci avait fait l'objet d'une décision du prédécesseur du Président le 8 mai 2023. Dans cette affaire, le député faisait l'objet de menaces de représailles de la part d'acteurs étrangers pour des positions qu'il avait prises lors de débats.

Dans sa décision, le Président a déclaré que la question soulevée par le député touchait directement aux privilèges et aux immunités qui sous-tendent la capacité collective d'exercer les fonctions parlementaires sans entrave.

Au terme de son étude sur cette question de privilège fondée de prime abord, le Comité a présenté son 63e rapport à la Chambre le 10 avril 2024. Bien que le rapport n'ait pas encore été adopté, il contient de nombreuses recommandations. Dans le cadre de son examen de cette nouvelle question de privilège, le Comité pourra s'appuyer sur les conclusions de ce rapport et formuler d'autres recommandations à la Chambre.

[*Traduction*]

Trois des recommandations du 63e rapport s'adressent à l'Administration de la Chambre.

La première propose d'élaborer une formation sur l'ingérence étrangère et de l'offrir dans le cadre du Programme d'orientation des députés et sur une base continue. Cette formation était en cours de préparation depuis un certain temps et j'ai le plaisir de dire qu'elle est maintenant offerte aux caucus et qu'elle fera partie du prochain programme d'orientation.

Dans sa deuxième recommandation, le Comité demande que l'Administration de la Chambre désigne une personne-ressource responsable d'assurer la liaison avec les députés sur toute question liée aux menaces d'ingérence étrangère. La troisième recommandation, qui va dans le même sens, vise l'élaboration d'un protocole pour informer les whips des menaces d'ingérence étrangère.

Je remarque que des ententes avec nos partenaires en matière de sécurité relatives à ces recommandations sont déjà en place. Nous serons heureux de vous fournir de plus amples renseignements à ce sujet au cours de la séance.

[*Français*]

Cette nouvelle question de privilège donne au Comité l'occasion d'examiner certains éléments supplémentaires qui ont été mis en lumière concernant les cyberattaques visant les députés individuellement, et le Parlement dans son ensemble.

Les cyberattaques ont plusieurs objectifs, l'un des plus évidents étant de perturber nos systèmes techniques et donc de réduire la capacité des députés de faire leur travail. Il peut s'agir de tentatives de vol d'information confidentielle, ce qui a une incidence sur la capacité des députés de travailler sur des fichiers sensibles. Ces attaques peuvent également être perçues comme des tentatives d'intimidation des députés et donc comme une ingérence dans les activités de la Chambre. Lorsque des députés font l'objet de diverses formes d'obstruction, c'est la Chambre dans son ensemble qui peut être entravée dans son travail.

Comme l'a indiqué le Président dans sa décision, ces types d'attaques sont de plus en plus fréquents. La question soulevée par le député de Sherwood Park—Fort Saskatchewan concernait les cyberattaques perpétrées par une entité étrangère au moyen de courriels, mais d'autres technologies modernes peuvent être utilisées pour perturber les travaux parlementaires. Dans certains cas, les entités à l'origine des attaques peuvent être identifiées, et dans d'autres, non.

[*Traduction*]

Un autre élément à prendre en compte est la difficulté, pour la Chambre, de faire valoir ses droits lorsqu'une entité étrangère est à l'origine d'actions répréhensibles. De plus, la Chambre peut, dans une certaine mesure, atténuer l'impact et les risques lorsque des attaques ciblent ses propres systèmes ou d'autres systèmes qui, comme les services de courriel personnels, sont utilisés par les députés pour remplir leurs fonctions, mais sa capacité demeure néanmoins limitée. Les députés peuvent actuellement utiliser divers outils pour remplir leurs fonctions parlementaires. Certains de ces outils sont soutenus par les services de TI de la Chambre, et d'autres non.

[*Français*]

Lorsqu'il examine une question de privilège, le Comité se prévaut généralement des pouvoirs habituels, comme il le ferait pour n'importe quelle étude. S'agissant de privilège, il cherche à établir les faits. Il peut proposer des recours et d'autres mesures sous forme de recommandations dans un rapport présenté à la Chambre.

Je vais maintenant demander à mon collègue Benoit Dicaire, dirigeant principal de l'information par intérim, de fournir plus de renseignements sur la cybersécurité à la Chambre des communes.

M. Benoit Dicaire (dirigeant principal de l'information par intérim, Services numériques et biens immobiliers, Chambre des communes): Merci, monsieur le greffier.

Merci, monsieur le président.

Je suis ici aujourd'hui pour vous parler de la cybersécurité à la Chambre des communes, plus précisément pour vous donner le contexte de l'évolution de notre position en matière de cybersécurité et de l'engagement de l'Administration de la Chambre des communes à protéger l'institution et ses utilisateurs contre les cybermenaces.

Le paysage des cybermenaces évolue constamment, et il devient de plus en plus complexe et difficile. La prolifération des technologies dans cette nouvelle réalité numérique introduit une croissance importante des nouveaux vecteurs de menaces. De plus, la sophistication des auteurs de menaces pousse l'Administration de la Chambre des communes à faire constamment évoluer notre programme de cybersécurité et à l'adapter afin de réduire les risques émergents.

[*Traduction*]

L'équipe de sécurité de la TI de l'Administration de la Chambre a pour mandat de renforcer la cyberrésilience du Parlement face à un environnement de menaces numériques en constante évolution. Cette équipe s'emploie tout spécialement à protéger la disponibilité des ressources de TI afin d'assurer la continuité des activités parlementaires et d'assurer la confidentialité et l'intégrité de l'infrastructure, des systèmes, des utilisateurs, y compris les députés, et de leurs données, que ce soit à Ottawa, dans les circonscriptions ou lorsqu'ils sont en déplacement ou travaillent à distance. Son mandat concerne uniquement les informations et les appareils parlementaires. Notre rôle ne s'étend pas au-delà des fonctions législatives des députés.

● (1110)

[*Français*]

La cyberrésilience du Parlement repose sur une approche intégrée fondée sur des mesures proactives comme la surveillance continue, le renseignement, la chasse aux menaces, la gestion de la vulnérabilité, l'élaboration de guides d'intervention en cas d'incident et la tenue d'exercices réguliers.

Il est tout aussi important de prendre des mesures réactives pour assurer notre capacité à détecter efficacement les incidents, les menaces et les atteintes à la sécurité, à intervenir rapidement lors de la détection, et à nous en remettre au fur et à mesure qu'ils se produisent.

[*Traduction*]

Cette approche s'inspire de normes et de pratiques exemplaires internationalement reconnues, telles que la série ISO 27000, le cadre de cybersécurité du NIST et les directives ITSG 22 et 33. Elle garantit que les contrôles et les processus de sécurité sont en place pour atténuer les cyberrisques et intervenir correctement en cas de cyberincidents.

En outre, cette approche intégrée s'appuie sur divers partenariats essentiels pour collaborer efficacement, communiquer des informations et renforcer notre position de cybersécurité. Je donnerai plus d'informations sur ces partenariats dans la partie de la réunion qui se déroulera à huis clos.

Voilà qui conclut la partie publique de notre présentation. Nous serons heureux de répondre à vos questions ou à vos préoccupations.

Merci.

Le président: Merci beaucoup, monsieur Janse et monsieur Dicaire.

Chers collègues, j'ai un bref rappel à faire. À la dernière séance, j'ai rapidement avancé l'idée qu'il serait utile à la présidence que les députés, lorsqu'ils posent des questions, aient devant eux un chronomètre ou qu'un collègue tout près en ait un. Ce n'est certes pas une exigence, mais cela m'éviterait d'interrompre le député qui a la parole et de le déconcentrer. Ce peut être une distraction, mais ce serait utile au bon déroulement de la séance.

Monsieur Genuis, vous avez les six premières minutes. Je vous cède la parole.

M. Garnett Genuis (Sherwood Park—Fort Saskatchewan, PCC): Merci, monsieur le président.

Nous sommes là pour discuter du fait que 18 parlementaires ont été ciblés par APT31, une entreprise de piratage affiliée à l'État chinois. J'étais l'un d'eux. L'attaque visait les parlementaires de l'Alliance interparlementaire sur la Chine, qui est, je dois le souligner, un vaste et important réseau qui réunit des législateurs de divers pays et continents et de différentes traditions politiques pour travailler à des questions liées au Parti communiste chinois.

J'aurais dû être informé de cette attaque, mais je ne l'ai pas été. Mes questions porteront sur l'avertissement à donner aux députés. Les déclarations publiques du gouvernement laissent entendre qu'il était au courant de cette attaque. Il a choisi de ne pas informer les députés, mais il a communiqué certains renseignements à l'Administration de la Chambre.

Pouvez-vous confirmer que le gouvernement a communiqué de l'information concernant cette attaque à l'Administration de la Chambre et préciser quand il l'a fait?

M. Eric Janse: Merci de la question, monsieur Genuis.

En effet, il y a eu des échanges entre les partenaires de la sécurité et l'Administration de la Chambre à ce moment-là. Nous pourrons peut-être vous donner plus de détails pendant la partie à huis clos de la séance, monsieur Genuis.

Ce qui a été souligné dans le rapport — et nous pouvons certes le confirmer de notre côté, et nos partenaires de la sécurité peuvent le faire aussi —, c'est que, si une situation semblable se produisait aujourd'hui, les choses se passeraient différemment.

M. Garnett Genuis: Le gouvernement aurait pu informer directement les députés. À mon avis, il n'y a aucune raison pour qu'il ne l'ait pas fait. Prétendre qu'il a informé quelqu'un d'autre ressemble à une excuse.

Lorsque l'Administration de la Chambre a été mise au courant, a-t-on discuté de la possibilité d'informer les députés? Le gouvernement a-t-il dit qu'il s'attendait à ce que les députés soient informés ou, au contraire, à ce qu'ils ne le soient pas? Est-ce une question qui a été abordée au cours des échanges?

M. Eric Janse: Cela ne me plaît pas, monsieur Genuis, mais je propose que nous abordions cette question à huis clos.

M. Garnett Genuis: Le gouvernement a-t-il cherché ou non à transmettre cette information aux députés? Je n'insisterai pas davantage sur le fait que c'est pour lui une question de responsabilité politique. S'il vous avait demandé de ne pas communiquer l'information aux députés, cela aurait sa place dans le débat public sur la question. S'il a fait d'autres observations... Vous savez ce que vous savez, et je ne suis pas au courant. Je ne vais donc pas insister au point de vous rendre mal à l'aise. Je n'en pense pas moins que, quelles que soient les indications que le gouvernement a données sur la communication ou non de l'information aux députés, il s'agit d'une authentique question d'intérêt public.

● (1115)

M. Eric Janse: Vous avez raison. Pour vous donner une réponse vraiment complète, je préfère attendre la séance à huis clos.

M. Garnett Genuis: Nous reviendrons peut-être sur la question, et le Comité pourra alors décider quels renseignements devraient être communiqués au public.

Une chose m'a vraiment dérangé. La plupart des députés ont été attaqués sur leurs comptes parlementaires. Ce n'est pas mon cas. L'attaque a visé mon compte personnel. C'était lié à mon travail parlementaire, bien sûr, mais mon compte de courriel personnel, qui n'est pas public, a quand même été ciblé.

Au départ, le bureau du Président de la Chambre a réagi dans les médias en disant que l'incident n'était pas trop inquiétant parce que l'attaque avait été repoussée. Je crois comprendre, mais vous pourriez peut-être me donner des précisions, que les services de sécurité de la Chambre des communes ne s'occupent d'aucune façon de la surveillance ou de la protection des comptes personnels non parlementaires des députés. Le bureau du Président et l'Administration de la Chambre des communes ne seraient d'aucune façon en mesure de dire si l'attaque contre un compte personnel a réussi.

Qu'en pensez-vous?

M. Eric Janse: Je peux confirmer que l'Administration de la Chambre ne surveille aucunement les courriels personnels.

Le président: Il vous reste environ 90 secondes, monsieur Genuis.

M. Garnett Genuis: D'accord.

À propos des protocoles en place à ce moment-là et maintenant, il y a eu de nombreux cas de menaces et les députés n'ont pas été informés. Ces protocoles ont changé, si je comprends bien, de sorte que, si le même genre d'incident se produisait aujourd'hui, les députés en seraient informés immédiatement. Pouvez-vous le confirmer? La directive signifie-t-elle que les députés seront informés des menaces qui ont été lancées contre eux avant que la nouvelle directive ne soit publiée, menaces qui pourraient toujours présenter un intérêt pour eux aujourd'hui?

M. Eric Janse: Je vais vous donner une réponse générale, mais je peux entrer un peu plus dans les détails pendant la partie de la séance qui se déroulera à huis clos.

En effet, il y aurait une communication plus rapide avec les députés que par le passé, mais il y a quand même une question de seuil. Comme mes notes et la décision du Président y ont fait allusion, il y a malheureusement beaucoup d'attaques contre la Chambre. Nous ne voudrions pas que le SCRS ait un bureau satellite à la Chambre, parce qu'il faudrait constamment donner des informations aux députés.

Si ce genre de chose surgissait aujourd'hui, par opposition à il y a deux ou trois ans, ce serait géré différemment.

M. Garnett Genuis: Il me reste 15 secondes.

C'est encore assez flou. Il est vrai qu'il y a beaucoup de menaces, mais si un député, parce qu'il travaille à une question de politique étrangère, est ciblé expressément par un gouvernement étranger — au lieu de faire l'objet d'une menace générale —, il me semble raisonnable que ce député ait le droit de savoir, surtout s'il peut prendre des dispositions pour protéger à la fois son compte parlementaire et son compte personnel.

Vous dites qu'il n'est toujours pas sûr que les députés seraient informés.

M. Eric Janse: Je déteste faire cette réponse, mais nous pourrons en discuter pendant la partie à huis clos. Je pourrai vous donner une réponse plus complète.

M. Garnett Genuis: À mon avis, c'est une question d'intérêt public...

Le président: Monsieur Genuis, j'ai usé de latitude avec vous.

Chers collègues, si vous constatez que vous en êtes à vos 20 ou 30 dernières secondes au début d'une série de questions, n'hésitez pas à céder le reste de votre temps à la présidence. Je vais simplement l'ajouter à votre temps de parole pour permettre une utilisation plus efficace des questions. Je ne veux certainement pas éliminer toute forme de productivité.

Monsieur Genuis, merci beaucoup.

Madame Romanado, vous avez la parole pendant six minutes.

Mme Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Merci beaucoup, monsieur le président.

Je remercie les témoins de comparaître de nouveau devant le Comité.

J'ai des questions auxquelles vous ne pourrez sans doute répondre qu'à huis clos. J'attendrai donc la séance à huis clos pour les poser. Une fois que nous aurons fait un tour complet, si le Comité le veut bien, nous pourrions commencer la séance à huis clos un peu plus tôt, au lieu de poser des questions auxquelles on ne peut malheureusement pas répondre en public.

Le Centre de la sécurité des télécommunications, le CST, a fourni au comité de la procédure et des affaires de la Chambre une chronologie des faits qui décrit la situation en précisant les dates.

Monsieur Dicaire, nous croyons comprendre qu'une surveillance s'exerce sur les comptes de courriel parlementaires, évidemment, mais quel est le protocole en ce moment dans le cas où la Chambre des communes reçoit un appel du SCRS ou du CST disant qu'ils ont des raisons de croire que le compte personnel d'un parlementaire a été ciblé? Expliquez-nous ce qui se passerait, car il semble y avoir des renseignements dans cette chronologie qui montrent, malgré les multiples points de contact avec l'Administration de la Chambre des communes, que des choses n'ont pas été faites, ou qu'il a fallu quelques jours avant que des mesures ne soient prises. Si vous pouviez nous expliquer tout cela, ce serait utile.

● (1120)

M. Benoit Dicaire: Merci de la question, madame Romanado.

Cela n'arrive pas souvent avec des partenaires sur le front cybernétique parce qu'ils comprennent notre mandat lorsqu'il s'agit de menaces précises concernant l'identité personnelle des députés. Ce n'est pas souvent le cas, car nos interactions avec les partenaires se rattachent habituellement à notre mandat. Comme vous le savez, certains de ces organismes ont des mandats précis, et ils n'interagissent avec nous que lorsque cela intéresse expressément le Parlement.

Nous recevons des renseignements de divers partenaires. Lorsque nous discuterons à huis clos, je pourrai en dire un peu plus. Toute information transmise à l'équipe de cybersécurité du Parlement est triée et gérée. Nous examinons le niveau de risque lié à telle menace en particulier. S'il s'agit d'une menace physique, nous communiquons avec mon collègue, le sergent d'armes. S'il s'agit d'ingérence étrangère ou de ce genre de scénario, nous nous adressons précisément au sergent d'armes.

La plupart de nos relations, de mon point de vue, se situent sur le plan de la technologie. Quand il s'agit d'éléments technologiques, il est très rare qu'une interaction concerne une personne en particulier. Il s'agit surtout de l'infrastructure. C'est le genre de scénario qui se présente à nous.

En général, c'est probablement la meilleure réponse que je puisse donner en public. Stéphan Aubé pourra peut-être ajouter quelque chose.

M. Stéphan Aubé (administrateur en chef, Chambre des communes): En 2014, le Bureau de régie interne a modifié la politique d'utilisation acceptable pour décrire clairement la marche à suivre si les renseignements personnels d'un député sont ciblés. Dans le cas du groupe chargé de la cybersécurité, dans tous les cas où les renseignements d'un député sont compromis, la première discussion a lieu avec le bureau du député et directement avec le député. C'est la marche à suivre qui est documentée et qui a été approuvée par le Bureau de régie interne au sujet des menaces précises qui visent des députés.

Si jamais nous avons besoin d'accéder au contenu — le contenu ne serait pas communiqué à l'Administration de la Chambre parce que l'autorisation du député est indispensable —, nous pourrons ensuite transmettre la question aux agents supérieurs de la Chambre. Si nous estimons que l'infrastructure de la Chambre est menacée et que nous devons protéger l'institution, nous en discuterons.

Le document que nous suivons pour les incidents concernant les membres est la politique d'utilisation acceptable de 2014.

Mme Sherry Romanado: Monsieur Aubé, il y avait une politique d'utilisation acceptable dès 2014, mais les faits se sont produits en 2021. S'il y avait déjà une politique en place qui énonçait clairement le protocole à suivre en cas de cyberattaque non liée à l'utilisation des TI des Communes, comme dans le cas de M. Genuis, pourquoi n'a-t-on pas communiqué avec lui? Vous venez de dire que vous avez besoin de l'approbation d'un député pour avoir accès à ses renseignements. Comment se fait-il qu'il n'ait pas été mis au courant?

M. Stéphan Aubé: Notre mandat, du point de vue de la sécurité des TI, est axé sur le Parlement et le rôle législatif du député. Nous ne nous occupons pas actuellement de la protection des renseignements personnels des députés. Dans un cas de cette nature, si je n'ai pas accès à l'information, je ne peux pas appliquer le protocole. Les députés dont l'infrastructure à la Chambre a été touchée auraient été avisés.

● (1125)

Mme Sherry Romanado: Vous venez de dire que vous ne vous occupez pas actuellement des systèmes de TI à l'extérieur de la Chambre des communes. Est-ce exact?

M. Stéphan Aubé: Je veux dire à l'extérieur du mandat de la Chambre des communes.

Mme Sherry Romanado: Merci.

Le président: Merci, madame Romanado.

[*Français*]

Madame Gaudreau, je vous cède la parole pour six minutes.

Mme Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Merci, monsieur le président.

Je vais faire une petite introduction, car il s'est passé beaucoup d'événements au cours des dernières heures. J'ai mis ça sur papier pour m'assurer d'être concise.

Au cours du dernier mois, nous avons appris que des députés étaient ciblés et que leur courriel personnel avait été la cible de stratagèmes d'États étrangers pour leur soutirer des renseignements de nature délicate. L'objectif était, nous pouvons l'imaginer, de faire du chantage ou d'utiliser ça de manière néfaste. Nous le savons.

Nous apprenions hier que le Comité des parlementaires sur la sécurité nationale et le renseignement tirait la sonnette d'alarme. Là, c'est clair: le gouvernement n'en fait pas assez. Il faut donc essayer de faire quelque chose. C'est très important.

J'ai l'impression — et nous le constatons — que le premier ministre ne prend pas ces questions suffisamment au sérieux. En fait, ce sont des députés qui en tirent profit, car, l'ingérence étrangère, il est même possible de la susciter. C'est pour moi un choc aujourd'hui d'apprendre cela.

Pendant ce temps, nous apprenons que de faux documents sont en train de circuler. Des documentaires qui sont diffusés probablement en russe, dont vous êtes sûrement bien au courant, circulent notamment sur Internet au sujet des Jeux olympiques qui auront bientôt lieu en Europe. Des médias européens sont copiés en ligne. On parle de fausses nouvelles et de faussetés, et c'est d'un réalisme incroyable. Il y a même une série qui entretient cette confusion chez les gens. Nous sommes à quelques jours des élections européennes, qui concernent plus de 700 millions de personnes. Imaginez l'impact que tout cela aura sur ces gens.

Après un an, j'essaie de comprendre comment il se fait que les membres du Comité permanent de la procédure et des affaires de la Chambre sont encore ici, aujourd'hui, pour s'attaquer à l'ingérence et se voir obligés de faire un grand pas de géant. Je n'ai pas l'impression que nous sommes bien équipés pour le faire. C'est ce que je constate quand je parle au public.

Je comprends maintenant que le privilège parlementaire englobe vraiment tout ce qui est lié à notre travail, que ce soit en circonscription, en comité ou ailleurs.

Nous parlons maintenant de collecte de renseignements personnels par le truchement d'une adresse courriel Gmail. Nous nous entendons pour dire que ça va loin. Des gens viennent voir nos factures, qui nous sommes. Ils peuvent tout savoir. C'est une source énorme pour ce qui est de la collecte de renseignements personnels. La capacité de chantage peut aussi être énorme.

En quoi est-ce différent de ce qui concerne le député de Wellington—Halton Hills?

M. Michel Bédard (légiste et conseiller parlementaire, Chambre des communes): Je vous remercie de la question.

Je vais couvrir l'aspect touchant le privilège parlementaire. Mes collègues pourront ensuite vous donner davantage de détails sur le mandat de l'Administration de la Chambre des communes quant à notre infrastructure de technologie de l'information.

En ce qui a trait au privilège parlementaire, la situation a été reconnue par le Président de la Chambre des communes dans cette décision. On parle d'actes d'ingérence ainsi que de menaces envers un député en raison de ses fonctions parlementaires. Le Président a statué que cela constituait une question de privilège fondée de prime abord, même si l'attaque visait le courriel personnel du député en question.

Comme vous l'avez énoncé, il y a potentiellement un risque de menaces ou de toutes sortes d'actes d'ingérence, même si on utilise les outils personnels du député. Toutefois, dans le cadre des fonctions parlementaires, pour ce qui relève de l'Administration de la Chambre des communes, le mandat et la capacité de celle-ci sont limités quant aux instruments qu'il est possible de déployer.

Monsieur Aubé, voulez-vous ajouter des commentaires?

M. Stéphan Aubé: Merci, monsieur Bédard.

Présentement, ce que nous pouvons faire, compte tenu de notre capacité à cet égard, c'est protéger l'institution et nous assurer que le Parlement continue de fonctionner.

C'est dans ce cadre que l'infrastructure de technologie a été mise en place et que nos partenariats ont été noués afin de bien protéger le Parlement et d'assurer son bon fonctionnement.

Nous le faisons à l'égard des fonctions exercées par les députés, tant lorsqu'ils se trouvent dans leur bureau de circonscription, lorsqu'ils voyagent ou lorsqu'ils sont sur la Colline du Parlement, que lorsqu'ils interagissent avec des concitoyens.

Par contre, lorsqu'il s'agit de la vie privée des gens et de relations internationales, nous ne sommes pas en mesure de répondre à ce type de situation. D'autres agences au sein du gouvernement sont mieux outillées pour le faire.

Notre mandat est de protéger le Parlement...

● (1130)

Mme Marie-Hélène Gaudreau: Je suis désolée de vous interrompre, car il me reste peu de temps de parole. Je suis tout à fait rassurée en ce qui a trait à mon rôle de parlementaire, je tiens à le dire. Je l'ai vécu.

Qui peut nous aider?

Vous dites qu'il y a d'autres possibilités, que d'autres agences peuvent vous aider à faire votre travail. Vous devez l'accomplir partout. On ne peut pas dire que votre travail ne concerne que mon rôle de parlementaire, lorsque je suis ici. Ça continue lorsque je suis à la maison.

Qui nous aide? Qui vous aide?

Le président: Il vous reste environ 20 secondes pour répondre à la question, monsieur Janse.

M. Eric Janse: D'accord.

Je dirais que c'est un travail d'équipe. Il y a l'Administration de la Chambre des communes, notre partenaire sur la Colline du Parlement, et il y a aussi nos partenaires dans le domaine de la sécurité, par exemple nos partenaires en matière de cybersécurité ou de services de police. C'est vraiment grâce aux partenariats établis avec tous ces groupes que nous pourrons faire face à tous ces défis.

Le président: Merci, madame Gaudreau.

[*Traduction*]

Madame Mathyssen, vous êtes en ligne avec nous aujourd'hui. Vous avez la parole. Six minutes. À vous.

Mme Lindsay Mathyssen (London—Fanshawe, NPD): Merci. Je suis heureuse de me joindre à vous virtuellement, même si c'est parfois difficile.

Je voudrais poursuivre dans la même foulée que Mme Gaudreau...

Je suis préoccupée, bien sûr. La députée a parlé des informations qui sont ressorties du rapport au sujet de l'influence exercée sur des députés et de la ligne de démarcation entre notre vie personnelle et notre vie et notre travail parlementaires. On pourrait sans doute prétendre que nous sommes des acteurs tout à fait politiques et partisans. Pour ma part, je cherche à éviter toute interaction entre mon travail parlementaire et mon travail partisan et politique. Les deux aspects sont cloisonnés. Bien sûr, je ne fais pas mon travail partisan, comme la collecte de fonds pour le NPD — peu importe les termes employés — en me servant de mon courriel parlementaire, et pourtant, il est fortement touché par l'ingérence étrangère. Nous le voyons dans les échanges qui viennent d'être publiés dans les médias au sujet de la course à la direction du Parti conservateur.

Pouvez-vous nous parler des attaques personnelles que nous recevons? Comment sommes-nous censés maintenir une distinction et nous efforcer de me pas être de mauvais protagonistes, alors que nous tentons d'assumer les deux aspects de notre travail?

M. Eric Janse: Je vais peut-être commencer. C'est une très bonne question, madame Mathyssen, et il est évident que le Comité voudra y réfléchir.

À propos des raisons qui expliquent notre présence ici-même et du cas de M. Genuis, normalement, les questions de privilège dans les délibérations parlementaires sont liées aux travaux de la Chambre ou d'un comité. Dans ce cas-ci, c'est le travail que M. Genuis a fait avec une organisation externe, mais qui — comment puis-je dire? — influence ou favorise son travail à la Chambre ou en comité. Par conséquent, c'est en partie pour cela que le Président de la Chambre a décidé qu'il y avait présomption d'atteinte au privilège et qu'une étude plus approfondie s'imposait.

Mes collègues veulent peut-être ajouter quelque chose.

Patrick McDonell, voulez-vous intervenir?

M. Patrick McDonell (sergent d'armes et dirigeant de la sécurité institutionnelle, Chambre des communes): Si je comprends bien la question, il se peut que vous receviez un courriel de harcèlement sur vos comptes personnels ou dans votre vie personnelle et que cela ne concerne pas le travail parlementaire. Est-ce exact, madame Mathyssen?

Mme Lindsay Mathyssen: Il s'agit davantage de la séparation que nous ménageons entre les deux aspects. Nous menons une action politique; nous sommes partisans, et ce travail doit se faire à l'extérieur de la Cité parlementaire et des contrôles que vous exercez. Comment pouvons-nous vous aider à maintenir cette séparation, mais aussi à protéger les deux aspects de notre vie?

M. Patrick McDonell: Mes services sont responsables des deux aspects. Sur le plan personnel, si vous avez des préoccupations en matière de sécurité, vous pouvez vous présenter à mon bureau et nous les analyserons et communiquerons avec l'organisme de sécurité compétent, qu'il s'agisse du SCRS, de la GRC ou du service de police local. Cependant, il n'y a pas, au bureau du sergent d'armes, de distinction entre ce qui est parlementaire et ce qui est personnel. Notre seule préoccupation est la sécurité des députés.

● (1135)

Mme Lindsay Mathyssen: Le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement, le CPSNR, qui vient d'être publié, parle de députés qui, sciemment ou pas tout à fait sciemment, ont fourni des renseignements à des gouvernements étrangers. Si nous ne savons pas ce qui se passe du côté personnel, comment sommes-nous censés être en mesure de communiquer avec le sergent d'armes, par exemple, au sujet de ces questions et de ces menaces? Si nous ne les percevons pas de cette façon, cela devient assez compliqué.

M. Patrick McDonell: Oui, et je crois que votre question porte sur le fait que la communication dans l'espace personnel est de nature ouverte et non pas secrète. Bien sûr, quand c'est secret, c'est beaucoup plus difficile à détecter.

Mme Lindsay Mathyssen: J'essaie d'en venir au rapport du CPSNR qui a été publié. Comment sommes-nous censés éviter de fournir des renseignements dans l'espace personnel également? Travaillez-vous avec des institutions comme le SCRS? Dans le même ordre d'idée, avez-vous vu des obstacles que le Comité pourrait gérer pour aider à régler les cas complexes que le rapport du CPSNR a révélés cette semaine?

M. Patrick McDonell: Nous aurons bientôt des séances d'orientation. Sécurité publique assure la coordination avec nous, et nous faisons appel au SCRS, au CST et à la GRC pour donner des séances d'information aux caucus.

De plus, nous avons intensifié nos efforts de sensibilisation à la sécurité. À la dernière réunion du Bureau de régie interne, on nous a accordé plus de ressources afin que nous puissions mieux informer les députés sur les menaces actuelles et les tenir au courant du contexte actuel des menaces.

Mme Lindsay Mathyssen: Cela dépend en grande partie de la personne. C'est aux députés de savoir.

Le président: Madame Mathyssen, je vais permettre à M. McDonell de répondre très rapidement, mais votre temps de parole est écoulé.

Mme Lindsay Mathyssen: Je suis désolée. J'ai oublié d'appuyer sur le bouton de mon chronomètre, monsieur le président.

Le président: Pas de problème.

Monsieur McDonell, voulez-vous répondre très rapidement?

M. Patrick McDonell: J'ai toujours pensé que la sécurité est une responsabilité partagée, et plus nous apprenons comment servir les députés, mieux nous pouvons assurer leur sécurité.

Le président: Merci beaucoup.

Nous en sommes maintenant à la deuxième série de questions. La durée des interventions est différente.

Monsieur Genuis, vous avez la parole. Cinq minutes.

M. Garnett Genuis: Merci, monsieur le président.

À propos de la protection de la sécurité de notre démocratie, je crains que le gouvernement actuel ne cherche à se défiler et à se soustraire à ses responsabilités.

Si j'ai bien compris, les TI de la Chambre des communes ont un mandat très précis et étroit, qui est de protéger les systèmes de TI des Communes. Est-ce exact?

M. Eric Janse: Oui.

M. Garnett Genuis: Nous avons reçu des renseignements non classifiés au sujet d'échanges qui ont eu lieu entre le gouvernement, les représentants du gouvernement et la Chambre des communes. Ils donnent à penser que le gouvernement a fourni à la Chambre des communes des renseignements de nature essentiellement technique et dit qu'il était au courant de ces attaques. Il a communiqué des renseignements que la TI pourrait utiliser pour protéger les députés contre ces attaques, dans la mesure où le système de TI de la Chambre des communes est en cause. Est-ce exact?

M. Benoit Dicaire: C'est exact.

M. Garnett Genuis: Le gouvernement a avancé comme excuse pour n'avoir pas informé les députés, qu'il pensait que c'était à la Chambre des communes de le faire. Il me semble un peu fort de juger raisonnable que les renseignements techniques communiqués à la TI de la Chambre des communes amèneraient les professionnels de la TI à quitter leur poste de travail, monter à l'étage et commencer à parler de ces menaces aux députés. Il ne me semble pas que ce soit le travail des professionnels de la TI de la Chambre des communes. Êtes-vous d'accord?

● (1140)

M. Benoit Dicaire: Nous donnons suite à tout ce qui nous est envoyé en fonction des risques et de ces éléments.

Lorsque le Comité siégera à huis clos, nous pourrons probablement mieux vous renseigner au sujet de l'information précise que nous avons reçue au cours de cette séance d'information non classifiée, mais je peux dire publiquement que ce genre d'intervention fait penser à la résolution d'un casse-tête. Il ne s'agit pas de vous donner des renseignements précis...

M. Garnett Genuis: Eh oui. Au fond, je cherche sans doute à savoir qui est généralement responsable dans cette affaire, car nous ne voulons pas que, en matière de sécurité, tout le monde se renvoie la balle. Nous voulons que chacun assume ses responsabilités.

Je cède peut-être aux stéréotypes ou bien je me trompe, mais il me semble peu probable qu'il incombe aux spécialistes de la TI aux Communes qui reçoivent des informations de nature technique pour réagir aux menaces, de diffuser cette information et de se promener un peu partout pour renseigner les députés. C'est plutôt le rôle des experts en sécurité du gouvernement et non celle des techniciens de la TI aux Communes.

Ai-je raison? Je vois des hochements de tête.

M. Stéphan Aubé: Effectivement, monsieur Genuis. Nous gérons les menaces qui nous sont signalées. Nous en cherchons les traces et, une fois que nous les avons trouvées, nous réagissons. Si des députés sont touchés, nous agissons de la sorte. Quant à l'auteur de la menace qui s'attaque à nous et à ses intentions, nous ne sommes pas au courant. Nous nous occupons seulement de la menace concrète.

M. Garnett Genuis: Tout à fait.

Le gouvernement du Canada, dans ses communications à ce sujet, a essayé de vous blâmer de ne pas avoir communiqué avec les députés au sujet des menaces. Il a prétendu que des employés qui ont un mandat très étroit et très précis concernant le système de TI de la Chambre des communes auraient dû prendre l'initiative d'évaluer et de mesurer la menace et d'informer les députés. Ce que vous confirmez, c'est que vous avez un mandat précis qui consiste à protéger le système de TI de la Chambre des communes. Ce mandat ne s'étend pas à mon courriel personnel, ne comprend pas les évaluations plus générales des menaces à la sécurité, ni la responsabilité de décider qu'il est dans l'intérêt public ou non d'informer les députés.

Si vous êtes à l'aise pour le faire, répondez à la question suivante: que répondez-vous aux communications du gouvernement qui semble vous blâmer plutôt que d'assumer la responsabilité de la décision de ne pas informer les députés?

M. Stéphan Aubé: Il serait préférable d'en discuter à huis clos, monsieur.

M. Garnett Genuis: D'accord. Vous êtes entièrement protégé pour tous les propos que vous tenez au Comité, mais je ne veux pas vous placer dans une position plus inconfortable que le gouvernement ne l'a déjà fait. J'ai beaucoup de respect pour le travail des employés de la Chambre des communes, mais il n'est ni juste ni raisonnable de s'attendre à ce que quelqu'un fasse quelque chose qui ne fait pas partie de son travail.

Comme on l'a dit, vous ne faites pas le suivi de mes courriels personnels. Vous ne vous occupez pas de ma sécurité dans ce genre de situation, et vous n'êtes pas nos organismes de sécurité. La Chambre des communes n'est pas un organe de sécurité. C'est la responsabilité du gouvernement de communiquer avec les députés sur ces questions, et il ne l'a pas fait.

Le président: Merci beaucoup, monsieur Genuis.

[*Français*]

Madame Fortier, vous avez la parole pour cinq minutes.

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

Je remercie les témoins d'être ici aujourd'hui pour répondre aux questions des membres du Comité.

Ma première question vise à mieux comprendre la situation.

Mis à part les membres de l'Institut d'administration publique du Canada, ou IAPC, qui ont été ciblés, savez-vous si d'autres parlementaires à l'extérieur de cette organisation l'ont aussi été pendant cette période?

M. Benoit Dicaire: Juste pour clarifier les choses, parlez-vous de parlementaires canadiens?

L'hon. Mona Fortier: Oui, je parle de parlementaires canadiens.

M. Benoit Dicaire: Non, il n'y a pas d'autres parlementaires canadiens qui ont été ciblés. Outre ce qui a été mentionné, il n'y a pas d'information supplémentaire à ce sujet.

Cela dit, des parlementaires d'autres pays ont été ciblés.

L'hon. Mona Fortier: Parfait. Merci beaucoup.

En tant que députée, je suis évidemment très préoccupée par ce qui est survenu pendant cette période et par ce qui se produit peut-être encore.

Quelles sont les mesures qu'un député doit prendre s'il reçoit un courriel préoccupant?

M. Benoit Dicaire: Je remercie la députée de la question, monsieur le président.

C'est une bonne question, madame Fortier. Des protocoles ont été établis et mis en place. Je m'attarderai surtout sur ceux qui concernent les courriels, puisque vous en avez parlé.

Nous avons plusieurs services en place, notamment des services de cybersécurité, qui sont accessibles 24 heures sur 24, 7 jours sur 7, où une personne peut téléphoner pour faire analyser un courriel en particulier. Nous avons aussi mis sur pied plusieurs campagnes de sensibilisation à ce sujet.

Je ne sais pas si vous l'avez vu, mais il est possible de sélectionner l'icône « hameçonnage » dans l'application de courriel lorsqu'on souhaite en signaler un qui est suspect.

● (1145)

L'hon. Mona Fortier: Comme vous le savez, cette question a été soulevée il y a quelques années. Depuis ce temps, nous avons reçu une directive ministérielle selon laquelle un député doit être immédiatement informé lorsqu'une menace est détectée.

D'une part, cette directive a-t-elle amélioré le flux d'information vers la Chambre des communes? Les députés sont-ils mieux informés?

D'autre part, pensez-vous que si cela s'était produit après l'envoi de la directive, le résultat aurait été différent?

M. Stéphan Aubé: Monsieur le président, je vais répondre à ce que je peux répondre.

Lorsqu'on nous informe d'un risque, nous faisons notre devoir, c'est-à-dire que nous communiquons avec le député.

La majeure partie du temps, lorsqu'on nous contacte, nous devons aborder le cas comme étant une menace sur le plan technique, sans savoir qui est derrière cette attaque à l'égard du parlementaire.

Je ne peux pas faire de commentaires sur la question de savoir s'il s'agit d'un risque lié à de l'influence intergouvernementale, car ce n'est pas ce sur quoi mon travail se concentre. Nous ne savons pas ces choses.

L'hon. Mona Fortier: Monsieur Dicaire, vous avez parlé plus tôt des divers niveaux de menace. Vous sembliez parler d'une grille.

Pouvez-vous nous expliquer les raisons qui vous incitent à communiquer avec le député ou le parlementaire?

M. Benoit Dicaire: L'information qui nous est communiquée est, dans chaque cas, très technique. C'est en quelque sorte une question d'analyse afin de savoir si quelqu'un en particulier a été visé ou si c'est un groupe de personnes ou une infrastructure particulière qui ont été visés. Le niveau d'intervention est ensuite choisi en fonction du niveau de risque que la situation comporte.

Comme M. Aubé l'a dit, si une information montre que quelqu'un est visé par une menace telle qu'elle est définie dans la politique relative à l'utilisation acceptable du réseau, nous allons en informer directement le bureau du député. Je pourrais vous citer des exemples d'interventions qui ont été faites directement par l'équipe de cybersécurité. Dans l'un des cas, un des membres de cette équipe a téléphoné au bureau d'un député pour valider des choses particulières concernant de l'information qui avait été reçue.

C'est un peu ce à quoi ressemble le protocole associé à ce type de situation. Nous examinons l'efficacité des mécanismes de défense. Par la suite, s'il y a encore un risque résiduel, nous en faisons part directement au bureau du député.

L'hon. Mona Fortier: Je vais vous poser une question un peu simple. Lorsqu'une situation exige que vous contactiez le bureau d'un député, entrez-vous d'abord en communication avec le député lui-même avant de joindre son équipe?

Pouvez-vous nous expliquer votre approche? Je pense que cela pourrait aider à clarifier certaines choses quant à l'équipe entourant un député.

Le président: Il vous reste environ 20 secondes pour répondre à la question, monsieur Aubé.

M. Stéphan Aubé: Parfait, monsieur le président.

Lorsqu'une attaque vise un député en particulier, notre première réaction est d'entrer en contact avec lui. Si nous n'arrivons pas à le joindre, nous parlons au chef de cabinet. Si nous n'arrivons pas à joindre ce dernier, nous parlons à quelqu'un de l'équipe. Nous demandons alors que l'on contacte le député pour que celui-ci communique avec nous.

Nous abordons ces sujets directement avec les députés. C'est notre approche.

L'hon. Mona Fortier: Merci.

Le président: Merci, tout le monde.

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

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

Je vous avoue que je suis très préoccupée quant à notre démocratie. Un projet de loi sera adopté sous peu. C'est un grand virage que nous devons prendre, et cela me fait peur.

Je suis aussi préoccupée par le fait que votre capacité d'agir est limitée dans l'exercice de vos fonctions. Nous passerons bientôt à huis clos. J'aimerais vraiment, puisque vous êtes les personnes toutes désignées pour nous proposer des pistes de solution, savoir ce dont vous avez besoin pour prévenir ce type de situation, pour agir et pour prendre des mesures.

Cela va aussi loin que de nous dire quel est le rôle des parlementaires, alors que la propagande s'insinue jusque dans nos comptes personnels, alors que je ne peux même pas déterminer moi-même ce qui est vrai et ce qui ne l'est pas. Quand des séries sont conçues pour influencer des millions de personnes qui les écoutent, ça va loin. Cela devrait sonner l'alarme.

J'aimerais dire aux gens qui nous regardent que je juge important que nous mettions dans notre rapport toutes les recommandations que vous allez faire.

Cela dit, j'aurai des questions très précises à poser au cours des prochaines minutes.

Merci beaucoup, monsieur le président.

● (1150)

M. Eric Janse: J'aimerais répondre brièvement à la question.

Mme Marie-Hélène Gaudreau: Bien sûr, vous avez le temps de le faire.

Le président: Vous avez la parole, monsieur Janse.

M. Eric Janse: Je vais vous donner une réponse plus globale bientôt. Nous pourrons alors en discuter davantage.

Comme le sergent d'armes l'a mentionné plus tôt, lors de deux ou trois réunions antérieures du Bureau de régie interne, des ressources assez considérables ont été approuvées, surtout pour le Bureau du sergent d'armes. Cela a aussi une incidence sur d'autres services qui sont liés à la sécurité et à la cybersécurité.

Nous croyons que, pour l'instant, notre position est bonne. Nous pourrons bientôt vous fournir des réponses précises à vos questions.

Mme Marie-Hélène Gaudreau: J'en profite pour dire que ce qui a été mis en place jusqu'à maintenant fonctionne très bien. J'ai moi-même participé à une séance d'information organisée par le Service canadien du renseignement de sécurité. Le Bureau du sergent d'armes m'a aussi offert de l'accompagnement. Le signal d'alerte est là. Il faut donc s'en occuper.

Je vous remercie.

Le président: Merci, madame Gaudreau.

[*Traduction*]

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

Mme Lindsay Mathyssen: Merci.

En ce qui concerne cette question de privilège, nous n'avons pas été les seuls à être informés de ce piratage par les médias. D'autres membres de l'IAPC — de la Belgique, de la Nouvelle-Zélande, de l'Australie et d'autres — en ont également eu connaissance par la voie des médias publics, si j'ai bien compris. Leurs gouvernements sont de part et d'autre du spectre politique. Dans la majorité des cas, ils n'ont pas informé leurs membres.

Que faisons-nous pour nous informer au sujet des enquêtes menées par les autres parlements qui étudient cette question, ou pour en tirer des leçons? Comment intégrons-nous cela dans nos propres études, et comment abordons-nous le problème dans notre pays?

M. Benoit Dicaire: C'est une excellente question, madame Mathyssen. Je pourrais parler un peu plus de nos partenariats quand nous serons réunis à huis clos.

Je peux certainement affirmer publiquement que nous avons des partenariats avec d'autres parlements qui ont été touchés par ce genre d'attaques. Nous sommes en dialogue constant avec nos partenaires de ces parlements.

Mme Lindsay Mathyssen: Nous constatons, évidemment, qu'il y a divers niveaux de compréhension de la gravité de la situation. Même dans le rapport du CPSNR dont j'ai parlé tout à l'heure, qui a fait les manchettes, il y a une interprétation différente du renseignement.

Comment vous donne-t-on la capacité, en tant qu'organisme ne recueillant pas de renseignements, de tirer des conclusions sur la portée de l'ingérence étrangère? Avez-vous des ressources adéquates? C'est un sujet dont nous parlons souvent, même dans le cadre de l'étude sur le harcèlement. Avez-vous les ressources dont vous avez besoin? Avez-vous besoin de quelque chose afin de pouvoir mieux informer le Comité pour la préparation de son rapport?

M. Eric Janse: C'est une très bonne question, madame Mathyssen.

Pour l'instant, nous estimons que nous disposons des ressources appropriées avec ce que le Bureau de régie interne nous a accordé récemment. Cela pourrait changer à l'avenir, mais au nom de mes collègues ici présents, je pense que pour le moment, nous estimons avoir les ressources nécessaires.

Mme Lindsay Mathyssen: Éprouvez-vous une certaine gêne à interpréter ces renseignements vis-à-vis de la Chambre des communes et des organismes de sécurité parce que vous n'êtes pas un organisme de renseignement?

M. Patrick McDonell: Nous avons d'excellentes relations avec les organismes de sécurité. Nous n'éprouvons absolument aucune gêne à communiquer avec notre principal partenaire en matière de renseignement, qui est le SCRS.

Le président: Merci beaucoup, madame Mathyssen.

Monsieur Duncan, vous avez la parole pour cinq minutes.

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

Je remercie les témoins d'être ici ce matin.

J'ai quelques questions.

Je tiens à reconnaître que je pose cette question en public. Je tiens à préciser que je ne vous demande pas de divulguer des noms de députés ou d'acteurs d'États étrangers dans votre réponse.

Le Président a jugé que le fait de ne pas avoir avisé M. Genuis et les autres députés visés dans cette affaire constituait de prime abord une question de privilège. L'administration de la Chambre, le gouvernement et les organismes de sécurité avaient été informés au sujet de certains députés et d'un acteur étranger menaçant, mais les députés n'ont été mis au courant que lorsque des révélations externes ont été faites, dans ce cas-ci, par l'entremise du FBI et du département de la Justice des États-Unis. M. Genuis a soulevé, à juste titre, la question de savoir qui a la responsabilité de parler aux députés à ce sujet.

Cela dit, j'aimerais poser à chacun d'entre vous une question en vous demandant de répondre par oui ou par non, afin de ne rien divulguer du point de vue de la sécurité, ou de ce qui est en cours d'examen.

L'un d'entre vous a-t-il connaissance d'autres cas passés ou actuels où vous avez été informés, dans le cadre de vos rôles respectifs, par le CST, le SCRS, le FBI, un organisme de sécurité ou quiconque au sein du gouvernement fédéral, qu'un acteur étranger identifiable visait ou vise un député ou un groupe de députés, et où les personnes visées n'ont pas été informées de cette menace? Si vous êtes au courant de cela en ce qui concerne un ou plusieurs députés et un acteur d'un État étranger en particulier, savez-vous si les députés concernés n'en ont pas encore été informés?

● (1155)

M. Benoit Dicaire: En ce qui concerne la cybersécurité, je peux répondre par la négative.

Allez-y, monsieur McDonell.

M. Patrick McDonell: La réponse est non, monsieur.

M. Eric Duncan: À votre connaissance, il n'y a pas de cas en suspens.

Dans ce cas-ci, vous saviez que des députés étaient ciblés et vous aviez été informés par les organismes de sécurité que le... Il n'y a pas d'autres cas en suspens dont nous allons entendre parler dans trois mois par l'entremise d'un lanceur d'alerte ou d'un reportage des médias disant qu'il s'est produit telle ou telle chose. À votre connaissance, il n'y a aucun cas en suspens de députés qui n'ont pas été informés.

M. Patrick McDonell: Chaque fois que notre principal partenaire en matière de renseignement communique avec nous et nous fournit des renseignements concernant un député, nous communiquons immédiatement avec le député en question.

M. Eric Duncan: Monsieur Janse, j'aimerais vous poser une question.

Le Comité a adopté un ordre de production de documents s'adressant au gouvernement et à l'Administration de la Chambre. Cet ordre permet aux ministères de caviarder certains passages des documents conformément à la Loi sur l'accès à l'information. Étant donné que la Chambre des communes n'est pas un ministère du gouvernement et qu'elle n'est pas assujettie à la Loi sur l'accès à l'information, compte tenu de votre rôle, pouvez-vous confirmer que l'Administration de la Chambre nous fournira les documents non caviardés en réponse à cet ordre?

M. Eric Janse: C'est certainement notre intention.

Monsieur Bédard, voulez-vous ajouter quelque chose?

M. Michel Bédard: Nous avons reçu l'ordre de production de documents du Comité. Selon notre interprétation de cet ordre, l'Administration de la Chambre étant considérée comme un ministère, nous devons appliquer les principes qui y sont énoncés au sujet des passages caviardés. Si le Comité souhaite apporter des précisions supplémentaires au sujet de son ordre de production, nous nous ferons un plaisir de l'appliquer tel qu'il a été adopté par le Comité.

M. Eric Duncan: Selon votre interprétation, vous êtes un ministère, mais selon la nôtre, la Chambre des communes n'est pas un ministère et n'est pas une agence, de sorte qu'elle n'est pas visée par ce qui figure dans la directive du Comité.

M. Michel Bédard: Monsieur, avec tout le respect que je vous dois, lorsque les comités adoptent des ordres de production de documents, nous devons les interpréter. Lorsque nous avons lu l'ordre, la façon dont il a été rédigé... Il n'est pas inhabituel que, dans une loi du Parlement, la Chambre des communes soit considérée comme un ministère dans un but très précis, mais en général, et en raison de la séparation des pouvoirs, il est très clair que la Chambre des communes n'est pas un ministère. Selon notre interprétation de l'ordre de production de documents, nous avons été assimilés à un ministère aux fins de cet ordre, et nous devions donc suggérer des caviardages pour le Comité.

L'ordre de production renvoie à des lois du Parlement. Ce n'est pas clair, parce qu'il parle de la « Loi sur l'accès à l'information et la protection des renseignements personnels ». Ce sont deux lois distinctes. Lorsqu'il s'agit d'ordres de production de documents, nous devons toujours les interpréter lorsqu'il y a ambiguïté. Si vous avez besoin de consulter l'administration et notre bureau pour la rédaction d'un tel ordre, nous nous ferons un plaisir de vous aider pour nous assurer que l'ordre reflète bien l'intention du Comité.

Le président: Monsieur Duncan, je crains que votre temps soit écoulé.

Monsieur Collins, vous avez les cinq dernières minutes avant que nous suspendions brièvement la séance.

Monsieur Collins, vous avez la parole pour cinq minutes.

M. Chad Collins (Hamilton-Est—Stoney Creek, Lib.): Merci, monsieur le président.

Permettez-moi de commencer par le seuil à partir duquel nous considérons qu'un député a été attaqué de quelque façon que ce soit. Nous lisons dans le rapport que ces attaques sont lancées assez souvent, probablement quotidiennement, par des acteurs qui cherchent à miner nos efforts pour faire avancer nos entreprises.

Quel est le seuil pour votre équipe? J'ai entendu parler d'un « travail d'équipe » aujourd'hui. Quel est le seuil établi par l'équipe pour la notification aux députés? Qu'est-ce qui est considéré comme une menace mineure? Qu'est-ce qui déclenche un signal d'alarme interne qui vous amène à informer un député.

● (1200)

M. Benoit Dicaire: Je peux parler brièvement des cybermenaces, puis mon collègue pourra probablement parler du risque lié aux menaces physiques.

Tout ce qui touche les données des députés, l'information des députés, est considéré comme critique, alors nous voyons s'il y a quoi que ce soit relativement à ces paramètres. Parfois, ce sont les identités numériques qui sont ciblées plutôt que l'infrastructure, un service ou une application en particulier. S'il y a une attaque touchant les données d'un député, nous communiquons directement avec son bureau.

Les autres catégories se résument au facteur de risque ou au risque résiduel. Des mécanismes de protection sont-ils en place et peuvent-ils protéger l'infrastructure pour assurer la continuité des opérations? Cela réduit le risque pour notre capacité de nous protéger, mais si quelque chose présente un risque résiduel, nous communiquons avec le bureau du député.

M. Chad Collins: Le protocole de 2014 dont il a été question précédemment a-t-il atteint le seuil?

M. Stéphan Aubé: Je préférerais que nous en discutions à huis clos, monsieur. Je dois parler des incidents pour répondre à cette question.

M. Chad Collins: Très bien, je comprends.

Il s'agit d'une grande organisation, et quelqu'un, dans l'une des réponses, a parlé d'un travail d'équipe. Bien sûr, le rapport fait état de tous les aspects qui entrent en ligne de compte lorsqu'il y a un échange d'information. À ce moment-là, il y a beaucoup de collaboration et beaucoup de gens ont la main sur le volant. Je crois important que nous comprenions qui conduit.

Pouvez-vous nous parler de la hiérarchie des responsabilités partagées dans tous les secteurs? Pouvez-vous nous parler de vos relations? Lorsqu'un secteur demande des renseignements à un autre et qu'ils ne sont pas fournis, qui intervient pour régler le problème?

M. Eric Janse: C'est une question très intéressante, monsieur Collins. Il s'agit absolument d'une collaboration. Je ne sais pas s'il y a une hiérarchie en tant que telle, mais c'est une collaboration entre différents groupes qui ont des mandats précis. Je pense que c'est une question d'échange d'information et, souvent, de décision collective sur les mesures à prendre, et ce qui doit être fait en conséquence.

M. Chad Collins: En ce qui concerne la collaboration qui a eu lieu, nous avons lu que, dans certains cas, des renseignements ont été demandés, mais qu'il y a eu des retards ou que les renseignements n'ont pas été communiqués. En pareils cas, qui intervient pour régler le problème? Je ne veux pas parler de conflits, mais il y a eu un accroc dans la collaboration dont vous avez parlé. Que se passe-t-il en pareils cas? Qui, au sein de la hiérarchie — parce qu'il y a une hiérarchie au sein de l'organisation — est responsable de régler ce genre de problème lorsque la collaboration ou la communication s'interrompt?

M. Benoit Dicaire: Je pense que la collaboration est vraiment forte au sein des partenariats. Je peux en témoigner. Nous avons mis en place des protocoles liés à l'échange de renseignements. Comme M. Aubé l'a mentionné au sujet du partage des données des députés, nous ne le faisons pas explicitement sans votre consentement. Il y a parfois des demandes de partage de données qui nécessitent un consentement. À ce moment-là, nous ne les communiquons pas nécessairement à moins qu'il y ait un risque et que le bureau du député donne son consentement.

Cela dépend aussi du type d'activité. Nous avons parlé plus tôt des menaces. Il y a beaucoup de travail d'enquête à faire, et il s'agit de rassembler les pièces du casse-tête. Parfois, la pertinence de l'information n'est pas claire au moment de la demande, alors nous devons clarifier l'information que nous avons à ce moment-là.

M. Chad Collins: Je ne parle pas nécessairement de...

Le président: Monsieur Collins, il ne reste que quelques secondes. Si vous voulez poser une dernière question rapidement, je vais vous permettre de le faire.

M. Chad Collins: Bien sûr.

Je pense que le problème se situe à l'interne — pas au niveau du député — lorsqu'on demande une information. Disons que le CST demande des renseignements au personnel de sécurité des TI de la Chambre des communes et que ces renseignements n'arrivent pas. Quelqu'un les a demandés pour une raison précise. C'est pour essayer d'aller au fond des choses, dirons-nous.

Pouvons-nous savoir à huis clos ou en séance publique pourquoi cette information n'a pas été communiquée par quelqu'un?

● (1205)

Le président: Veuillez être très concis.

M. Benoit Dicaire: Nous en parlerons à huis clos, monsieur.

Le président: C'est bien et concis. Merci.

Chers collègues, nous allons suspendre la séance pendant quelques instants, puis nous poursuivrons à huis clos.

À titre de rappel, lorsque nous siégeons à huis clos, seuls le personnel autorisé, les députés et les témoins peuvent être présents dans la salle. J'aurais quelques brèves observations à faire à ce sujet, mais nous allons faire une courte pause pour nous préparer à accueillir notre prochain groupe de témoins.

Madame Mathyssen, je crois que vous devrez vous inscrire avec un nouveau lien. Nous allons demander au greffier de vous aider.

Chers collègues, c'était une autre heure productive. C'était significatif, informatif et efficace. Je vous remercie de votre collaboration. Nous nous reverrons dans quelques minutes.

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