CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

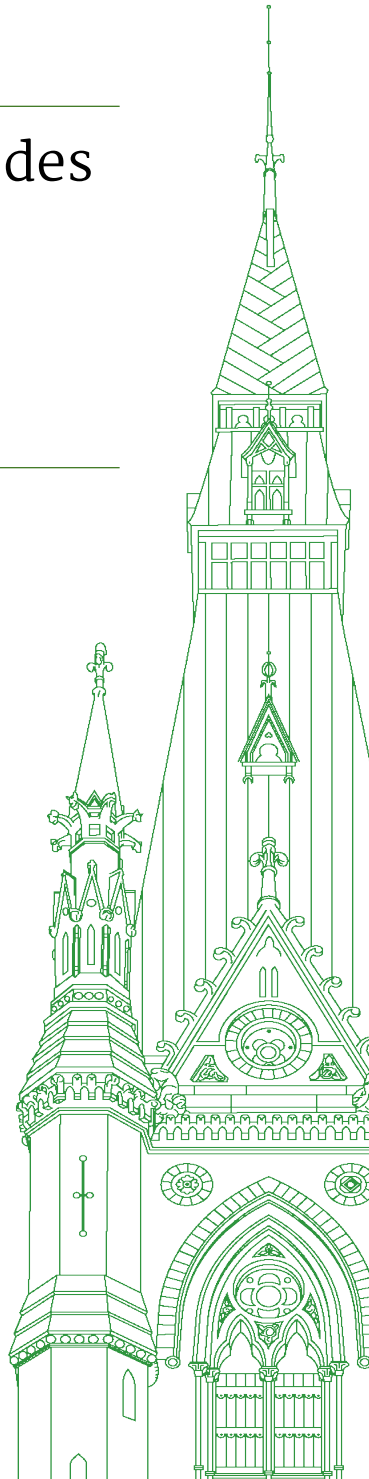
44e LÉGISLATURE, 1re SESSION

Comité permanent de la procédure et des affaires de la Chambre

TÉMOIGNAGES

NUMÉRO 121

Le jeudi 13 juin 2024



Président : M. Ben Carr

Comité permanent de la procédure et des affaires de la Chambre

Le jeudi 13 juin 2024

● (1100)

[*Traduction*]

Le président (M. Ben Carr (Winnipeg-Centre-Sud, Lib.)): Bonjour à tous. J'espère que vous passez une bonne semaine.

[*Français*]

Je vous souhaite la bienvenue à la 121e réunion du Comité permanent de la procédure et des affaires de la Chambre.

[*Traduction*]

Chers collègues, nous poursuivons notre étude de la question de privilège concernant des cyberattaques menées contre des députés.

Je vais faire un rappel de courtoisie, comme toujours lorsque nous entamons une séance. Assurez-vous que votre oreillette est placée sécuritairement sur un des autocollants situés de chaque côté de vous pour protéger la santé et le bien-être des interprètes, qui réalisent un travail si important pour nous.

Chers collègues, des collègues parlementaires se joignent à nous aujourd'hui. Le format reste le même.

Nous accueillons aujourd'hui James Bezan, député de Selkirk—Interlake—Eastman; Garnett Genuis, député de Sherwood Park—Fort Saskatchewan; et l'honorable John McKay, député de Scarborough—Guildwood.

Chaque témoin pourra présenter un exposé de cinq minutes, puis nous passerons à la première série de questions, comme à l'habitude.

Messieurs, je ne sais pas qui veut commencer. Je ne suis pas sûr que vous en ayez discuté entre vous, mais y a-t-il un volontaire pour commencer? M. Genuis, d'accord.

Monsieur Genuis, sur ce, vous avez la parole pour un maximum de cinq minutes pour présenter votre exposé.

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

Nous avons déjà exposé les faits importants de cette affaire à la Chambre. Je serai heureux de les répéter en réponse à vos questions, mais je vais utiliser mon exposé pour plutôt avancer des arguments précis sur ce que nous pouvons apprendre de cette situation.

D'un côté, nous nous attendons en général à ce que la sécurité nationale soit entourée d'un haut niveau de confidentialité. Même si, dans une démocratie libre, les gens devraient normalement avoir accès aux informations sur ce que fait le gouvernement, on garde scrupuleusement les renseignements sur la sécurité nationale, parce que nos adversaires pourraient les utiliser contre nous.

De l'autre, c'est un principe bien établi de la sécurité nationale qu'il faut communiquer les informations aux citoyens s'ils en ont besoin pour se défendre. Par exemple, si nous étions en guerre et qu'on allait bombarder une région en particulier de façon imminente...

Le président: Monsieur Genuis, je suis désolé de vous interrompre. Les interprètes viennent tout juste de me dire que votre cadence est un peu rapide, donc si vous pouviez juste ralentir un peu... Je serai généreux, et si nous devons vous donner 30 secondes de plus pour le bien-être des interprètes, nous allons vous les offrir.

Allez-y, madame Romanado.

Mme Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Dans le même ordre d'idées, je crois comprendre que M. Duncan a demandé aux témoins de fournir leur exposé avant la réunion. Les avons-nous reçus? Je ne suis pas sûre que les interprètes en ont une copie.

Le président: Je ne connais pas la réponse à cette question, madame Romanado.

M. Garnett Genuis: Je vous ai envoyé mon exposé.

Le président: Vous nous l'avez envoyé, d'accord.

Merci, monsieur Genuis. J'ai arrêté le chronomètre. Il vous reste 4 minutes et 15 secondes.

M. Garnett Genuis: Merci, monsieur le président. Je vous remercie de votre indulgence.

De l'autre, c'est un principe bien établi de la sécurité nationale que nous devons communiquer les informations aux citoyens s'ils en ont besoin pour se défendre. Par exemple, si nous étions en guerre et que nos adversaires allaient bombarder une région de façon imminente, on s'attendrait à ce que le gouvernement avertisse les citoyens de cette attaque pour qu'ils puissent se mettre à l'abri. On ne s'attendrait pas à ce que le gouvernement garde ces informations secrètes, évidemment. Si un terroriste plaçait une bombe dans un édifice, on s'attendrait à ce que cet édifice soit immédiatement évacué, et on ne s'attendrait pas à ce que le gouvernement garde ces informations secrètes, juste parce qu'il est question de sécurité nationale.

Ce qui est bien sûr vrai pour les attaques physiques devrait, par extension du même principe, aussi s'appliquer aux cas plus bénins de cyberattaques et d'autres genres d'attaques venant de l'étranger. Le principe demeure que la victime ou la victime potentielle a le droit de savoir ce qui l'attend pour qu'elle puisse se défendre.

Qui plus est, l'ingérence étrangère constitue un cas particulier où l'exposition joue un rôle central dans la solution. On peut réduire de beaucoup les conséquences de la désinformation étrangère quand les gens sont mis au courant de la source. De cette manière, la désinformation est dénoncée comme étant de la propagande, et elle perd ainsi son pouvoir de persuasion. La prise de contrôle de nos institutions par des intérêts étrangers peut être renversée si l'on expose les faits, et les politiciens qu'on identifie comme des collaborateurs étrangers sont moins susceptibles d'être réélus. Quand les gens savent que la source de quelque chose est un État étranger hostile, la sensibilisation peut atténuer la menace.

Le gouvernement actuel utilise la sécurité nationale comme excuse pour garder secrètes les informations sur l'ingérence étrangère qui seraient d'intérêt national, ou qui aideraient à protéger les victimes et à réduire l'incidence globale. Nous connaissons trois exemples de ce phénomène: le secret qui a longtemps entouré l'affaire des documents du laboratoire de Winnipeg, la non-dénonciation aux députés des menaces qui pèsent contre eux et leur famille — ce qui nous a amenés à soulever deux questions de privilège distinctes que le Président de la Chambre a reconnues — et l'insistance actuelle du gouvernement pour tenir secrets les noms des parlementaires qui ont intentionnellement collaboré avec des États étrangers hostiles. C'est difficile de voir comment on sert l'intérêt public en gardant le secret sur ces trois affaires.

En ce qui concerne l'ingérence étrangère, nous devrions agir de façon stratégique et déclassifier certaines informations précisément pour lutter contre cette ingérence. Pour se défendre de ne pas m'avoir informé des menaces qui pesaient contre moi, le gouvernement a parlé de ces menaces à la Chambre des communes. Il a dit qu'il respectait le rôle de la Chambre à titre d'institution distincte du pouvoir exécutif.

En réponse à cette situation, je vais faire cinq observations.

Premièrement, comme vous le savez, on a ciblé mon compte de courriel personnel. Ces attaques contre des comptes parlementaires ont été signalées au personnel des TI de la Chambre des communes. Je présume qu'on n'a même pas informé l'administration de l'attaque contre moi, parce que cela n'a rien à voir avec son travail.

Deuxièmement, nous n'avons toujours pas entendu de témoignages clairs sur les informations exactes qui ont été transmises au personnel des TI de la Chambre et le moment où cela a été fait. On ne sait pas s'il s'agissait simplement de quelques détails techniques, ou plutôt de l'ensemble des informations que le FBI a transmis à nos services de renseignement. Sans brosser le portrait complet de l'affaire, il aurait été difficile de nous informer de la situation.

Troisièmement, de par les arguments qu'il nous soumet, le gouvernement semble bien mal comprendre le travail des professionnels des TI, qui ne sont pas un service de renseignement ou de communications. Ils travaillent à des questions de TI. En principe, il serait étrange que ces professionnels décident de leur propre chef d'aller parler aux parlementaires des menaces auxquelles ils sont confrontés.

Quatrièmement, les représentants du Centre de la sécurité des télécommunications ont reconnu dans leur témoignage qu'il y avait sans doute des bémols à apporter aux informations transmises qui ont empêché des employés de la Chambre de retransmettre les informations sans permission. Je recommande que le Comité demande des informations plus nombreuses et plus claires sur ce qui a été communiqué exactement au service des TI de la Chambre des communes. Il faut savoir quand on a communiqué ces informations et avec quelles réserves.

Enfin, la logique sous-jacente des arguments du gouvernement pour garder le secret est profondément lacunaire, parce que les députés disposent de droits et de privilèges. Les droits et privilèges qui nous sont conférés nous permettent de faire notre travail dans l'intérêt de nos électeurs. On peut abdiquer ces droits ou les modifier avec l'accord de la Chambre, mais ce n'est pas l'administration de la Chambre qui en dispose, qui les contrôle ou qui les modifie. Pour respecter les droits et l'indépendance des députés, il faut leur donner les outils et les renseignements dont ils ont besoin. Le gouvernement prétend que c'est l'administration de la Chambre qui est titulaire de nos droits, plutôt que les députés eux-mêmes. Évidemment, il n'y a rien de plus faux.

Monsieur le président, je conclus ainsi mon exposé. Je répondrai à vos questions avec plaisir.

● (1105)

Le président: Merci beaucoup, monsieur Genuis.

Passons-nous à M. Bezan ou à M. McKay?

Monsieur Bezan, vous avez la parole pendant cinq minutes.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président.

Bonjour, chers collègues.

Je fais aussi partie des 18 députés et sénateurs membres de l'Alliance interparlementaire sur la Chine. Le groupe APT31 nous a ciblés il y a longtemps, en 2021 et en 2022.

Ce qui est choquant, c'est en tant que parlementaires, on ne nous a jamais dit que nous faisions l'objet d'une tentative de piratage ou d'une cyberattaque par le régime communiste de Chine. Si nous avions été mis au courant, nous aurions pu prendre des mesures de protection et correctives à titre de parlementaires, mais nous n'avons pas pu le faire, parce qu'on ne nous en a jamais informés. Les services des TI de la Chambre des communes ne nous ont jamais informés, pas plus que la GRC. Le SCRS ne nous a pas informés ni le CST, qui a finalement reçu des informations du FBI qu'il a transmis aux services des TI de la Chambre.

Le FBI nous a tous renseignés le 9 mai. Je pense que c'est embarrassant. C'est finalement ainsi que nous avons été informés de la façon dont l'attaque s'est déroulée et des moyens de nous protéger.

Je dois dire que par le passé, le sergent d'armes offrait... et il a offert de nous donner une séance d'information cet après-midi. Les informations ne sont pas classifiées, mais il est question de la façon de nous protéger contre les attaques de cybersécurité et de quelles mesures nous devons adopter. Par le passé, des représentants du CST m'ont donné une séance d'information, ainsi qu'à d'autres personnes ciblées par la mésinformation et la désinformation de la RPC sur les réseaux sociaux.

Bien sûr, la Chambre des communes, Affaires mondiales Canada et la Défense nationale ont remis un téléphone jetable à tous ceux d'entre nous qui voyagent dans le cadre de nos activités parlementaires, et ils nous ont renseignés en matière de voyages. Je connais peut-être un peu mieux que d'autres les menaces à la cybersécurité qui existent, mais cela n'excuse pas les mesures que la Chambre des communes et les responsables ont prises, parce qu'il ne s'agit pas d'un incident isolé. Ces menaces se produisent tout le temps, et il faut mieux nous informer.

La RPC m'espionne depuis un certain temps. Je participe à diverses activités. J'appuie Hong Kong Watch. Je suis membre du Groupe d'amitié parlementaire Canada-Taïwan, comme bon nombre d'entre vous. Un certain nombre d'entre nous autour de la table sont allés à Taïwan pas plus tard que l'an dernier.

Dans son rapport, le Comité des parlementaires sur la sécurité nationale et le renseignement nomme aussi l'Iran. Je suis cofondateur du groupe des Parlementaires canadiens pour les droits de la personne et la démocratie en Iran. Comme vous le savez, j'ai beaucoup insisté pour qu'on désigne la Brigade Al-Qods comme organisation terroriste en 2012. Au gouvernement, j'ai été l'instigateur de la fermeture de l'ambassade et des consulats iraniens au Canada, et la communauté persane a reconnu mes efforts.

Bien sûr, la Fédération de Russie me cible sur les réseaux sociaux avec des trolls, pas des robots, depuis longtemps. Dans le groupe des 13, j'ai été une des premières personnes interdites de séjour en Russie en 2014. Je suis vice-président du Groupe d'amitié parlementaire Canada-Ukraine. J'affiche clairement mon soutien à l'Ukraine, et la Russie s'attaque bien sûr à ceux d'entre nous qui défendent l'Ukraine. J'ai présenté la loi de Sergei Magnitsky.

Pourquoi est-ce que tout cela, toutes les activités qui dépassent mon simple rôle de parlementaire et mes activités quotidiennes comptent? C'est parce que l'espionnage moderne, l'intimidation et les tactiques d'ingérence étrangère bafouent non seulement nos droits et privilèges collectifs, mais aussi nos privilèges personnels. C'est la nouvelle norme.

Dans l'ouvrage de Bosc et Gagnon, la décision du Président qu'on trouve aux pages 107 et 108 précise que:

> ... les députés doivent pouvoir se livrer à leurs activités parlementaires sans être dérangés. Les voies de fait, les menaces et les insultes à l'égard d'un député au cours des délibérations du Parlement, ou alors qu'il circule dans l'enceinte parlementaire, constituent une atteinte aux droits du Parlement.

Il est aussi indiqué ce qui suit à la page 111:

> Un député peut aussi faire l'objet d'obstruction ou d'ingérence dans l'exercice de ses fonctions par des moyens non physiques.

● (1110)

Nous devons moderniser nos efforts pour protéger notre privilège contre les cyberattaques. Cela ne diffère pas d'une obstruction ou d'une ingérence par des moyens physiques alors que nous accomplissons nos tâches. Cela me préoccupe particulièrement. Je suis ministre du cabinet fantôme conservateur pour la Défense nationale. Je suis vice-président du Comité permanent de la défense nationale, et M. McKay en est le président. Nous siégeons à divers comités. Nous communiquons des informations. Je conseille notre chef. Nous élaborons des politiques et des idées pour notre programme.

Si ceux qui tentent de pirater mes courriels et mes communications me ciblent, monsieur le président — et je sais qu'il me reste peu de temps —, alors nous devons prendre des mesures correctives. Le laissez-faire et la culture de nonchalance du Cabinet du premier ministre et du Bureau du Conseil privé se sont propagés dans les ministères et notre façon de fonctionner par ici. Nous devons nous assurer d'être plus énergiques dans notre façon de nous protéger les uns les autres contre ces cyberattaques. Cela signifie que nous devons savoir quand nous devons reclassifier les informations et modifier notre façon de les communiquer.

Merci.

Le président: Merci beaucoup, monsieur Bezan.

Monsieur McKay, vous avez la parole pendant cinq minutes tout au plus.

L'hon. John McKay (Scarborough—Guildwood, Lib.): Merci, monsieur le président.

Je vais juste reprendre là où M. Bezan s'est arrêté et parler de l'enjeu principal qui occupe le Comité, soit le moment où il faut informer les députés de ces attaques. Ces attaques sont tout simplement inévitables; elles sont de grande ampleur, et vont augmenter en nombre.

J'espère bien que votre comité va se pencher sur la façon, le moment et l'endroit où l'on nous informe de ces attaques, parce que, bien franchement, je crois comprendre qu'on commet environ un million d'attaques par jour contre le Parlement du Canada. Je ne pense pas que tous les députés veuillent être mis au courant de chacune de ces attaques.

À certains égards, nous avons la chance que les données montrent jusqu'ici que nous n'avons pas subi de dommages. Il n'y a pas eu d'atteinte, et les pare-feu tiennent le coup. Cela dit, c'est plutôt embarrassant — je suis d'accord avec mes amis — d'apprendre de la part d'un service de sécurité étranger qu'on nous a attaqués. Je dois admettre que c'est tout à fait inacceptable, selon moi.

Le FBI a informé le CST, qui a informé nos services de sécurité, et ces derniers sont convaincus qu'il n'y a pas eu d'atteinte et nous laissent dans l'ignorance. Nous n'avons rien su pendant deux ans, et ce n'est qu'en raison d'un document descellé du FBI que nous avons été mis au courant de ces attaques.

Lorsque des représentants du FBI nous ont donné une séance d'information, ils nous ont dit se sentir pilonnés — je pense que c'est le mot qu'ils ont utilisé — à 50 contre 1. Ces attaques sont massives, et le FBI se sent dépassé.

À mon avis, ce comité doit examiner nos protocoles. C'est clair que les protocoles actuels sont inacceptables. Pendant deux ans, nous avons tous les trois, en plus de tous nos collègues, été très vulnérables.

● (1115)

J'espère sincèrement que le Comité traitera du cœur de la question. Il ne faut pas trouver quelqu'un à qui jeter la pierre ou dire que nous aurions dû faire ceci ou cela. Des protocoles doivent être établis parce que toutes les personnes assises autour de cette table, tous les collègues, sont vulnérables. J'espère que vous vous servirez de cet épisode révélateur de notre vulnérabilité — qui n'a entraîné par ailleurs aucun préjudice pour autant que je sache — pour donner des instructions à ceux qui sont chargés de nous protéger.

Pour revenir encore une fois au point de vue de M. Bezan, notre participation à un grand nombre d'activités nous rend vulnérables et fait partie de nos privilèges parlementaires.

J'appuie la motion de M. Genuis, mais je veux que le Comité se concentre sur la mise en place de protocoles appropriés.

Merci.

Le président: Merci beaucoup, monsieur McKay.

Chers collègues, nous passons à la première série de questions.

Monsieur Cooper, vous avez la parole pour six minutes.

M. Michael Cooper (St. Albert—Edmonton, PCC): Merci beaucoup, monsieur le président.

Merci, chers collègues.

Le Comité a reçu une chronologie des événements établie par le CST. La chronologie indique que le SCRS a présenté, pas plus tard qu'en novembre 2021, des informations sur la cyberattaque menée par le groupe APT31 de Pékin à 35 clients du gouvernement du Canada.

J'ai demandé au directeur du SCRS le nom des personnes ayant reçu les informations. M. Vigneault a fourni une liste au Comité tout en précisant qu'en règle générale, les produits de ce type étaient remis au Bureau du Conseil privé, y compris au conseiller à la sécurité nationale et au renseignement du premier ministre.

Que pensez-vous du fait que 35 clients du gouvernement du Canada, dont faisait probablement partie le ministère du premier ministre, soit le Bureau du Conseil privé, aient reçu des informations sur la cyberattaque aussi tôt qu'en novembre 2021, mais que vous et les autres députés qui étaient ciblés n'ayez pas été mis au courant?

N'importe qui souhaiterait...

L'hon. John McKay: Je serais heureux de répondre à cette question.

Monsieur Cooper, je pense que vous avez touché au nœud de l'affaire. Nous n'étions pas, si je puis dire, dans la liste des destinataires. Les protocoles à l'époque — il y a deux ans — se sont avérés franchement inadéquats.

J'espère que le Comité proposera des solutions parce que c'est inacceptable que nous n'ayons rien su pendant les deux dernières années.

M. James Bezan: Je vais ajouter quelque chose.

Des informations ont été transmises aux fonctionnaires. Comme l'indique le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement, la conseillère à la sécurité nationale et au renseignement n'a pas communiqué ces informations aux personnes concernées. Les informations sur l'attaque auraient dû nous être communiquées personnellement.

Quant à la culture au gouvernement du Canada sur la classification et la communication des informations, surtout les informations sur l'intimidation étrangère — précisons que l'attaque commise par APT31 n'est rien de moins que de l'intimidation par une force étrangère —, nous devons repenser les protocoles à suivre dans les cas d'intimidation étrangère. Le conseiller à la sécurité nationale doit prendre des mesures plus vigoureuses pour s'assurer que les informations parviennent aux parties concernées dans le système et qu'elles ne se rendent pas seulement au premier ministre.

Dans cette situation qui concerne des députés, les informations devraient être communiquées ou les personnes concernées devraient être contactées directement, que ce soit par le chef du caucus ou le président du caucus. Assurons-nous de ne pas répéter les mêmes erreurs. La communication des informations est essentielle à l'exercice de nos fonctions.

M. Michael Cooper: Monsieur Genuis, la parole est à vous.

M. Garnett Genuis: Je suis d'accord avec ce que mes collègues ont dit.

Merci d'avoir posé cette question importante, monsieur Cooper.

J'ajouterais un point au sujet de la diffusion des informations.

Lors des réunions précédentes, nous avons essayé de savoir quelles informations exactement avaient été communiquées notamment à l'Administration de la Chambre des communes. Les messages du gouvernement à ce sujet indiquaient que les « informations » — ce qui sous-entend toutes les informations — ont été communiquées à l'Administration de la Chambre des communes.

J'ai approfondi la question avec Mme Xavier, du CST. Je lui ai demandé si l'Administration de la Chambre des communes avait été mise au courant que l'auteur de la menace était APT31.

Mme Xavier a choisi soigneusement ses mots. Ce n'est qu'en lisant le compte rendu après la réunion que j'ai vraiment compris le sens de ses propos. Voici sa réponse à l'une de mes questions: « 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. »

Lorsque je lui ai demandé ensuite si elle avait indiqué à l'Administration de la Chambre des communes que l'auteur de la menace était APT31, Mme Xavier a refusé de confirmer cet élément en disant que ce serait plus approprié de discuter de certains éléments de la menace à huis clos.

Dans son témoignage, la cheffe du CST indique avoir divulgué ce qui lui semblait être la source de la menace, mais ne confirme pas avoir précisé à l'époque que cette source était APT31. De grandes questions restent sans réponse. Je crois que les fonctionnaires se livrent à un tour de passe-passe à propos de la nature des informations qui ont été communiquées notamment à l'Administration de la Chambre des communes.

● (1120)

M. Michael Cooper: Merci de votre réponse.

Même si je suis entièrement d'accord avec M. McKay sur la nécessité de trouver des solutions pour éviter que ce qui est arrivé se reproduise, je pense qu'il faut aussi se pencher sur la question de la responsabilité. Sur ce plan, le gouvernement a carrément abdiqué ses attributions en jetant le blâme sur l'Administration de la Chambre des communes.

Ensuite, lorsqu'une enquête sur l'Administration de la Chambre des communes a été lancée, le blâme est tombé sur les TI de la Chambre des communes. Pourtant, 35 clients du gouvernement du Canada, y compris fort probablement le ministère du premier ministre, soit le Bureau du Conseil privé, avaient été informés de la situation en novembre 2021. C'est plus d'un an et demi avant que vous ne soyez finalement informés de la situation grâce au FBI.

Je le répète, l'idée que les services de TI — qui exécutent un travail de nature technique pour assurer l'intégrité des systèmes de TI de la Chambre des communes — soient chargés d'informer les députés ne tient pas la route. Partagez-vous cet avis?

Une part de responsabilité devrait-elle revenir au Bureau du Conseil privé et à la conseillère à la sécurité nationale et au renseignement, puisque ces derniers ont été informés en novembre 2021 et qu'ils n'ont rien dit et rien fait pendant un an et demi? Ces instances n'auraient pas agi sans l'intervention du FBI.

Le président: Monsieur Cooper, malheureusement, le temps est écoulé. Vous aurez certainement l'occasion de soulever ce point à la prochaine série de questions.

M. Michael Cooper: Serait-il possible de simplement obtenir une réponse...

Le président: Malheureusement, votre préambule...

M. Michael Cooper: Je trouve très intéressant que vous m'interrompiez lorsque je soulève un point important.

Le président: Je ne vous interromps pas. J'applique tout simplement les règles de façon équitable. Vous aurez d'autres occasions de poser les questions à vos collègues.

Madame Romanado, la parole est à vous.

Mme Sherry Romanado: Merci beaucoup, monsieur le président. Par votre entremise, j'aimerais remercier les témoins de leur présence.

Je vais commencer par...

Monsieur le président, c'est mon temps de parole. Si M. Cooper voulait bien cesser de m'interrompre, ce serait...

M. Michael Cooper: Je veux une réponse à ma question.

Mme Sherry Romanado: Vous avez eu la possibilité de poser vos questions, monsieur Cooper. Je vous remercie de ne pas gruger mon temps de parole.

Chers collègues, je tiens d'emblée à préciser, vous auriez dû être mis au courant de la situation à l'époque. J'en suis entièrement convaincue. Je veux être certaine que vous me comprenez. Je suis tout à fait d'accord pour dire que ce qui est arrivé était inapproprié et que vous auriez dû être informés de la situation.

Nous essayons d'aller au fond des choses pour savoir ce qui est arrivé et formuler des recommandations pour que la situation ne se reproduise pas.

Je veux seulement obtenir des précisions de la part de chacun d'entre vous sur certains détails.

Monsieur Genuis, vous avez mentionné que c'était votre compte courriel personnel qui a été attaqué. Le confirmez-vous?

M. Garnett Genuis: C'est exact.

Mme Sherry Romanado: Votre compte courriel parlementaire a-t-il été touché également?

M. Garnett Genuis: Je ne pense pas que mon compte parlementaire ait été attaqué. À ma connaissance, seul mon compte personnel l'a été.

Mme Sherry Romanado: À quelle date avez-vous appris que vous aviez été victime d'une cyberattaque?

M. Garnett Genuis: J'en ai été informé plus tôt cette année par l'Alliance interparlementaire sur la Chine, ou IPAC. Nous avons eu une séance d'information conjointe. Pour revenir à la séquence des événements, M. McKay et moi-même, qui sommes les coprésidents de l'organisme, avons été les premiers à être mis au courant. Nous avons assisté à une séance avec des députés plus tard la même journée. J'ai été convoqué à ces réunions à très court préavis, mais tout cela s'est passé en l'espace de quelques jours à la fin avril de cette année.

● (1125)

Mme Sherry Romanado: Merci.

Monsieur Bezan, dans votre cas, parmi vos comptes courriel, quels sont ceux qui ont été visés par la cyberattaque?

M. James Bezan: Selon ce que nous a communiqué l'IPAC lors de sa séance d'informations fondée sur les données du FBI, c'était pour la plupart d'entre nous le compte P9 qui était visé. Sauf erreur, on nous a dit — même si je ne me suis jamais entretenu avec les services de TI, le Service de protection parlementaire ou le sergent d'armes — que les TI ont pu intercepter les attaques à temps. Le pare-feu a fonctionné.

Dans le cas de M. Genuis, c'est son compte personnel qui a été visé, ce qui est troublant. Pour répondre à ce que disait M. Cooper, j'ajouterais que...

Mme Sherry Romanado: Je n'ai pas le temps...

M. James Bezan: ... le Service de protection parlementaire, le sergent d'armes et les services de TI de la Chambre des communes ont tous un rôle à jouer pour nous tenir informés lorsque ces choses se produisent.

Mme Sherry Romanado: Je suis d'accord.

Je vais m'adresser à M. McKay.

Monsieur McKay, la cyberattaque visait-elle votre compte personnel, votre compte parlementaire ou les deux?

L'hon. John McKay: À ma connaissance, c'était mon compte P9.

Mme Sherry Romanado: Vous l'avez appris à la fin du mois d'avril cette année. Est-ce exact?

L'hon. John McKay: Oui.

Mme Sherry Romanado: Le Comité a entendu le CST, l'Administration de la Chambre des communes et le SCRS. Comme vous avez sûrement dû le noter, M. Genuis, la structure semble permettre à chaque service de dire: « Ce n'est pas mon rôle d'informer les députés. » Chacun travaille dans les limites de sa description de tâches et personne ne semble savoir qui a la responsabilité d'informer les parlementaires. Notre étude a pour objet entre autres de mettre en place des protocoles adéquats pour se préparer à une autre situation...

Une directive ministérielle a été émise à l'intention du SCRS en mai 2023 qui indiquait que les députés devaient être mis au courant.

Auriez-vous des recommandations pour le Comité concernant... Je ne vous demande pas de proposer un processus détaillé. Si une situation comme celle-là se reproduisait, quelle voie de communication recommanderiez-vous d'utiliser pour que les députés soient mis au courant immédiatement?

L'hon. John McKay: Si je devais établir un protocole, j'aurais en tête le fait que — comme M. Cooper le soulignait dans sa question — plusieurs responsables au gouvernement semblaient être au courant, mais pas nous. C'est inacceptable.

Je voudrais souligner aussi que nous ne sommes pas le gouvernement du Canada. Nous sommes le Parlement du Canada, et nous mélangeons souvent les deux. Nous interagissons avec les organismes gouvernementaux, en l'occurrence avec le SCT. Il faut donc que tous les protocoles qui seront mis en place soient dirigés vers les responsables de la Chambre des communes qui assurent notre sécurité. Le Comité devrait se concentrer sur cet aspect.

C'est extrêmement difficile d'élucider les tenants et aboutissants concernant entre autres le moment et la manière. J'espère que le Comité concentrera son énergie sur ces aspects plutôt que de dénoncer à tout vent le fait que tout le monde savait sauf nous.

M. James Bezan: Est-ce que je peux enchaîner avec un commentaire?

Je crois vraiment que la responsabilité liée à notre présence physique et à notre protection physique relève du Service de protection parlementaire sous la direction du sergent d'armes et de la GRC. Ces deux instances devraient aussi être responsables de notre protection contre les cyberattaques. Que les attaques soient physiques ou non, quelqu'un doit assumer le leadership. Le Service de protection parlementaire est le premier responsable de notre sécurité contre les cyberattaques, les hypertrucages, l'IA et toutes ces menaces qui vont en s'accroissant et qui planent de plus en plus sur les parlementaires.

Mme Sherry Romanado: Étant donné que notre rôle nous oblige à avoir des comptes de courriel personnels — pour nos activités partisanes et ainsi de suite —, recommanderiez-vous la mise en place de protocoles sur l'utilisation des comptes courriel personnels, vu que nous avons tous ce type de compte?

Le président: Il reste 10 secondes pour un témoin.

M. Garnett Genuis: Je ne pense pas que les services de sécurité de la Chambre des communes puissent nous suivre partout. Nous utilisons nos comptes personnels. Nous nous déplaçons physiquement ailleurs au pays. Les services de renseignement doivent prendre le relais dans une perspective globale. S'ils détiennent des informations sur une menace qui pourrait se manifester dans notre compte courriel personnel, dans notre circonscription ou lors de nos déplacements, ils doivent nous en informer parce qu'ils analysent le contexte de la sécurité bien au-delà de ce qui se passe au Parlement et dans nos appareils de fonction.

Le président: Merci beaucoup, madame Romanado.

● (1130)

[*Français*]

Madame Gaudreau, vous avez maintenant la parole pour six minutes.

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

Monsieur McKay, avez-vous su ce que le groupe APT 31 pouvait vous faire subir? Quelle en est la mécanique?

[*Traduction*]

L'hon. John McKay: On nous a dit que c'était une attaque de pixel. Je vais vous en lire une description parce que je ne suis pas certain de comprendre de quoi il s'agit:

> Les courriels que vous avez reçus provenaient du domaine « nropnews.com », auquel plusieurs adresses de courriel et noms de faux journalistes sont rattachés. Cette attaque de type reconnaissance par pixel consiste à introduire un pixel-espion dans une photographie ou une image. Lorsque le destinataire ouvre le courriel, le pixel-espion transmet alors certaines informations à l'expéditeur.

C'est une technique d'hameçonnage en quelque sorte.

[*Français*]

Mme Marie-Hélène Gaudreau: À quel moment avez-vous eu cette information?

[*Traduction*]

L'hon. John McKay: C'était à la fin du mois d'avril.

M. James Bezan: Sauf erreur, nous avons été informés de la situation le 24 avril par l'IPAC, qui nous a transmis les informations parce que nous sommes membres de l'organisme.

M. Garnett Genuis: Outre les aspects techniques, la description fournie par M. McKay dénote les premières phases d'une attaque fort probablement de grande envergure. Voilà le principal élément concret à retenir. C'est à ce stade que les pirates rassemblent des informations qu'ils pourront utiliser dans le cadre d'attaques subséquentes.

Nous avons reçu des informations de la part du FBI sur les techniques précises que nous pouvons utiliser pour nous protéger contre des attaques qui gagnent en ampleur. Voilà pourquoi il est primordial que nous soyons informés. C'est lorsque nous apprenons que nous sommes peut-être la cible des premiers stades d'une attaque de reconnaissance que nous pouvons mettre en place des mécanismes pour mieux nous protéger. Dans notre cas, nous n'avons pas pu le faire, puisque nous ne savions rien.

[*Français*]

Mme Marie-Hélène Gaudreau: Pour ma part, ce qui me renverse et me bouleverse, c'est qu'on étudie ça depuis des mois, on se questionne et on veut prévenir ça. Personnellement, je ne suis pas dans le service des renseignements, mais j'ai trouvé, sur le Web, le 15 décembre 2021, un document sur la campagne d'attaque du mode opératoire APT 31.

Honnêtement, je me serais attendu à ce que le Centre de la sécurité des télécommunications, ou CST, nous donne les détails et les techniques. Dans le journal *Le Monde*, on décrit comment le groupe APT 31 fonctionne. C'est pour ça que, pour moi, il est important de savoir quand vous l'avez su, mais, aussi, si les techniques étaient claires. Ça se trouve avec des recherches qu'on peut faire soi-même.

Le CST aurait pu corriger le tir. Êtes-vous satisfait du service rendu au moment où on se parle, dans l'urgence?

[*Traduction*]

L'hon. John McKay: Non.

M. James Bezan: Je dirais que nous ne serions pas ici si... Nous sommes tous très déçus.

Le CST est une excellente organisation. Elle est très respectée au sein du Groupe des cinq. Nous parlons de qui est l'ultime responsable. Le SPP est responsable de la protection parlementaire et a un rôle à jouer dans ce domaine. Le SCRS et le CST sont des agences tournées vers l'extérieur — nos agences du renseignement qui ont la capacité de faire face aux cyberattaques. Ce sont ces agences qui doivent s'assurer que les députés de la Chambre des communes sont au courant. Là encore, il faut communiquer des renseignements, les classer et veiller à ce que des mesures appropriées soient prises pour que nous puissions prendre des mesures correctives afin de nous protéger.

Nous sommes nos propres bureaux parlementaires indépendants. Par ailleurs, nous avons une faiblesse collective: nos courriels et nos communications en ligne.

[*Français*]

Mme Marie-Hélène Gaudreau: Ce que je comprends, c'est que vous êtes d'accord que nous utilisons la surclassification et que, dans notre culture de l'information, on se dit que ce n'est pas pour nous, mais que, finalement, le monde nous regarde. Aujourd'hui, avec tout le temps qu'on a mis, imaginez les nouvelles tactiques qui sont en place.

Êtes-vous prêts à réviser autant le privilège parlementaire que jusqu'où protéger notre vie privée au détriment de l'ingérence, justement? Qu'en pensez-vous? On veut tout réviser, mais, selon vous, faut-il vraiment faire une réforme et se questionner?

● (1135)

[*Traduction*]

Le président: Il vous reste environ 30 secondes.

L'hon. John McKay: Permettez-moi de dire ceci: vous avez ici trois membres du comité de la défense. Ils sont tous d'accord pour dire que nous surclassons tout. C'est un point de vue bien établi au comité de la défense.

Cela dit, oui, lorsque ces règles ont été rédigées, il était bien trop tard. Elles n'envisageaient pas ce genre de problème. Ce comité rendrait un excellent service en mettant à jour la manière dont nous traitons des choses telles que les attaques par hameçonnage.

M. Garnett Genuis: En seulement 10 secondes, je dirais que l'échange de renseignements est un moyen essentiel de lutter contre l'ingérence étrangère. Informer les gens de ces attaques est un élément important. Ce n'est pas le seul moyen et il ne fonctionne pas pour tout le monde, mais c'est un élément essentiel pour lutter contre ces menaces.

[*Français*]

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 de comparaître aujourd'hui. Il est intéressant de voir cette configuration différente, plutôt que de se réunir au comité.

Je veux revenir sur ce que vous avez dit, monsieur McKay, sur le quand, le si et le comment.

C'est difficile. Comme nous le savons tous, à la Chambre des communes, nos courriels sont plutôt semi-publics à ce stade. Des gens déchiffrent le code en permanence. Il y a des millions d'attaques chaque jour contre la Chambre des communes. Cette attaque particulière de MPA31, de menace persistante avancée, a été déjouée. Par conséquent, comme on nous l'a dit, vous n'avez pas été informé.

Comment, d'après vous, devrions-nous aller de l'avant dans ce cas, si et comment devrions-nous procéder, quand ces attaques sont si nombreuses? Comment voulez-vous que la Chambre des communes progresse face à une telle complexité et à un tel nombre?

L'hon. John McKay: Si j'avais une réponse à cette question, je l'enverrais par la poste. Je pourrais même vous faire payer.

C'est la question cruciale qui se pose à ce comité. Je ne suis pas tout à fait sûr de la façon de s'y prendre, car le volume est énorme. Le niveau de menace est variable. Le problème est que le niveau de menace n'est pas seulement variable du point de vue de la sécurité nationale, mais aussi du point de vue de chaque parlementaire. Ce que je peux percevoir comme une menace, M. Bezan ou M. Genuis peuvent le percevoir différemment.

J'aimerais pouvoir répondre à votre question.

Mme Lindsay Mathyssen: Cela dépendrait-il plutôt de la personne qui se livre à des activités d'hameçonnage?

L'hon. John McKay: Ce serait l'une des choses. Même si vous dites, « Eh bien, c'est une menace de la Chine », c'est un niveau de menace. Une menace de l'Iran est un autre niveau de menace. Un type dans son sous-sol à Moose Jaw est un autre niveau de menace — sans vouloir manquer de respect à Moose Jaw.

M. James Bezan: Je m'attends à ce que l'intelligence artificielle soit utilisée pour amplifier et accroître le nombre de cyberattaques auxquelles nous sommes tous confrontés. Je pense que l'aspect le plus important est ce qui se passe collectivement. Nous devons savoir quand les attaques sont très ciblées. La MPA31 était très ciblée sur les 18 d'entre nous.

Je pense que c'est à ce moment qu'il faut commencer à dire, d'accord, vous devez commencer à surveiller vos comptes personnels. Vous devez surveiller ce que vous faites sur vos iPhone et dans d'autres applications et comment vos mots de passe sont protégés. Vous savez, c'est ce genre d'éléments que vous commencez à communiquer avec les gens.

Si ce n'est qu'une attaque généralisée visant tous les P9, tous les A1, tout notre personnel individuel ou collectif, je pense que nous laissons le soin à notre personnel des TI et au CST de la contrecarrer. Lorsque des gens nous ciblent en tant qu'individus ou qu'ils s'en prennent à ceux d'entre nous qui siègent au comité de la défense nationale, nous devrions le savoir.

M. Garnett Genuis: Je peux ajouter des commentaires.

Je ne pense pas qu'il soit compliqué, au niveau des principes, de dire que s'il y a des tentatives générales d'hameçonnage qui ciblent tous les comptes, qui arrivent régulièrement et qui sont plus ou moins sophistiquées, alors il s'agit d'une catégorie différente de celle où vous, madame Mathyssen, seriez ciblée par un État étranger parce qu'il n'a pas aimé une motion que vous avez présentée à la Chambre ou à un comité. Je pense que dans un tel cas, vous voudriez savoir que vous êtes la cible d'un acteur particulier pour quelque chose que vous avez fait. Cette situation pourrait vous obliger à prendre des mesures supplémentaires pour vous protéger, différentes de celles exigées des autres députés.

Je pense que cela devrait clairement lancer une conversation entre les agences de sécurité et vous, ce qui est un peu différent de ce qui se fait généralement avec tous les députés.

● (1140)

Mme Lindsay Mathyssen: Plus tard dans cette législature, ce comité étudiera la mesure législative sur la « nécessité de savoir » qui a été proposée par M. Ruff, le projet de loi C-377. Nous avons eu de nombreuses conversations à ce sujet à notre comité de la défense, notamment en ce qui concerne le niveau d'habilitation de sécurité que certains députés pourraient ou devraient avoir. Dans quelle mesure est-ce important, d'après vous?

Dans le cadre de cette conversation, comment les députés s'y prennent-ils pour savoir ce qu'ils savent et ce à quoi ils ont accès dans ce contexte de menace accrue?

Le président: Il reste environ une minute, chers témoins.

M. James Bezan: J'appuie sans réserve le projet de loi de M. Ruff. Je pense que c'est la bonne façon de procéder pour nous fournir des classifications — qu'elles soient secrètes, très secrètes ou plus élevées, en nous fondant sur les règles que nous avons. Nous devons absolument passer par les habilitations de sécurité requises et les vérifications des antécédents. Je ne m'attends pas à ce que ce soit généralisé et que, dès que vous êtes élu, vous obtenez une habilitation de niveau très secret. Je pense qu'il y a une procédure appropriée.

Je pense que c'est même un peu plus différent. Je suis d'accord avec M. Genuis pour dire qu'à mesure que nous en savons plus sur l'ingérence étrangère et sur les cyberattaques dont nous sommes victimes sur la Colline, nous pouvons communiquer ces renseignements au public. Nous pouvons rétablir la confiance dans nos institutions démocratiques.

L'une des façons de traiter cette question de manière plus générale est que le Parlement publie un rapport annuel sur les cyberattaques auxquelles nous sommes confrontés et sur la manière dont nous avons pu y faire face. Je pense que c'est une façon de rendre des comptes et de mieux comprendre l'évolution de la menace de cybersécurité à laquelle nous sommes confrontés.

Le président: Je vous remercie, madame Mathyssen.

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

M. Michael Cooper: Je vous remercie, monsieur le président.

Mesdames et messieurs les députés, acceptez-vous l'affirmation du gouvernement selon laquelle il incombe à l'Administration de la Chambre des communes et, en fait, aux services de TI de la Chambre des communes d'informer les députés d'une cyberattaque de cette nature?

M. Garnett Genuis: Je vais commencer, monsieur le président.

Non, je ne l'approuve pas. J'ai présenté, je crois, cinq points distincts dans ma déclaration liminaire pour expliquer pourquoi je ne suis pas d'accord. C'était, dans mon cas, un témoignage personnel. Il y a des lacunes dans ce que nous savons de ce qui a été dit à la Chambre. Le gouvernement ne comprend pas la nature et les attentes des professionnels de la TI, la possibilité d'émettre des réserves et le fait que les députés ne sont pas des créatures de la Chambre. Nous avons nos propres droits.

Monsieur Cooper, pour faire suite à vos remarques précédentes, nous pouvons parler d'échec systémique, de systèmes qui ne font pas ce que nous attendons d'eux. Ensuite, nous pouvons parler de la responsabilité individuelle, des personnes qui ne font pas le choix de s'assurer que les renseignements arrivent à destination.

Je pense qu'il est important de parler des systèmes, mais nous ne pouvons pas non plus passer à côté de la reddition de comptes que vous avez soulignée, à savoir que les gens avaient ces renseignements et ont fait le choix de ne pas prendre les mesures nécessaires pour les transmettre à ceux qui étaient ciblés. Je ne pense pas que nous devrions utiliser une discussion sur les systèmes pour détourner l'attention du fait que les gens dans ces systèmes ont fait des choix, et que ces choix ont amené les députés à être plus vulnérables aux menaces étrangères.

L'hon. John McKay: Je ne suis pas aussi enthousiaste à l'idée de blâmer le gouvernement pour tout. Je pense qu'il s'agit plutôt d'un échec des protocoles. Apparemment, lorsque le FBI a communiqué les renseignements aux divers gouvernements, certains d'entre eux avaient exactement le même protocole que le Canada. D'autres gouvernements avaient des protocoles beaucoup plus détaillés. J'ai tendance à penser qu'à ce stade, deux ans plus tard, ces protocoles doivent être changés.

Je ne veux pas prendre tout le temps. Vous voulez que M. Bezan intervienne.

● (1145)

M. Michael Cooper: Oui.

M. James Bezan: Je n'adhère pas à cet argument. Ce n'est pas seulement le protocole. C'est une culture. Ça commence tout en haut. Ça commence dans le Cabinet du premier ministre. Ces renseignements doivent être communiqués. La façon dont ils classifient ces renseignements, la façon dont ils sont transmis, que ce soit par le CST, le SCRS, la GRC ou le Service de protection parlementaire ou le Président de la Chambre, et la façon dont ils communiquent ces renseignements, tout commence par un oui ou un non du Cabinet du premier ministre.

M. Michael Cooper: Je pense que je vais m'opposer un peu à ce que M. McKay a dit au sujet de la directive ministérielle qui a été émise en mai 2023, à la suite de la dernière question de privilège concernant M. Chong. À la suite de cette directive ministérielle, une nouvelle séance d'information sur la cyberattaque de MPA31 a été organisée à l'intention des clients concernés du gouvernement du Canada. Là encore, aucun député n'a été informé.

Cela vous donne-t-il confiance dans la directive ministérielle et dans l'approche de ce gouvernement pour informer les députés?

L'hon. John McKay: Permettez-moi de réagir à l'opposition et de dire que les directives ministérielles sont utiles mais tardives. Sont-elles correctement mises en œuvre? Je ne le sais pas. J'aurais espéré qu'une fois la directive ministérielle publiée en 2023, ils auraient pu revoir leurs décisions antérieures, particulièrement en ce qui nous concerne, et nous conseiller, même si nous avons été informés tardivement.

J'espère que ce comité fera savoir qu'il faut changer non seulement la culture, mais aussi le système et la rapidité de la mise en œuvre du changement.

M. Garnett Genuis: M. McKay semblait approuver plutôt que de désapprouver.

L'hon. John McKay: J'aimerais penser que nous pouvons passer un peu plus de temps à trouver des solutions et à analyser le problème au lieu de perdre notre temps à blâmer ceux qui auraient dû l'être. Je suis tout à fait disposé à accepter que c'était une erreur. Nous aurions dû être nommés.

M. James Bezan: Il y a en fait un schéma ici. On en revient au conseiller à la sécurité nationale et au renseignement...

Le président: Monsieur Bezan, je vais vous laisser répondre. Je vous laisse un peu de marge de manœuvre si vous voulez répondre.

M. James Bezan: Je dirais simplement qu'il y a des raisons de blâmer, non seulement au Cabinet du premier ministre mais aussi au Bureau du Conseil privé avec le conseiller à la sécurité nationale et au renseignement. Ce que nous avons vu au Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR, avec la non-communication des renseignements, ce que nous avons vu dans les rapports, ce que nous avons vu dans l'affaire de M. Chong, les témoignages dans le cadre de l'enquête Hogue — tout indique que le CSNR n'a pas communiqué ces renseignements ou qu'il dit qu'ils ne sont pas importants, en particulier lorsqu'il s'agit de parlementaires.

La position de la culture est que nous n'avons pas besoin de savoir. Mais vous savez quoi? Nous avons besoin de savoir.

Le président: Je vous remercie.

L'hon. John McKay: Je ne sais pas si nous sommes vraiment en désaccord.

Le président: Monsieur McKay, je suis désolé. J'ai fait preuve d'un peu de souplesse ici.

Monsieur Duguid, vous disposez de cinq minutes.

M. Terry Duguid (Winnipeg-Sud, Lib.): Merci, monsieur le président.

Je veux remercier mes collègues de comparaître aujourd'hui.

Monsieur le président, je ne suis pas un ancien membre de ce comité. Je pense que j'y siège depuis le début de la session en octobre. Pendant environ les deux tiers du temps, nous nous sommes concentrés sur des motions de privilège relatives à l'ingérence étrangère. Il y a des thèmes très communs. Il y a le manque de coordination, le manque de communication et, bien entendu, le fait que les députés ne sont pas informés, ce qui, je pense que nous sommes tous d'accord, est totalement inacceptable.

L'autre observation que j'ai faite est que cette question est devenue très partisane. J'ai été frappé par l'une des déclarations de M. McKay, le plus ancien député autour de cette table, qui a servi avec distinction pendant de nombreuses années — je ne vous fais pas d'éloges, ne vous inquiétez pas —, à savoir que nous devons vraiment aller au-delà de la partisanerie sur cette question particulière. Il est question de notre pays. Il est question de la sécurité des députés.

Monsieur McKay, vous avez peut-être entendu le président du CPSNR, qui a accordé un certain nombre d'entrevues hier, lorsqu'il a abordé ce même thème. Il s'agit de la sécurité de notre pays, de la sécurité de nos décideurs. Cela dépasse le cadre d'un député ou d'un parti. Il a suggéré que les dirigeants des principaux partis de notre Parlement se réunissent dans une salle. Ils doivent travailler ensemble. Ils doivent mettre fin à la partisanerie. Comme nous en avons parlé aujourd'hui, ils doivent trouver des solutions et des protocoles, en tirant évidemment parti de l'enquête Hogue.

Je me demande simplement ce que vous en pensez. J'aimerais aussi entendre les réflexions de mes autres collègues.

● (1150)

L'hon. John McKay: Loin de moi l'idée d'être en désaccord avec M. McGuinty sur quoi que ce soit. Je pense qu'il soulève un point valable. Je voudrais toutefois ajouter quelque chose.

Ne vous contentez pas de vous en remettre aux dirigeants. Nous sommes apparemment tous des adultes ici. Nous devons veiller à notre sécurité. Je serais très contrarié si les dirigeants ne prenaient pas les choses au sérieux, mais je le serais encore plus si nous ne les prenions pas au sérieux. Il s'agit d'un comité sérieux.

Mme Mathyssen a posé une question très difficile. Je pense que M. Bezan a commencé à ventiler la réponse à cette question un peu mieux que M. Genuis ou moi-même, et c'est le travail difficile qui doit être fait ici parce que ces situations vont continuer de se produire.

Honnêtement, je ne sais pas où les protocoles doivent être élaborés. J'ose dire qu'il faut les écrire au crayon ou avec quelque chose qui disparaît, parce qu'ils vont changer environ une semaine après qu'on les a mis en place. Nous devons prendre nos responsabilités, et M. McGuinty a tout à fait raison. Nous devons prendre nos responsabilités.

M. James Bezan: Monsieur le président, je voudrais juste ajouter quelque chose. Pour répondre à la remarque de M. Duguid, il y a certainement des choses dont on peut parler au niveau du caucus, que ce soit par l'entremise des chefs de parti, des leaders parlementaires ou des whips, en ce qui concerne l'action collective, mais il y a toujours le privilège individuel et la façon dont nous l'équilibrons. Au final, tout dépend de la manière dont nous communiquons les renseignements et de la classification de ces renseignements.

En ce qui concerne les cyberattaques, nous ne parlons pas de renseignement ni de la manière dont les renseignements sont colligés. Nous parlons en fait d'une cyberattaque cinétique qui a été documentée et qui est connue. Une partie de ces renseignements ont peut-être été communiqués par l'entremise de partenaires du Groupe des cinq, mais ces partenaires — ou d'autres alliés de l'OTAN — ont souvent pris des mesures beaucoup plus rapidement que nous.

Pour l'attaque MPA31, plus particulièrement, la Suède en a eu connaissance immédiatement et l'a communiquée à ceux qui étaient visés presque immédiatement, et il y a un autre pays européen qui a communiqué cette information très rapidement.

Je pense que c'est un point essentiel. Nous ne devons pas nous reposer sur nos lauriers et regarder ce que les autres pays font. Nous devons agir énergiquement et nous assurer que ce que nous faisons est proactif et que chacun d'entre nous est mieux préparé et protégé.

M. Garnett Genuis: Monsieur Duguid, pour répondre brièvement à ce que vous avez dit, je suis d'accord sur l'importance de trouver des solutions.

Avec tout le respect que je vous dois, j'ai cependant parfois remarqué que les appels à réduire la partisanerie sont lancés dès qu'il y a un échec important de la part du gouvernement. Le gouvernement ne parvient pas à faire quelque chose qu'il aurait dû faire, et alors il dit, « Eh bien, réduisons la partisanerie; soyez gentils avec nous ». Il faut trouver des solutions, mais il faut aussi rendre des comptes sur les choix qui ont été faits.

Le président: Merci beaucoup, monsieur Duguid.

[*Français*]

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

Mme Marie-Hélène Gaudreau: Monsieur le président, je vais rebondir sur les propos de mon collègue.

De manière préventive, puisque les Ouïghours et Taïwan, c'est connu, avez-vous été contactés pour être vigilants? Est-ce qu'on a ça ici? Avez-vous eu ça?

[*Traduction*]

L'hon. John McKay: On n'a pas communiqué avec moi.

M. James Bezan: Non, je suis prudent par défaut. Au pays, cependant, je pense que nous sommes un peu moins sur nos gardes. Quand nous sommes au Canada, nous pensons qu'il n'y a pas de risques. Certains de mes téléphones jetables ont été piratés lorsque j'étais en Ukraine. Nous appliquons des protocoles supplémentaires lorsque nous nous rendons en Europe.

Mme Mathyssen, M. McKay et moi sommes allés en Estonie l'été dernier. Nous avions tous des téléphones jetables. Nous avons laissé nos autres téléphones, nos iPad et tous les autres appareils à la maison. Lorsque nous nous sommes approchés de la frontière russe à Narva, j'ai même éteint mon téléphone et je l'ai placé dans mon sac de sécurité. Je l'ai mis en mode avion avant de l'éteindre. Des gardes-frontières russes nous ont filmés pendant tout le temps où nous étions à la frontière. Puis, de retour à bord de l'autobus, à une bonne trentaine de kilomètres de la frontière, j'ai ouvert le sac, et mon téléphone était allumé. Il n'était plus en mode avion, et il avait été piraté.

Ce genre d'attaques se produit. Je pense que nous vivons tous des histoires de ce genre lorsque nous voyageons. Cela m'est déjà arrivé lorsque j'étais secrétaire parlementaire de la Défense, à l'époque, sur un bon vieux BlackBerry, mais c'est différent. Ces attaques surviennent ici même, chez nous, alors il faut être encore plus prudent.

● (1155)

L'hon. John McKay: J'ai vécu une expérience semblable en Ukraine, où nous avons tout simplement tout éteint. C'est à peu près la seule mesure qu'on puisse prendre.

[*Français*]

Mme Marie-Hélène Gaudreau: Il me reste quelques secondes.

Est-ce que vous croyez que nous sommes suffisamment équipés, techniquement, bien qu'on ait des modèles du Groupe des cinq? On a entendu parler de l'Australie et on est un peu gêné du fait que, depuis 1984, on n'a pas fait les changements nécessaires. Croyez-vous qu'on est bien équipé, au Canada?

[*Traduction*]

Le président: Je vais laisser un témoin répondre rapidement, je vous prie.

L'hon. John McKay: C'est une question très difficile qui n'est peut-être pas tout à fait pertinente à cette conversation.

Si je regarde la situation dans son ensemble, je pense que le Canada est un pays très avancé en ce qui concerne sa participation au Groupe des cinq et à divers autres enjeux cybernétiques. Sur cette question, nous ne le sommes peut-être pas autant.

[*Français*]

Le président: Merci, madame Gaudreau.

[*Traduction*]

Madame Mathyssen, nous vous écoutons pendant deux minutes et demie.

Mme Lindsay Mathyssen: Je veux reprendre là où nous nous sommes arrêtés dans la conversation sur l'autorisation de sécurité que nous devrions tous recevoir. Monsieur Genuis, je pense que vous avez dit que nous pourrions parler des systèmes et des échecs, mais qu'il y a une responsabilité personnelle et que les gens qui font ces choix exposent les autres députés à un plus grand risque.

Je suis préoccupée, bien sûr, par le contexte plus large, par le nuage qui plane maintenant au-dessus du Parlement. Beaucoup de parlementaires l'ont dit à la suite du rapport du Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR. Je m'inquiète de la façon dont nous mettons en place ces processus et ces systèmes afin de faire face à ce nuage plus vaste qui nous préoccupe puisqu'il mine notre privilège.

Comme vous l'avez aussi dit, la mentalité commence au sommet. Comment appliquer ce principe à votre propre chef qui refuse de recevoir une séance d'information qui lui permettrait éventuellement de faire partie de la solution?

M. Garnett Genuis: Je suis heureux de répondre à cette question. La nature des exigences associées à cette séance d'information fait en sorte qu'il ne pourrait aucunement utiliser cette information pour faire quoi que ce soit. Si une personne est informée et qu'elle est tenue, à la suite de cette séance d'information, de ne rien dire à personne, de ne prendre aucune mesure à l'égard de l'information, quelles actions pourraient être entreprises?

Nous avons une loi qui s'applique à tous les partis, même si je ne suis pas certain qu'elle est utilisée. La Loi instituant des réformes exige que chaque caucus tienne un vote au début de la législature sur un mécanisme par lequel les membres du caucus pourraient participer à la décision concernant la composition du caucus. Supposons qu'un chef de parti se rende compte qu'il y a un problème. Il ne pourrait pas soulever cette question auprès de son caucus. Il ne pourrait pas porter cette question à l'attention du directeur de la campagne nationale. Il ne pourrait en parler à personne.

Ce dont nous avons besoin, c'est d'un processus de reddition de comptes, et non d'une séance d'information secrète à la condition qu'on ne puisse rien faire avec l'information. Ce n'est pas efficace.

Mme Lindsay Mathyssen: Il est intéressant que vous ayez mentionné la Loi instituant des réformes...

Le président: Il vous reste environ 30 secondes.

Mme Lindsay Mathyssen: L'un des anciens directeurs des communications de Stephen Harper, Kory Teneycke, a dit que le fait d'utiliser la Loi instituant des réformes comme excuse est une « idée fausse. » Il a dit que la séance d'information était « une occasion de faire preuve de leadership, et [qu'il pensait] qu'ils devraient l'accueillir favorablement. »

M. Garnett Genuis: Je pense que M. Teneycke a tout à fait tort à ce sujet. Bien sûr, il peut décrire sa propre compréhension de la Loi instituant des réformes.

La Loi instituant des réformes est très claire quant à la façon dont les caucus prennent des décisions, et je dirais seulement que j'aurais aimé que le Parti libéral se conforme à la Loi et tienne ces votes au début de la législature, parce qu'il faut s'inquiéter si cette loi n'est pas respectée.

Le président: Merci beaucoup, madame Mathyssen.

Chers collègues, cela met fin à notre discussion avec le premier groupe de témoins. Je tiens à remercier M. McKay, M. Genuis et M. Bezan de s'être joints à nous aujourd'hui.

Nous vous remercions de votre temps, messieurs.

L'hon. John McKay: Merci.

Le président: Nous allons suspendre brièvement la séance pour nous préparer à accueillir le deuxième groupe de témoins, et nous reprendrons immédiatement.

● (1155)

_____(Pause)_____

● (1200)

Le président: Chers collègues, nous allons reprendre nos travaux.

Nous allons passer au deuxième groupe de témoins sur le même sujet.

Nous souhaitons la bienvenue aux députés suivants, nos collègues qui se joindront à nous pour le deuxième groupe de témoins d'aujourd'hui. Nous accueillons M. Kmiec, député de Calgary Shepard, Mme Stephanie Kusie, députée de Calgary Midnapore, et l'honorable Judy Sgro, députée de Humber River—Black Creek.

Chers collègues, vous disposerez chacun de cinq minutes pour votre déclaration préliminaire, puis nous passerons à une série de questions comme à n'importe quel autre comité.

Chers témoins, avez-vous déterminé qui pourrait commencer, ou est-ce qu'un d'entre vous veut simplement lever la main?

Mme Stephanie Kusie (Calgary Midnapore, PCC): Nous allons suivre l'ordre de l'avis de convocation, c'est certain. C'est ainsi que nous devrions procéder. Nous devrions suivre l'ordre de l'avis de convocation.

Le président: Nous pouvons nous y prendre de différentes façons.

Mme Stephanie Kusie: Je pense qu'il est toujours bon de suivre l'avis de convocation.

Le président: Monsieur Kmiec, allez-y.

Mme Stephanie Kusie: C'est bien.

M. Tom Kmiec (Calgary Shepard, PCC): Merci, monsieur le président.

J'essayais d'être un gentleman.

J'ai eu l'occasion d'écouter les témoignages du premier groupe de témoins de ce matin. Je n'ai pas remis de notes d'allocution aux interprètes, alors je vais parler lentement et je ferai une pause lorsque je passerai au français.

Je vais répéter ce que j'ai dit à la Chambre des communes. Je crois que le gouvernement du Canada avait la responsabilité morale et éthique de dire aux 18 parlementaires que nous étions ciblés par une unité spéciale de la République populaire de Chine, ou RPC, pour une forme de surveillance numérique, moi y compris. Je suis l'un d'eux. Je suis membre de l'Inter-Parliamentary Alliance on China, ou IPAC. Le gouvernement du Canada a manqué à sa responsabilité morale et éthique de nous avertir.

J'ai six points à faire valoir à la lumière des témoignages que j'ai entendus. Je veux en parler.

Le premier concerne le témoignage des représentants du Centre de la sécurité des télécommunications, ou CST, sur le moment où ils ont été mis au courant. Ils ont dit:

> [...] 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 lumière de ce témoignage, je dois supposer qu'il s'agissait d'APT31. Je ne savais pas du tout que des menaces planaient à ce moment-là. Je ne savais pas non plus ce qu'était APT31 jusqu'à ce que j'apprenne le 24 avril — par mes deux coprésidents et le directeur général de l'IPAC — que j'avais été l'une des cibles de cette campagne de la RPC.

Depuis, je n'ai eu aucun contact direct avec le CST ou le SCRS. J'ai toutefois reçu des communications du FBI. Le 9 mai, j'ai assisté à la même séance d'information du FBI que d'autres députés, pendant laquelle on nous a expliqué exactement ce qu'est APT31.

Plus tard, dans son témoignage devant le Comité, Caroline Xavier, du CST, a dit: « Je peux confirmer que, lorsque nous avons pris connaissance en 2021 de certaines anomalies » — il est intéressant qu'elle emploie le mot « 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. »

Elle a poursuivi en donnant des détails à ce sujet:

> [...] 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.

Lorsque j'ai appris que j'avais été ciblé, on m'a répondu par une citation le 25 avril. La voici, tel qu'elle a été copiée-collée par le sergent d'armes: « Pour vos dossiers, nous avons enquêté sur cette activité pendant qu'elle était en cours, bien avant qu'elle ne soit rendue publique. »

Mon personnel a fait un suivi et a posé la question suivante: « Dites-vous que le Bureau du sergent d'armes était au courant de cette activité et qu'il a fait enquête auparavant, ou faites-vous référence à l'Administration des TI de la Chambre? »

Le Bureau du sergent d'armes n'était pas au courant de cette enquête. Cependant, l'équipe de cybersécurité de la Chambre des communes, le service d'information et l'Administration des TI ont déclaré qu'ils ont participé à l'enquête pendant qu'elle était en cours.

J'aimerais attirer votre attention sur une autre réponse à une question de M. Genuis. Mme Caroline Xavier a répondu que, dans le cadre de ces mesures, « [son équipe a] fourni 12 rapports à la Chambre des communes. » La période a commencé en janvier 2021. Encore une fois, je ne sais pas ce que contenaient ces rapports. Je n'ai pas l'avantage d'avoir assisté aux séances à huis clos dont les membres de ce comité ont bénéficié, alors je suis désavantagé.

● (1205)

[*Français*]

En réponse à une question posée par Mme Marie-Hélène Gaudreau, Mme Xavier a dit:

> 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.

Il est impossible de contacter le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications si on ne sait pas qu'il existe. C'est la première fois que je me rends compte qu'un tel service pour les parlementaires existe. Je suis élu depuis 2015 et c'est la première fois que j'entends parler de ce service, qui existe depuis 2019.

De plus, il est impossible de demander l'aide du Centre canadien pour la cybersécurité du gouvernement si on ne sait pas qu'on est visé par une agence étrangère en tant que parlementaire.

[*Traduction*]

Lors du contre-interrogatoire et dans la foulée des questions de Mme Mathyssen, M. Genuis a souligné que le CST a fait l'observation suivante lors de différentes séries de questions: les institutions gouvernementales doivent respecter les parlementaires de la Chambre des communes. Cependant, il est difficile de se sentir respecté par le SCRS, le CST ou l'Administration de la cybersécurité des TI de la Chambre des communes lorsqu'ils ne se donnent pas la peine de nous dire que nous sommes la cible de campagnes et d'organisations étrangères.

Je travaille beaucoup avec les communautés de la diaspora au Canada. Il y a souvent des gens qui me disent qu'ils ne peuvent pas être vus en ma compagnie dans une photo qui sera publiée en ligne, alors ils se retirent de la photo.

Dans mon bureau, j'ai également un drapeau ukrainien signé par bon nombre de nos stagiaires du Congrès des Ukrainiens Canadiens au cours des dernières années, et je suis certain que les représentants de la Fédération de Russie n'en sont pas ravis.

Enfin, j'ai des photos de manifestations à Hong Kong que des Albertains qui étaient sur les lieux m'ont apportées. Les Hongkongais qui viennent me rendre visite ne prennent pas de photos de ces images où je serais vu.

Merci, monsieur le président.

● (1210)

Le président: Merci beaucoup, monsieur Kmiec.

Madame Kusie, vous avez cinq minutes.

Mme Stephanie Kusie: Bonjour, chers collègues.

Dans la matinée du jeudi 25 avril de cette année, j'ai reçu un message urgent de mon collègue demandant un appel le plus rapidement possible. Je n'étais pas la seule destinataire, alors l'appel était prévu pour plus tard en après-midi. Les détails, une fois partagés, étaient troublants. Les participants à l'appel avaient été la cible d'une cyberattaque d'APT31, un groupe de pirates mis sur pied par la RPC.

Cette nouvelle est pour le moins troublante. On pense immédiatement à ses transactions les plus intimes. Il est impossible de ne pas le faire. On se met rapidement à repasser toutes nos communications dans notre esprit.

Ce n'est un secret pour personne que nos communications électroniques renferment les détails les plus précieux de nos vies: où nous sommes, avec qui nous nous trouvons et ce que nous faisons. On implore alors assez rapidement Jésus dans ces moments, puis on ressent peu après un ressentiment accablant et on se demande: « Comment cela a-t-il pu se produire, et pourquoi? »

En tant que députée ou ancienne diplomate canadienne, je n'ai jamais tenu mes postes pour acquis. Par le passé, j'ai consigné en détail, auprès des autorités, les relations où j'ai remis en question la motivation de ceux qui tissaient des liens avec moi. Mes soupçons s'éveillaient toujours lorsqu'on m'offrait des cadeaux somptueux, ou lorsque je remarquais un passé suspect et des efforts forcés pour créer une proximité.

En 2021, après avoir changé de résidence, j'ai demandé qu'on inspecte mes maisons pour y détecter des microphones cachés. Les autorités m'ont informée que ces services n'étaient pas offerts au personnel à l'extérieur de l'exécutif du gouvernement. J'ai fait faire une évaluation de sécurité de ma demeure et j'ai fait installer le système de sécurité recommandé, en réponse à la remarque d'un collègue qui a dit qu'on pourrait voir qui m'a tuée après ma mort.

Est-ce que je souhaite la protection que certains de mes collègues ont en tout temps? Je suis très nerveuse à l'idée d'atteindre ce niveau de notoriété. Oui, il arrive qu'on me reconnaisse dans l'allée des vitamines et dans la section des charcuteries, mais on parle ici d'un autre niveau de notoriété.

L'aspect le plus troublant de cette affaire est d'avoir été informée non pas par une personne près de moi, mais par quelqu'un de plus éloigné. Je suis donc très reconnaissante d'avoir croisé Luke de Pulford lors de l'investiture du président taïwanais à Taïwan et de l'avoir remercié personnellement de ses renseignements et de nous en avoir fait part.

Malgré nos différences, j'ai toujours aimé les États-Unis, puisque j'y ai fait ma maîtrise et que j'ai été consule du Canada à Dallas de 2010 à 2013. Je ne suis pas surprise que ce soit en fait le Bureau fédéral d'investigation qui ait présumé cette atteinte et qui en ait informé l'IPAC, qui en a ensuite informé mon collègue, qui m'en a informée.

Cela ne change toutefois rien à la déception généralisée et persistante que j'éprouve à ne pas avoir été informée directement par le gouvernement canadien. En tant que consule, je me sentais responsable de tous les Canadiens dans ma région d'accueil. J'aurais voulu que les autorités canadiennes aient le même sentiment en m'informant de mes transgresseurs. Je peux seulement déduire qu'elles ne partageaient pas ce sentiment.

Ma déception est atterrante. J'essaie de me défaire de la peur qui m'habite lorsque je pense aux effets possibles sur ma famille et moi, comme on voudrait se débarrasser d'une dent que le dentiste dit devoir arracher à une date ultérieure. En tant que législatrice, je réfléchis à ce qui doit être fait pour me protéger et protéger ceux qui m'entourent, ainsi que mes collègues. Nous empruntons cette voie en sachant qu'une partie de notre vie ne nous appartient pas, mais ce genre de situation valide notre choix d'une manière beaucoup plus vaste que nous ne voudrions l'envisager.

En conclusion, je crois au mal, et pas seulement au sens biblique. Je crois à la malveillance dans le cœur des hommes — ceux qui veulent intentionnellement faire du mal à autrui. Il suffit de penser à Alexeï Navalny et aux 37 meurtres qui ont assombri les plus récentes élections mexicaines. Je ne parle pas de commentaires en ligne disant que je suis attirante ou non — je ne suis pas aussi sensible —, mais bien du potentiel qu'on nous fasse réellement du mal, à mes proches ou moi.

Cette attaque semble, en surface, avoir eu des répercussions minimes, mais elle témoigne d'une inquiétude beaucoup plus grave: quelqu'un me surveille. Les pirates veulent savoir ce que je fais, qui je rencontre et où je me rendrai.

Le mal, lorsqu'il est confronté, essaie toujours de se réaligner, mais les tactiques ne changent pas: diviser, conquérir, intimider et extorquer. Ces microactes d'agression sont à l'origine de la collecte de renseignements. La réalité, c'est que ce que vous ne savez pas peut vous nuire.

Merci beaucoup.

Le président: Merci beaucoup.

Madame Sgro, à vous la parole pour les cinq prochaines minutes.

● (1215)

L'hon. Judy A. Sgro (Humber River—Black Creek, Lib.): Je vous remercie, mais je n'aurai pas besoin de cinq minutes.

Merci beaucoup d'avoir organisé cette étude. Je vous suis reconnaissant de l'avoir réalisée, car c'est la première fois que je parle de cette question à quelqu'un. Nous en sommes rendus à deux mois plus tard, et c'est certainement inacceptable.

Pour revenir en arrière, oui, j'étais furieuse. J'étais livide lorsque j'ai reçu l'appel de l'IAPC. Nous avons eu une conversation commune, comme mes collègues l'ont déjà indiqué. La colère est partie, mais j'ai été très déçue, comme l'ont dit mes collègues. Ce n'est pas ce à quoi je m'attendais. Plus important encore, vous savez, c'est arrivé. Le pare-feu a tenu et, pour cette raison, ils ont estimé qu'il n'y avait aucune raison de nous le dire. Eh bien, je tiens à être mise au courant.

Tous les membres de ce groupe travaillent sur les droits de l'homme et nous abordons des sujets brûlants à la Chambre des communes et en dehors de celle-ci. Je pense que l'intention d'une grande partie de ce débat est d'intimider chacun d'entre nous afin que nous arrêtions de défendre les personnes qui n'ont pas de voix. Je pense qu'une part importante de notre travail consiste non seulement à représenter nos électeurs locaux, mais aussi à être la voix de ceux qui n'ont pas de voix. C'est grâce aux députés que certains des progrès que nous constatons dans différents dossiers se produisent, qu'il s'agisse du dossier du Tibet, de celui de l'Iran ou de celui de Taïwan, bien sûr. C'est parce que les députés ont eu le courage de se lever et de se faire entendre.

Oui, ils ont fait cela et nous n'en avons pas été informés, alors passons à autre chose. Qu'avons-nous appris de cette situation? Je crois que j'essaie toujours de trouver ce qu'il y a de bon dans une situation négative. Ma colère a disparu, mais ma déception est toujours là. J'espère que nous allons utiliser cette situation comme une occasion de mieux définir nos priorités et notre stratégie. J'espère que nous serons tous beaucoup plus conscients de la menace qui pèse sur nous et que nous prendrons davantage de responsabilités pour nous assurer que nous protégeons nos systèmes. On m'a dit que le fait d'éteindre les ordinateurs une fois par semaine contribuait à éliminer les virus ou les tentatives d'accès. C'est très simple. Personne ne me l'a jamais dit depuis que je suis ici. Toutefois, nous devons prendre la situation au sérieux. Nous devons, avec votre aide, mettre en place un plan.

Je veux dire que je ne savais même pas à qui demander s'il y avait d'autres dommages qui auraient pu être... Je n'en avais aucune idée après toutes ces années passées ici. Je sais que le sergent d'armes est là, mais je ne savais pas où aller, à qui demander ou comment mieux me protéger. Je pense que ce sont des choses sur lesquelles nous sommes tous, ou nous avons été, jusqu'à présent, extrêmement naïfs, mais d'après une conversation récente avec le CSIS et d'autres agences... Je sais que certains logiciels d'IA qui peuvent clairement reproduire mon comportement lors d'une réunion d'une demi-heure à laquelle je ne suis pas présent.

Je pense que nous sommes beaucoup plus menacés aujourd'hui que nous ne l'avons jamais été auparavant, et nous devons trouver un moyen de le faire. Comment allons-nous nous protéger les uns les autres? Quel est le rôle de chacun et qui met en place quoi? Cela doit être plus public. Je pense que le Comité de liaison devrait également rendre compte une fois par an au minimum, en même temps que tous les autres rapports, du nombre de problèmes de cybersécurité et de ce genre de questions. Nous devons être mieux informés, et c'est à vous qu'il incombe de formuler des recommandations.

Je pense qu'il faut mettre beaucoup plus l'accent sur le respect des parlementaires, comme l'a mentionné mon collègue. Penser que nous sommes dispensables et que, par conséquent, ils ne prendront pas la peine de nous dire que quelque chose nous a attaqués sur les médias sociaux, que si nous ne le savons pas nous-mêmes, ils ne vont pas nous le dire... Eh bien, leur travail consiste à s'assurer que nous sommes protégés. Lorsque nous parlons d'inciter davantage de personnes à se présenter à des fonctions publiques, s'ils le font, nous avons au moins la responsabilité de veiller à ce qu'ils disposent de tous les outils nécessaires pour être protégés afin qu'ils puissent faire le travail que nous voulons tous faire ici.

Je vous remercie.

Le président: Je vous remercie, madame Sgro.

Chers collègues, nous allons à présent entamer notre première série de questions.

Monsieur Duncan, à vous la parole pour les six prochaines minutes.

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

Je remercie nos témoins de leur participation.

Je m'appuierai sur ce que vous avez dit dans vos introductions et sur la première heure avec nos autres collègues qui étaient présents. Je vais peut-être poser quelques jalons.

Après avoir pris connaissance de la menace et des ratés en matière de notification, est-ce que l'un d'entre vous a eu des conversations ou des échanges avec le BCP, le cabinet du premier ministre, le ministre de la Sécurité publique ou son ministère au sujet de ce qui s'est passé exactement? Vous ont-ils demandé votre avis ou vos suggestions sur la manière d'éviter cette situation à l'avenir?

Je vous demanderai de répondre si vous avez été en contact avec l'un des groupes ou services susmentionnés.

● (1220)

L'hon. Judy A. Sgro: Non, cela n'a jamais été le cas.

Mme Stephanie Kusie: Je ne l'ai pas fait, mais cela vient du fait que j'ai déjà été ministre du cabinet fantôme en matière d'institutions démocratiques. Depuis cette époque, je crois fondamentalement que le gouvernement n'agit pas suffisamment contre l'ingérence étrangère, ce qui, selon moi, est inextricablement lié à notre protection et à notre cybersécurité en tant que parlementaires, et ce après au moins six interactions avec l'ancien ministre des Institutions démocratiques, ainsi que des discours que j'ai prononcés à la Chambre des communes.

Par ailleurs, la mise en place de la Charte du numérique, un outil inutile et inefficace, a été pour moi un autre point d'achoppement de l'année 2019.

Donc, non, mais je pense que c'est parce que, si rien n'a été fait jusqu'à présent, cela m'a semblé inutile.

M. Tom Kmiec: Non, je n'ai eu aucun contact. Les seules personnes qui ont pris contact avec moi sont les représentants du FBI lors de la séance d'information du 9 mai.

M. Eric Duncan: Je vous remercie.

Ce que je veux dire, c'est qu'il y a manifestement un problème de protocole, mais je pense que le problème le plus important est un problème de culture. Il existe actuellement des protocoles dont les fonctionnaires pensaient qu'ils informeraient les parlementaires, ce qui n'a pas été le cas. Le problème plus important est celui d'une culture organisationnelle qui émane du BCP, du CPM et de différentes agences qui, franchement, me semble-t-il, ont fait preuve de négligence en supposant que quelqu'un d'autre s'en occuperait, de sorte qu'il n'y a pas eu de suivi adéquat.

Je voudrais demander à chacun d'entre vous ses commentaires sur la culture organisationnelle actuelle, qui consiste à ne pas assurer le suivi et à ne pas veiller à ce que les personnes menacées soient informées en temps utile, qu'on leur fournisse les ressources appropriées, etc. Dans votre réponse, vous pourrez peut-être parler de ce qui doit changer et de qui est responsable.

En ce qui concerne la déception vécue par Mme Sgro, à qui doit-on s'adresser pour avoir des réponses? Qui est responsable de ces ratés?

M. Tom Kmiec: Monsieur le président, je répondrai à cette question en répétant ce qu'a dit Mme Sgro.

Je pense que le gouvernement nous considère comme jetables, parce que nous sommes des membres du Parlement. Nous allons et venons, et c'est ainsi que notre système est censé fonctionner. En particulier pour nous, les simples députés, je pense qu'il existe une culture au sein des agences et du gouvernement en général selon laquelle, parce que nous ne sommes que de passage, pour utiliser un terme que je lis parfois dans la réponse des fonctionnaires à mes demandes d'accès à l'information. Ils savent très bien que les élus ne sont en poste que de manière temporaire, et nous voient comme des pions interchangeables. Je pense que le gouvernement avait la responsabilité morale et éthique de nous tenir informer dès le départ.

Je demande simplement à ce que les députés soient mis au courant des différentes manières d'être aidé. Je peux ensuite aller demander au CST l'aide du centre de cybersécurité et du sergent d'armes. Je connais désormais mes options et les personnes-ressources, mais il m'a d'abord fallu me débrouiller seul.

Mme Stephanie Kusie: Je pense qu'il s'agit d'une naïveté coordonnée entre toutes les autorités. Historiquement, nous sommes entrés dans une autre ère, je dirais même plus récemment, je dirais même sur une base hebdomadaire ou mensuelle. Toutefois, j'ai l'intime conviction, et je suis certaine que je serai contestée sur ce point, que l'indifférence et l'incompétence du gouvernement actuel expliquent tous ces ratés majeurs en matière de sécurité. J'en suis tout à fait convaincue.

L'hon. Judy A. Sgro: Je pense que pendant de nombreuses années, nous avons tous été naïfs, que nous soyons parlementaires ou que nous travaillions dans un grand nombre de domaines différents. Le gouvernement actuel commence tout juste à prendre conscience des questions d'ingérence étrangère et à tout ce qui s'ensuit. Le monde est entré dans une nouvelle ère, et je pense que tout le monde a fait preuve de naïveté à ce sujet. Je ne pense pas que quiconque ait intentionnellement retenu quoi que ce soit qu'il pensait pouvoir nous nuire. Fort heureusement, le pare-feu a tenu. Nous sommes censés être tout à fait rassurés. Le pare-feu a tenu lorsque nous avons eu cette attaque de type APT31. C'est ce qu'on m'a dit. Apparemment, nous sommes censés nous réjouir.

Nous allons trouver un moyen de mieux protéger les parlementaires et la population canadienne au fur et à mesure que nous progressons dans ce dossier.

M. Eric Duncan: La culture du secret et, je pense, le manque de respect à l'égard des parlementaires, c'est que depuis que d'autres questions de privilège et d'autres problèmes ont commencé à être révélés, de nombreuses directives ont été émises pour améliorer le processus et dire que les parlementaires doivent être informés. Même après la divulgation de ces directives, les parlementaires n'ont toujours pas été informés.

Ce que je veux dire à propos de la culture organisationnelle, c'est que le protocole, cette directive, a été donné pour améliorer le processus, et qu'il a été littéralement ignoré avec toutes les excuses possibles.

Je parlerai simplement de la culture, madame Sgro. C'est nouveau et nous avons peut-être été naïfs, mais pour moi, il s'agit d'une culture qui consiste à prendre au sérieux tout protocole ou toute directive et à l'améliorer. Nous avons vu des exemples de ce qui a été dit, mais qui n'a pas été suivi d'effets concrets.

Je souhaite que toute personne ayant d'autres commentaires à faire à ce sujet puisse s'exprimer.

● (1225)

Le président: Nous allons entendre un témoin très rapidement, s'il vous plaît.

L'hon. Judy A. Sgro: Je voudrais simplement ajouter que lorsque nous avons discuté avec le FBI et l'IPAC et que nous avons demandé pourquoi nous n'avions pas été informés, on nous a répondu que, selon le système en vigueur, le FBI devait faire rapport à une personne particulière au sein du gouvernement du Canada. Il ne pouvait pas s'adresser directement à nous. Plusieurs semaines plus tard, le FBI a tenu une réunion d'information avec nous tous. Ils nous ont dit qu'il y avait un système en place qui faisait que le FBI ne pouvait pas nous informer directement. Il fallait passer par un protocole en place que personne ne semblait suivre.

Le président: Merci beaucoup, monsieur Duncan.

Madame Romanado, à vous la parole pour les six prochaines minutes.

Mme Sherry Romanado: Merci beaucoup, monsieur le président. Par votre intermédiaire, j'aimerais remercier mes collègues de leur présence.

Je vais commencer comme je l'ai fait pour le dernier panneau. Je crois fermement que vous auriez tous dû être informés. Il est très regrettable que vous ne l'ayez pas été.

Juste pour revenir sur ce point, monsieur Kmiec, vous avez mentionné que vous aviez eu une réunion avec le FBI le 9 mai, mais vous avez mentionné que vous n'aviez pas rencontré le CSIS ou le CST. Avez-vous rencontré quelqu'un depuis que cette affaire a été révélée? Quelqu'un, qu'il s'agisse du CST, du Services des TI de la Chambre des communes ou du SCRS, s'est-il entretenu avec vous?

M. Tom Kmiec: Non.

Mme Sherry Romanado: Madame Kusie, dans votre cas, quelqu'un vous a-t-il rencontrée?

Mme Stephanie Kusie: Non. Je vais en rester là, madame Romanado.

Mme Sherry Romanado: Et vous, madame Sgro?

L'hon. Judy A. Sgro: Le SCRS m'a rencontré... C'était à ma demande.

Mme Sherry Romanado: Donc, si je comprends bien, c'est vous qui aviez dû solliciter une rencontre avec le SCRS?

L'hon. Judy A. Sgro: C'est exact.

Mme Sherry Romanado: De toute évidence, le protocole ne fonctionne pas. Le fait que vous ayez dû prendre l'initiative de contacter vous-même le SCRS est très problématique.

Lors de la dernière comparution des responsables du SCRS et du CST, j'ai compris qu'il existe un malentendu fondamental par rapport au rôle réel des députés. Je ne suis pas une agente de renseignements. Je ne suis pas familière avec leur travail, mais je pense qu'il y a vraiment un décalage. Ils ne se rendent pas compte, comme l'a dit Mme Sgro, que le travail que nous faisons nous expose davantage au risque de susciter l'intérêt d'acteurs étatiques et non étatiques. Nous ne voulons jamais que les députés changent ce qu'ils font. Nous voulons qu'ils continuent à faire ce qu'ils font, parce que c'est un travail important, que ce soit ici au Canada ou à l'étranger, ou qu'ils défendent les droits de la personne.

Que recommanderiez-vous au Comité pour s'assurer que les agences de renseignement et les responsables de notre protection, que ce soit physiquement ou dans le monde virtuel, puissent bien comprendre la nature de notre travail parlementaire? De quelle manière le Comité devrait-il engager un dialogue sur ces enjeux essentiels?

Tous les témoins peuvent répondre à la question.

M. Tom Kmiec: Monsieur le président, je vais tenter de répondre à cette question.

Tout d'abord, ces agences doivent être tenues d'informer les parlementaires. Je veux éviter de revivre une situation gênante lors de laquelle le Bureau du sergent d'armes et les services de cybersécurité de la Chambre des communes se sont renvoyé la balle, prétextant chacun ne pas être au courant. Ensuite, ils viennent ici et tout le monde dit que quelqu'un d'autre a été chargé de le dire à quelqu'un. Ce n'est pas clair pour moi. Encore une fois, vous avez les discussions à huis clos qui ont eu lieu. Je note que le CST n'a cessé de répéter qu'il pouvait répondre à certaines de ces questions à huis clos.

J'ai besoin de savoir. Je dois savoir si je suis une cible. Cela changera la manière dont je fais mon travail, parce que cela a déjà eu un impact sur mon travail. Lorsque des personnes me contactent pour me rencontrer, si vous cherchez mon nom sur Google, c'est l'une des choses qui apparaîtra, de sorte que certaines personnes, certains dissidents et journalistes en exil, risquent de s'autocensurer. Ils ne nous contacteront pas. Si je lui envoie un courriel, si je le contacte sur ses médias sociaux, ceux-ci pourraient être mis sur écoute. Cela pourrait déjà être compromis par une agence étrangère.

Des renseignements publics montrent que ces agences étrangères s'intéressent à moi pour le travail que nous faisons tous ici. De ce fait, cela a déjà eu des conséquences réelles sur mon travail.

Je vous remercie, monsieur le président.

● (1230)

Mme Sherry Romanado: Je vous remercie. C'est un très bon point. Ce que nous examinons, ce n'est pas seulement la question de privilège, mais aussi la question de savoir qui est responsable de s'assurer que les députés sont au courant. Tout au long de cette étude, nous n'avons pas eu d'indication claire. Tout le monde, comme vous l'avez dit, rejette la responsabilité sur le dos des autres. Nous voulons corriger cette situation, évidemment.

Vous avez également mentionné que cela a changé votre façon de travailler. Voilà qui me semble très inquiétant. La réalité, c'est que chacun d'entre nous a des rôles différents à jouer, des parcours différents et tout le reste. À certains égards, nous sommes tous des cibles pour différents acteurs étatiques et non étatiques.

En ce qui concerne le protocole, nous avons une directive ministérielle qui, d'après ce que j'ai compris de la dernière réunion, n'a été adressée qu'au SCRS, et non au CST ou aux services des TI de la Chambre des communes. Recommanderiez-vous que la portée de la directive ministérielle soit élargie?

Madame Sgro, allez-y.

L'hon. Judy A. Sgro: Absolument, si cela s'avère nécessaire. On pourrait penser que ce n'est pas nécessaire, mais il semble qu'une directive ministérielle s'impose, alors commençons par cela. Ils doivent avoir cette directive. Ils doivent communiquer l'information aux parlementaires.

Je pense qu'il est difficile de croire que tous les gens qui s'occupent de nous protéger ne savent pas, pour revenir à la question de M. Kmiec, ce que nous faisons vraiment et que nous nous penchons sur beaucoup d'enjeux internationaux et toutes ces autres questions. Est-il possible qu'ils ne sachent pas dans quelle mesure nous sommes nombreux à nous aventurer dans des domaines qui semblent déranger la Chine, l'Iran, et j'en passe?

Je ne peux pas croire qu'ils ne sont pas au courant. Ils devraient peut-être passer un peu de temps avec les parlementaires ou regarder un peu ce qui se passe à la Chambre des communes. Peut-être que cela changerait les choses.

Mme Sherry Romanado: Il ne me reste que 15 secondes. Encore une fois, je tiens à vous remercier d'être venus aujourd'hui et de nous avoir fait part de vos commentaires, car nous nous devons de régler ce problème.

[*Français*]

Le président: Merci.

Madame Gaudreau, vous avez la parole pour six minutes.

Mme Marie-Hélène Gaudreau: Monsieur le président, honnêtement, aujourd'hui, je constate que c'est une rencontre des plus pertinentes. Je ne sens pas, comme à l'habitude, beaucoup de partisanerie. Nous sommes vraiment en train de parler du problème.

Je fais un petit retour sur ce qu'on a vécu. J'ai bien entendu quand vous avez dit qu'il faut prendre ça en main et qu'il faut aller au-devant.

J'ai posé la question. Un jour, il y aura un autre gouvernement. Est-ce normal que la confiance n'y soit plus? Quand nous avons rencontré les représentants du Centre de la sécurité des télécommunications, j'ai moi-même levé la main en disant que, considérant que je ne suis pas actuellement leur cliente et qu'ils font affaire avec le gouvernement, je veux être leur cliente.

J'aimerais entendre vos commentaires à ce sujet. Que pensez-vous de faire sortir cela? Ça fait partie de notre vie, être députée, c'est 24 heures sur 24, 7 jours sur 7. Qu'est-ce que vous en pensez?

Mme Stephanie Kusie: Selon moi, il est nécessaire d'évaluer le système au complet. Nous devons penser aux menaces. À mon avis, il est important de mieux informer les parlementaires et les députés, parce qu'en ce moment, il semble qu'il manque un système pour analyser les menaces. Il faut évaluer le système en entier, mais aussi les menaces contre chaque député. Selon moi, les menaces contre les députés sont différentes, selon les activités du député ou de la députée.

Comme je l'ai dit aussi, il est vraiment important d'avoir de la transparence ainsi que de la formation. Je pense que la formation est vraiment importante pour les députés. Pour ma part, je veux voir une révision complète du système pour qu'il y ait plus d'évaluations des menaces, plus de transparence et plus de formation.

Mme Marie-Hélène Gaudreau: Je veux juste être sûre, parce que j'ai peut-être manqué le début de vos remarques liminaires. Les attaques étaient-elles sur vos comptes personnels? Oui ou non.

M. Tom Kmiec: J'allais dire que, dans mon cas, c'était sur mon compte public que j'utilise. J'ai les trois courriels avec moi, aujourd'hui. Je les ai imprimés, parce qu'ils sont encore dans mon compte. Je peux ouvrir ces courriels à n'importe quel moment.

Cependant, dans le système de cybersécurité, personne ne m'a dit si je pouvais ouvrir ou non les courriels. Je les ai donc ouverts et je les ai imprimés, tous les trois. Ils sont encore dans mon compte. Personne ne m'a dit que je ne pouvais pas le faire. D'après ce que je sais, la technique de surveillance numérique de ces attaques fonctionne avec des pixels espions. Comme c'est un sujet qui est nouveau pour moi, j'ai fait une recherche sur Google pour me renseigner, avec l'aide de mon personnel. Tout est décrit parfaitement.

Dans mon cas, ça a touché mon compte courriel public. Mon personnel dans mon bureau de circonscription et mon personnel dans mon bureau sur la Colline ont accès à ces comptes pour m'aider dans mon travail. Chacun de ces ordinateurs aurait pu être touché par ces attaques en raison d'un manque de formation, qui aurait dû m'être donnée.

● (1235)

Mme Marie-Hélène Gaudreau: Est-ce que c'était votre compte personnel, madame Sgro?

[*Traduction*]

L'hon. Judy A. Sgro: C'était l'ensemble de mon compte de la Chambre des communes.

Puis-je revenir à la question de tout à l'heure sur ce que nous pouvons faire?

Vous savez, nous sommes en juin, et nous en apprenons beaucoup. J'espère qu'à la reprise des travaux de la Chambre en septembre, tous les parlementaires recevront une présentation très détaillée sur les questions de sécurité, de sorte que nous puissions commencer la session par...

[*Français*]

Mme Marie-Hélène Gaudreau: Je vous arrête, parce que mon temps est calculé.

D'ailleurs, je ne sais pas pour vous, mais notre caucus a été breffé par le Service canadien du renseignement de sécurité. Ça devient une nécessité mais, effectivement, je suis très préoccupée par la prévention parlementaire.

Étiez-vous dans la même situation?

Mme Stephanie Kusie: Je dirais plus ou moins. J'ai trois comptes. Le premier, c'est stephaniekusie.mp; le deuxième, c'est mon compte personnel de députée, mon adresse .p9; quant au troisième, c'est une adresse gmail. Dans mon cas, c'était le compte où il y a le moins d'information sensible, mais qui constitue une fenêtre donnant accès aux autres comptes. C'est ce qui me dérange le plus.

Mme Marie-Hélène Gaudreau: C'est exact.

J'ai une autre question. Tantôt, j'expliquais un peu ma grogne contre le fait que, moi qui n'ai aucune qualification en matière d'espionnage, j'ai trouvé sur le Web le 15 décembre 2021 un article expliquant la campagne d'attaque du mode opératoire APT31. On voit des articles de journaux, entre autres celui du 12 mai où on décrit ce qu'on a demandé quand on a eu la visite de représentants du Centre de la sécurité des télécommunications, qui ne nous ont rien donné comme éléments. Nous n'avons rien appris.

Ceci étant dit, et je vais finir là-dessus, il y a une députée, c'est dans le journal *Le Monde*, qui a fait part de son intention de déposer une plainte judiciaire, parce qu'elle a vécu exactement ce que vous avez vécu. Sur le fait, comme ça, dans votre situation, où vous situez-vous là-dedans? Êtes-vous suffisamment en colère pour que ça bouge?

M. Tom Kmiec: Pour ma part, je n'étais pas en colère quand j'ai su que j'ai été l'objet de ce type d'attaque de la part d'une agence étrangère. J'étais déçu que mon gouvernement n'ait pas pensé que ça valait la peine de me le dire ou de me protéger.

[*Traduction*]

Le président: D'accord.

[*Français*]

Merci beaucoup.

[*Traduction*]

Madame Mathyssen, vous avez six minutes.

Mme Lindsay Mathyssen: Merci, monsieur le président.

Merci aussi à vous trois d'être des nôtres aujourd'hui et de nous faire part de votre expérience.

Au dernier tour, j'ai parlé du fait que cette institution et les parlementaires en général recevraient des millions de messages. Je suis un peu préoccupée, car lorsque les représentants du SCRS et du CST étaient ici, ils ont expliqué — tout comme, je crois, les représentants de l'Administration de la Chambre — qu'ils fournissent régulièrement aux parlementaires des avertissements généraux et que, selon eux, cela suffit pour nous faire comprendre ce que serait l'ingérence étrangère ou une cyberattaque. Nous avons également parlé de la responsabilité personnelle et de ce que cela signifie pour chaque député. Nous venons de parler du fait que le SCRS nous a donné une séance d'information cette semaine lors des réunions de caucus.

Madame Sgro, vous avez parlé de la nécessité de ces séances d'information. Que voulez-vous voir en général, bien au-delà de ce qui se fait déjà? Je sais que ce serait probablement accablant pour les députés s'ils étaient informés de chacune des attaques lancées, mais à quoi devraient ressembler ces séances d'information, selon vous? Devraient-elles avoir lieu tous les trois mois, vu que l'information change si rapidement?

Donnez-moi simplement une idée de ce que vous en pensez.

L'hon. Judy A. Sgro: Je pense que nous devons cesser de rester muets sur le sujet et commencer à en apprendre davantage et à nous tenir au courant du nombre de menaces. Encore une fois, cela dépend aussi de la catégorie de menace.

Il faut mettre en commun plus de connaissances. Les choses évoluent si rapidement que, même si nous avions reçu une séance d'information il y a un an ou six mois, d'ici l'automne, les choses auraient recommencé à bouger très rapidement. Nous devons nous assurer de rester au fait de la situation. Nous sommes tous occupés. Je ne regarde même pas les médias sociaux. Je ne m'en sers pas. Je m'en fiche de ce qui s'y dit. Laissons-les faire ce qu'ils veulent parce que, pour ma part, je vais faire ce qui s'impose.

Cependant, lorsque la catégorie de menace atteint un certain point, il faut que quelqu'un communique avec moi et me dise: « Vous savez, ce que vous avez dit la semaine dernière a généré telle ou telle menace. » Faites-le-moi savoir. Je m'en occuperai en conséquence. Je crois qu'il faut des avertissements fréquents. Compte tenu de la rapidité avec laquelle les choses évoluent, je ne pense pas qu'il suffise de faire cela une fois par année ou une fois tous les trois ans au début d'une nouvelle législature.

● (1240)

Mme Stephanie Kusie: J'ai eu le plaisir de visiter la majorité des démocraties menacées dans le monde, sauf l'Ukraine. C'est le pays qui se démarque. Lorsque j'étais en Corée du Sud, les représentants coréens avaient une carte numérique des cybermenaces en temps réel. À notre époque, je ne vois pas pourquoi nous ne pourrions pas en être informés dans un rapport quotidien ou même dans un rapport sur les attaques. La technologie existe, à mon avis, et nous sommes en mesure d'intercepter ou de déceler et d'empêcher les attaques. Je crois que nous devrions recevoir beaucoup plus d'informations parce que nous en avons les moyens technologiques. Je pense que nous avons le droit de savoir.

Comme je l'ai dit, ceux d'entre nous qui participent davantage à des activités prodémocratiques et en faveur des droits de la personne auront certainement affaire à plus de menaces. Je pense que le gouvernement a la responsabilité de nous protéger lorsque nous faisons ce travail.

M. Tom Kmiec: Je vous remercie de la question.

À mon avis, ces séances d'information génériques ou ces courriels que nous recevons nous disent de ne pas ouvrir les courriels qui constituent un stratagème évident d'hameçonnage, et il y a un bouton « hameçonnage »... Je n'ai jamais utilisé cette fonction depuis 20 ans que j'utilise Outlook. Je ne peux donc pas vous dire à quoi elle sert. Je sais seulement qu'il ne faut pas ouvrir le courriel. C'est évident pour moi.

Je connais mes collègues ici présents. Je sais que Mme Kusie est très engagée auprès des exilés cubains qui luttent pour la liberté à Cuba. Je sais que Mme Sgro partage mon intérêt pour un Iran libre et qu'elle dirige l'un des différents groupes parlementaires. Lorsqu'il y a des attaques précises contre nous par des gouvernements étrangers ou des groupes étrangers, on devrait nous le dire sur-le-champ, au lieu de nous remettre ces mémoires génériques tous les trois mois ou en cas d'une attaque par hameçonnage sur la Colline du Parlement contre nos courriels. Ce n'est pas utile.

Je souhaite toutefois faire l'éloge d'un groupe: les gens de Parl-Voyage, qui nous donnent les téléphones jetables et nous informent de ce qu'il faut faire et des menaces en matière de sécurité. Lorsque je suis allé en Irak l'an dernier avec une délégation parlementaire, ils ont fait un excellent travail. Ils nous ont dit exactement ce qui était raisonnable, ce qui ne l'était pas et comment assurer la sécurité numérique des voyageurs dans les différents aéroports.

À part cela, comme je l'ai dit, personne du SCRS, du CST ou de tout autre organisme connexe n'est venu me parler, à l'exception du FBI, pour me dire et m'expliquer ce que je pourrais faire pour être plus en sécurité, et aucun d'eux ne m'a fourni des solutions concrètes, techniques et utilisables.

Mme Lindsay Mathyssen: Je vous remercie.

Le président: Il vous reste une minute.

Mme Lindsay Mathyssen: Madame Sgro, je voulais m'adresser à vous pour vous remercier de votre présidence du Groupe d'amitié Canada-Taïwan et de tout le travail que vous accomplissez à cet égard. Je suis allée, moi aussi, à Taïwan. Nous avons également entendu le point de vue des Taïwanais sur la façon dont ils gèrent les millions de messages provenant de la Chine chaque jour.

Ils ont nommé un ministre des Affaires numériques. Est-ce quelque chose que le Canada devrait reproduire? Avez-vous d'autres idées découlant de vos nombreux voyages et des leçons que vous en avez tirées en guise de pistes de solution?

L'hon. Judy A. Sgro: J'ai trouvé fascinant de voir les milliers et les milliers de messages de désinformation qu'ils reçoivent chaque jour. Leur équipe compte quatre personnes dont le travail consiste à surveiller le système, 24 heures sur 24, sept jours sur sept — c'est tout ce qu'elles font — et à publier des rectificatifs pour contrer la désinformation qui alimente les réseaux. Je pense que nous avons beaucoup à apprendre d'eux dans ce domaine particulier pour ce qui est de réprimer la désinformation.

Selon moi, la cybersécurité — dans son ensemble — doit être prise beaucoup plus au sérieux pour la suite des choses.

Le président: Merci beaucoup, madame Mathyssen.

Monsieur Calkins, vous avez cinq minutes.

M. Blaine Calkins (Red Deer—Lacombe, PCC): Merci, monsieur le président.

Je tiens à faire une distinction parce que je pense qu'il y a eu des tentatives d'amalgamer une foule d'attaques à l'incident qui s'est produit dans ce cas précis. Nous parlons ici d'hameçonnage. C'est tout à fait différent. Il ne s'agit pas d'une attaque par déni de service. Il ne s'agit pas d'une cyberattaque. Une attaque par hameçonnage est une attaque personnelle, parce que la vulnérabilité se situe sur le plan humain.

Je suis tout à fait convaincu que nos experts techniques... En fait, j'ai travaillé dans le domaine des TI dans une vie antérieure. Je suis maintenant tellement rouillé que je ne saurais pas comment fonctionnent les nouvelles technologies utilisées.

La différence ici, c'est qu'il s'agit d'une erreur commise par un être humain. C'est ainsi que les auteurs de ces attaques procèdent. Nous pouvons en fait contrecarrer la plupart des cyberactivités. Nous pouvons déjouer les attaques par déni de service. Nous pouvons faire obstacle à toutes ces attaques technologiques. Cependant, il s'agit d'une attaque qui se déploie lorsque l'un d'entre nous clique sur quelque chose qu'il ne devrait pas: c'est là que réside la vulnérabilité.

La différence dans ce cas particulier, c'est que la situation était suffisamment grave... Il ne s'agissait pas simplement de quelqu'un qui cherchait à nous arnaquer financièrement. Ce n'était pas un courriel envoyé par un soi-disant prince nigérian. C'était suffisamment grave parce qu'il s'agissait d'un acteur étatique étranger hostile, ou considéré comme potentiellement hostile, qui ciblait directement un groupe d'entre nous — 18 de nos collègues — dans le cadre de cette attaque.

Ce qui est frustrant pour moi, c'est que notre travail et notre responsabilité première... Nos tâches ne relèvent pas de la routine bureaucratique. En fait, nous devons faire preuve d'une grande souplesse. Notre travail ne se limite pas à un horaire fixe de neuf à cinq, du lundi au vendredi. Si nous voulons être en mesure de faire notre travail, nous devons savoir ce qui se passe. Si nous ne sommes pas informés...

Si les 18 parlementaires ont pris connaissance de la situation, c'est parce que le FBI a publié cette information; voilà qui est tout à fait embarrassant pour un pays comme le nôtre. C'est différent d'une cyberattaque. C'est différent de tous les autres messages aléatoires qui pourraient être envoyés à nos courriels. Il s'agit d'une activité hostile qui vise à faire quelque chose de subversif ou de préjudiciable aux députés et, partant, à l'ensemble de l'institution et à notre démocratie à la base.

Si on ne nous informe pas de quelque chose d'aussi précis... Le FBI a jugé que c'était suffisamment important. Ses agents semblent être en mesure de faire la distinction entre les cyberattaques, les attaques par déni de service, les attaques contre des infrastructures et les autres attaques aléatoires par hameçonnage ou par logiciel malveillant. Pourquoi le Canada ne peut-il pas en faire autant?

Comment sommes-nous censés demander des comptes au gouvernement si nous ne savons même pas qu'il y a un problème?

Je vous invite tous les trois à donner quelques conseils au Comité à ce sujet. À votre avis, quelle aurait été la meilleure façon de vous informer de la situation? Quel aurait été un délai plus approprié pour vous?

La seule raison pour laquelle nous en parlons, c'est parce que quelqu'un d'autre nous a mis la puce à l'oreille.

● (1245)

Le président: Monsieur Calkins, il reste environ 90 secondes pour les témoins.

M. Blaine Calkins: Je vais en rester là. Je sais que c'est une question très ouverte et très générale, mais...

L'hon. Judy A. Sgro: Si l'Alliance interparlementaire sur la Chine ne nous avait rien dit, nous ne serions pas au courant aujourd'hui. Il a fallu que cette organisation, qui n'a rien à voir avec le Canada, communique avec nous et nous informe, sinon nous ne l'aurions pas su.

Je reviens à l'idée que nous sommes déçus. Nous, les parlementaires, avons besoin de savoir quand une menace est proférée contre nous. Nous devons le savoir. Cela ne veut pas dire dans six mois. Si je recevais une menace aujourd'hui, d'après ce que j'ai dit hier, je ne saurais même pas à quelle porte frapper. Je sais que je vais m'adresser au sergent d'armes, mais que se passera-t-il ensuite?

Nous devons savoir quoi faire, quoi ne pas faire et à qui nous adresser lorsque nous recevons quelque chose qui, à nos yeux, représente une grave menace.

M. Tom Kmiec: Je vous remercie de la question.

J'ajouterais que le gouvernement du Canada doit traiter notre sécurité numérique comme la Chambre des communes traite notre sécurité physique. Je me sens en sécurité autour de la Cité parlementaire parce que je sais qu'il y a suffisamment d'agents du SPP, qui gèrent activement la sécurité des lieux.

En ce qui concerne la sécurité numérique, je suis certain qu'ils peuvent fermer nos courriels et assurer la sécurité de nos fichiers, quel que soit l'appareil sur lequel ils se trouvent, mais lorsque le CST a appris qu'il s'agissait du groupe APT31... On ne parle pas ici de simples amateurs installés dans leur sous-sol. Ce sont des hommes et des femmes dans la mire du département d'État américain, qui offre une récompense de 10 millions de dollars en échange de toute information menant à leur arrestation. Il s'agit d'une unité active du renseignement étranger.

Dès que cela a été découvert, le SCRS, le CST et la myriade d'organismes connexes auraient dû assumer une responsabilité objective. Ne m'envoyez pas un courriel. Appelez mon bureau. Communiquez avec moi directement. Dites-moi que je suis une cible. Dites-moi pourquoi je suis une cible, si vous êtes au courant, parce que j'aimerais le savoir.

Pour ce qui est de l'hameçonnage, je suis tout à fait d'accord avec vous. Les gens en sont victimes dans leur vie privée et professionnelle, mais le fait d'être la cible d'un service de renseignement étranger est nouveau.

● (1250)

Le président: Merci beaucoup.

Monsieur Hardie, vous avez lcinq minutes.

M. Ken Hardie (Fleetwood—Port Kells, Lib.): Merci, monsieur le président.

Je vous remercie de l'information que nous avons obtenue ce matin.

Le CPSNR, bien sûr, a produit un rapport. De toute évidence, comme nous l'avons appris, certaines personnes sont nommées dans ce rapport, qui se fonde sur les renseignements révélés dans le cadre de divers travaux effectués par les organismes canadiens.

Je veux revenir à la question de privilège. On a beaucoup parlé de la question de savoir si nous devrions divulguer les noms de ces personnes au monde entier. Ne devrions-nous pas réfléchir aux façons de divulguer cette information à ces personnes? Est-ce là une question de privilège?

Je vous demande simplement votre avis. Vous n'avez pas besoin d'avoir des connaissances encyclopédiques ou approfondies sur toute la question, mais qu'en pensez-vous?

Commençons par vous, madame Kusie.

Mme Stephanie Kusie: Absolument, je pense que c'est la première étape. À mon avis, les noms devraient être divulgués au monde entier, et c'est également la position de notre parti et de notre chef. Cette information devrait absolument leur être divulguée. Je sais que je fais constamment un inventaire...

M. Ken Hardie: Je vais vous demander une réponse assez courte à cette question, car j'ai beaucoup d'autres questions à poser.

Mme Stephanie Kusie: Alors, oui.

M. Ken Hardie: Qu'en pensez-vous, madame Sgro?

L'hon. Judy A. Sgro: Je crois que ces personnes devraient savoir qu'elles sont citées dans ce rapport pour le moins préoccupant, mais je ne pense certes pas que leurs noms devraient être rendus publics.

Sur quelle base pourriez-vous lancer le nom de qui que ce soit dans l'espace public?

Il y a beaucoup d'insinuations dans ce rapport, mais pas de preuve. Il y a un gros travail de renseignements et tutti quanti, mais vous ne pouvez pas décider tout à coup de dire que Ken Hardie est cité dans ce rapport en tant que personne qui pourrait travailler à l'encontre du Canada.

M. Ken Hardie: J'aurai quelque chose à dire à ce sujet dans une seconde.

Allez-y, monsieur Kmiec.

M. Tom Kmiec: Monsieur le président du comité Canada-Chine, je suis heureux de vous voir ici.

Je vais attirer votre attention sur la page 76 du rapport du Secrétariat du Comité des parlementaires sur la sécurité nationale et le renseignement, nommément au paragraphe 162 coiffé du titre Communications avec les parlementaires. Pour répondre brièvement à votre question, je voudrais vous lire un extrait de ce paragraphe et dire que, oui, ces noms devraient être divulgués. Voilà:

> Cette recommandation découle du fait que les parlementaires sont souvent au centre des activités d'ingérence menées par les États étrangers. Bien que le Comité reconnaisse que le SCRS a donné des séances d'information à certains députés, une stratégie d'information complète visant tous les parlementaires n'a pas été mise en place même si le BCP a demandé à deux reprises l'autorisation du premier ministre.

Cela renvoie directement au sommet.

M. Ken Hardie: Oui.

Il y a quelqu'un qui circule dans la région de Surrey en ce moment et qui est identifié comme un mandataire de l'Inde. Il dit à tout le monde, y compris au journaliste à qui j'ai parlé le week-end dernier, que lui et moi sommes comme ça. Ce n'est pas le cas. Je ne serais pas surpris que mon nom figure dans ce rapport rien qu'à cause de cela. Je mériterais de le savoir, même si cela se faisait en privé, car je pense qu'il s'agit d'une question de privilège.

Monsieur Kmiec, je dois vous féliciter pour le travail que vous avez accompli au sein du comité Canada-Chine. Vous avez été au cœur d'un grand nombre de témoignages et de commentaires très intéressants.

Nous savons que la Chine est très opiniâtre. Elle joue sur le long terme. Le groupe APT31 est une chose, mais je m'inquiète de l'effet cumulatif que son action pourrait avoir en conjugaison avec ce que fait le Front uni et tout le reste.

Pourriez-vous rassembler tous ces éléments et nous dire ce que nous devrions faire?

M. Tom Kmiec: Je vais essayer d'être aussi bref que possible.

De façon générale, je suis d'accord. Comme je l'ai découvert avec mon personnel, il y a beaucoup de différents groupes APT. Lorsqu'on fait une recherche, on s'aperçoit qu'il y a plusieurs unités. C'est la fine lame de l'épée que manie la République populaire de Chine. Comme vous le savez, monsieur le président, nous nous attendons à ce que les interventions de ce type se multiplient à l'avenir, à ce que des stratagèmes bien organisés soient menés contre les démocraties occidentales et les législateurs. Dans bien des cas, les législateurs sont considérés comme le maillon faible du gouvernement parce qu'en général, ils n'ont pas l'aide des organismes.

J'attire votre attention sur la déclaration des législateurs belges, qui ont dit qu'ils n'avaient pas non plus été informés par leur gouvernement qu'ils avaient été la cible d'APT31. Dans leur cas, ils ont déclaré qu'il s'agissait d'une attaque directe contre leur démocratie et leur Parlement parce que leur gouvernement ne les avait pas informés, et ils s'attendent à d'autres attaques de la part d'entités et d'agences de la République populaire de Chine.

Je dirais que, depuis 2012, lorsque Xi Jinping a pris le pouvoir, le Département du travail du Front uni est devenu un appareil de sécurité d'État qui intervient dans toutes les démocraties occidentales, et que nous devrions prêter une grande attention à toutes ses sous-entités, comme ces groupes de type APT31.

● (1255)

Le président: Nous sommes arrivés à la fin de votre temps de parole, monsieur Hardie.

Merci.

[*Français*]

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

Mme Marie-Hélène Gaudreau: Je vais juste revenir, monsieur le président. Je constate que ce que j'ai trouvé et qui provient de l'Agence nationale de la sécurité des systèmes d'information de la République française, c'est notre Centre de la sécurité des télécommunications. Lors de notre rencontre, on s'attendait à avoir des détails.

Je vous le dis: allez le chercher. À l'intérieur, il y a toute la chaîne d'infection — ça date de 2021 —, les vecteurs d'intrusion, les méthodes d'invasion, la victimisation, les infrastructures, les équipements ciblés et la porte arrière, par exemple. Tout est là, c'est accessible depuis 2021. Je vous invite à en prendre connaissance. On sera vigilant.

J'ai une seule question. Votre vie privée est-elle touchée? Si oui, vos familles sont-elles inquiètes?

[*Traduction*]

L'hon. Judy A. Sgro: Oui, mais cela ne va pas plus loin. Je leur ai dit de ne pas s'inquiéter, que je suis bien protégée. Je leur ai dit de ne pas s'inquiéter. Les choses sont ainsi faites.

[*Français*]

Mme Marie-Hélène Gaudreau: C'est inacceptable.

Mme Stephanie Kusie: Mon mari et moi acceptons la situation, en gros, car, étant donné la vie que nous vivons, nous n'avons pas de vie privée. C'est plus ou moins la vérité. Pour mon fils, c'est un peu plus compliqué, parce qu'il est jeune. Il a peur, il pense à des choses comme la guerre nucléaire. Il s'inquiète pour nous et se demande si c'est dangereux pour nous. Évidemment, nous devons continuer à vivre, tout en sachant que les menaces existent.

M. Tom Kmiec: Au quotidien, la réponse est non. Mes trois enfants savent que je voyage et que je prends des photos. Ceux de mes enfants qui ont le droit d'avoir un compte me suivent sur les réseaux sociaux. En fait, je n'amène pas mes enfants à beaucoup d'événements publics.

Cependant, je m'inquiète du fait que mes enfants sont en partie chinois et en partie juifs. Quand je vois les manifestations dans les rues et le racisme contre les personnes d'origine asiatique, j'ai des inquiétudes sur la culture de notre pays et les effets néfastes que des campagnes de ce genre, menées par des agences étrangères contre nous, auront sur notre culture et notre société.

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

Le président: Merci, madame Gaudreau.

[*Traduction*]

Madame Mathyssen, vous avez deux minutes et demie.

Mme Lindsay Mathyssen: L'une des raisons pour lesquelles les députés de l'Alliance interparlementaire sur la Chine n'ont pas été informés, c'est qu'une enquête était en cours et que l'on craignait qu'elle soit rendue publique, ce qui aurait pu la compromettre.

Acceptez-vous cette raison?

L'hon. Judy A. Sgro: Non, je ne l'accepte pas.

Ils savent comment gérer leur partie de l'opération. Nous sommes des parlementaires, nous ne comprenons donc pas nécessairement leur raisonnement, mais pour moi, cela n'a aucun sens. N'essayez pas de me protéger. Je peux me protéger moi-même, mais je dois savoir s'il existe une menace sérieuse. Je veux savoir. Cela ne changera probablement pas grand-chose, mais je veux savoir si c'est sérieux.

Je ne vois pas pourquoi on ne communiquerait pas cette information.

Mme Lindsay Mathyssen: En ce qui concerne la question de M. Hardie, je m'inquiète pour... Je ne suis pas d'un côté ou de l'autre de la question de savoir si nous devons divulguer les noms ou non. Le problème que je vois, c'est ce tribunal de l'opinion publique. Nous occupons des fonctions très publiques, comme nous venons de le dire.

Quel effet cela a-t-il sur un parlementaire? Selon moi, le renseignement n'est pas toujours synonyme de preuve. Pour cette enquête, comment pouvons-nous permettre que cela se produise, si je peux fusionner les deux questions?

● (1300)

Mme Stephanie Kusie: Nous devons réparer le système. Si le renseignement n'est pas une preuve, c'est un vrai problème, un problème sérieux.

Cela nous ramène à mon point de départ, c'est-à-dire à ce que je perçois comme étant de la naïveté et à la nécessité de réorganiser l'ensemble du système. Comme je l'ai dit, je crois que c'est le résultat de la naïveté. Je pense que c'est le résultat de l'indifférence, de l'inaction et de l'incompétence.

Il ne devrait pas en être ainsi. Nous devrions pouvoir nous fier au contenu du rapport. C'est un problème de taille. J'espère vraiment — qu'il s'agisse de ce gouvernement ou d'un autre — que ce problème pourra être résolu afin que nous puissions avoir confiance dans ce qui est publié.

Si ce n'est pas le cas, qu'est-ce que cela dit de nous en tant que nation? Que nous ne pouvons même pas avoir confiance dans les renseignements contenus dans ce qui est censé être le rapport le plus solide et le plus sensible? Je pense que c'est un bien triste constat. J'espère un jour vivre dans un État où nous pourrons prêter confiance à un rapport de cette importance et aux renseignements qui y figurent.

Merci.

Le président: C'est tout le temps que vous aviez, madame Mathyssen.

Monsieur Kmiec, si vous avez une courte réponse, vous pouvez y aller.

M. Tom Kmiec: Merci, monsieur le président.

Ma seule réponse serait de revenir au tout début de ma déclaration et à ce que j'ai dit à la Chambre des communes. Le gouvernement du Canada, lorsqu'il traite avec les législateurs, a la responsabilité objective de nous informer. Nous avions besoin de savoir. Or, il avait la responsabilité morale et éthique de nous informer et il a échoué.

Le président: Merci beaucoup.

Monsieur Kmiec, madame Kusie et madame Sgro, merci beaucoup de vous être joints à nous aujourd'hui. Nous apprécions beaucoup vos réflexions.

Chers collègues, je pense que nous avons eu une nouvelle série de réunions très productives et très instructives. Je vous remercie de votre coopération.

La séance est levée.