Le 23 juin 2020, le Comité permanent de la procédure et des affaires de la Chambre a adopté la motion suivante :

> *Il est convenu, - Que les transcriptions à huis clos des réunions tenues les 28 mai et 2 juin 2020 soient communiquées par le greffier du comité au dirigeant principal de l'information de l'administration de la Chambre des communes et à tout autre fonctionnaire jugé approprié ; et, que le dirigeant principal de l'information fournisse au comité, au plus tard le 3 juillet 2020, les transcriptions à huis clos recommandées concernant la sécurité nationale.*

Le 7 juillet 2020, le comité a accepté les expurgations suggérées par le directeur de l'information de la Chambre des Communes, en adoptant la motion suivante :

> *Il est convenu, - Que les sections spécifiées des transcriptions des débats à huis clos pour les réunions du comité du 28 mai et du 2 juin 2020 soient rendues publiques en tant que témoignages du comité, à condition que les expurgations convenues soient faites.*

Les témoignages expurgés de certaines parties de la réunion à huis clos du 2 juin 2020 figurent ci-dessous.

****

Standing Committee on Procedure and House Affairs

Comité permanent de la procédure et des affaires de la Chambre

UNEDITED, TRANSLATED EVIDENCE NUMBER 19,
TÉMOIGNAGES DU COMITÉ NUMÉRO 19, TRADUIT, NON ÉDITÉ

PARTIE À HUIS CLOS SEULEMENT - IN CAMERA PART ONLY

Tuesday, June 2, 2020 - Le mardi 2 juin 2020

* * *

(1230)

[*Traduction*]

La présidente: Merci beaucoup.

Je pense que si nous le faisons encore quelques fois, nous pourrons probablement gagner du temps une fois que tout le monde connaîtra la procédure.

Pour la deuxième partie de la réunion, nous accueillons M. Jones, du Centre de la sécurité des télécommunications. Bienvenue, monsieur Jones.

Les fonctionnaires de l'équipe d'administration de la Chambre sont toujours parmi nous: M. Patrice, M. Robert, M. Gagnon, M. Aubé et M. Dufresne. Merci de vous joindre à nous pour la deuxième partie de la réunion. Je suis certaine qu'il y aura beaucoup de questions intéressantes pendant la discussion.

En principe, ce n'est pas vraiment un autre groupe de témoins. Nous ne faisons que poursuivre la séance, mais nous devons siéger à huis clos. Nous avions initialement décidé de continuer par des séries de questions de cinq minutes, mais je crois que je vais vous proposer de reprendre au début des séries de questions. Je parle comme si c'était un nouveau groupe de témoins alors que nous n'en avons ajouté qu'un. À vrai dire, c'est tout simplement une séance de trois heures en compagnie d'un seul groupe de témoins.

Voulez-vous commencer par la série de questions de cinq minutes ou celle de six minutes?

Mme Rachel Blaney : Madame la présidente, j'aimerais commencer par la série de questions de six minutes. Je ne veux certainement pas n'avoir que deux minutes et demie.

La présidente: C'est ce que je pensais. Bien.

Je n'ai pas vraiment de liste précise des intervenants puisque nous commençons de cette façon. Qui aimerait commencer les questions du côté des conservateurs?

Monsieur Tochor, je vous en prie. Vous avez six minutes.

M. Corey Tochor: Merci de vous être joint à nous, monsieur Jones.

Du point de vue de la technologie et de la sécurité, que pouvons-nous ajouter au système pour repérer les erreurs ou la fraude? D'après vous, que pouvons-nous faire?

M. Scott Jones (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications) : Je suis désolé. Je ne suis pas certain d'avoir bien compris la question concernant la fraude. Parlez-vous d'usurpation d'identité?

M. Corey Tochor: Cela pourrait être fait de dizaines de façons. Quelle serait votre solution en cas de fraude, par exemple si des acteurs étrangers douteux s'en prenaient à notre démocratie, voire des partisans, des partis organisés ou tout simplement des partisans dans la population qui voudraient porter atteinte au droit d'un député de voter d'une façon ou d'une autre.

(1235)

M. Scott Jones: Je comprends. Merci.

C'est un des domaines dans lesquels nous travaillons avec M. Aubé et son équipe pour comprendre les différentes menaces, et on conçoit ensuite un mécanisme de sécurité pour faire face à ces menaces en adoptant une position défensive à plusieurs niveaux. Dans le cadre d'un partenariat de longue date avec la Chambre des communes, nous nous penchons sur la conception – nous collaborons avec la Chambre qui conçoit les solutions et nous réglons ensemble les questions de sécurité – et nous nous efforçons aussi de mettre en place une série complète de protections jusque dans l'application.

En réalité, ce que nous faisons, c'est chercher les différentes menaces, et nous veillons ensuite à avoir des moyens d'y faire face.

M. Corey Tochor: Mais que se produirait-il si une menace se concrétise?

M. Scott Jones: **********
****
****
****
****
**********.

M. Corey Tochor: **********
*****.

M. Scott Jones: **********
****
****
****
****
****
**********.

M. Corey Tochor: Pour pousser un peu plus le raisonnement – peut-être pas sur le plan technique –, on sait que, dans les faits, des pressions sont exercées en prévision des votes. Disons qu'un vote a été très serré et qu'on exerce ensuite des pressions sur des députés pour les faire voter autrement en invoquant un problème technique, une erreur au moment du vote. Vous trouveriez alors des lacunes dans cette politique ou des problèmes dans notre démocratie puisque des pressions injustifiées seraient exercées sur des personnes dans le but de les refaire voter autrement sous prétexte que c'était une erreur ou qu'un acteur étranger a infiltré notre système.

Partout dans le monde, il y a eu des exemples de différents problèmes technologiques dans des assemblées législatives virtuelles ou dans le cadre de votes virtuels. Êtes-vous au courant d'attaques contre notre Parlement virtuel, qui n'en est qu'à ses balbutiements?

M. Scott Jones: Je n'ai pas entendu parler de la moindre attaque contre le Parlement virtuel. Ce que nous faisons notamment depuis le début, entre autres choses essentielles, c'est concevoir la structure de sécurité. Quand il s'agit de choses comme les votes, je ne peux pas parler des contrôles procéduraux que la Chambre utilise pour veiller à ce que chaque député ait droit à un vote, mais d'un point de vue technologique, le chiffrement signifie sans aucun doute qu'on peut structurer la chose de manière à savoir que c'est bien tel ou tel député qui a voté.

C'est le même concept que nous utilisons lorsque, par exemple, nous signons des documents numériques. À l'heure actuelle, ** ** signe le document, car c'est ainsi que nous avons configuré les choses.

Le concept utilisé pour les votes est similaire.

M. Corey Tochor: Un peu comme chaque fois qu'on veut protéger quelque chose, si on dresse une clôture haute, les criminels se serviront tout simplement d'une échelle plus grande, et je n'ai donc toujours pas confiance. Quand il est question de notre façon de voter au Canada, nous parlons d'une tradition qui remonte à plus de 150 ans, et je ne suis pas convaincu qu'une solution technologique remplacera cette façon de procéder à temps.

De façon générale, les gens sont inquiets par rapport à l'objet de notre discussion, mais sur le plan technologique, quelle est la faille la plus facile à exploiter pour un mauvais acteur?

(1240)

M. Scott Jones: Si le contexte était différent, il est certain que ce que la plupart des acteurs exploiteraient serait tout simplement un périmètre de sécurité relâché, des correctifs qui manquent de rigueur et ainsi de suite.

** ** ** ** ** ** **.

** *** *** ** *** *******************.

On continue d'ajouter des niveaux de protection pour atténuer le risque jusqu'à ce qu'on se sente à l'aise avec le risque résiduel.

M. Corey Tochor: J'ai une brève question sur la biométrie…

La présidente : Votre temps est malheureusement écoulé, monsieur Tochor. Désolé.

C'est maintenant au tour de M. Turnbull.

M. Ryan Turnbull (Whitby, Lib.): Merci, madame la présidente.

Je remercie tous les témoins de s'être joints à nous. Je tiens notamment à remercier M. Aubé et M. Jones.

Je sais que, d'après les observations de la présidence, nous semblons avoir surmonté beaucoup de problèmes en vue de tenir des délibérations hybrides. Je tiens à dire que je trouve cela très rassurant, tout comme tout le bon travail que vous accomplissez à cette fin.

Je veux aborder trois thèmes dans mes questions. Tout d'abord, monsieur Aubé, vous avez parlé de la façon dont la plateforme Zoom ********** **********. Je trouve cela très rassurant.

Ce que je voulais demander à M. Jones, si c'est possible, c'est à quel point ********** **********est sécurisé? Je suis désolé; je ne suis pas technicien et j'emploie vaguement les termes. Je vous prie donc de ne pas hésiter à me corriger si j'en ai mal utilisé certains.

********** **********.

Pouvez-vous parler des protocoles de données et des données liées à cette plateforme?

M. Scott Jones: Absolument. Je suis certain que M. Aubé peut probablement donner plus détails. Lorsque nous examinons les mesures générales de sécurité en matière de TI pour protéger, par exemple, un centre de données, nous parlons de trois choses, des aspects liés à la sécurité physique, qui relèvent plus de la Chambre des communes – M. Aubé pourrait en parler. Il est toutefois surtout question d'un partenariat à long terme entre les services de TI et la Chambre des communes. Nous nous occupons ensemble de la sécurité. Le périmètre est très solide et renforcé en fonction de l'évolution du domaine de la cybersécurité, mais même pour ce qui est de la gestion des appareils que tout le monde reçoit, je sais que les contrôles en place font en sorte que la Chambre des communes figure parmi les meilleures organisations, y compris celles du secteur privé, sur le plan de la sécurité des TI.

M. Ryan Turnbull: Merci.

J'imagine, monsieur Aubé, que vous voulez peut-être en parler vous aussi.

Vous évaluez périodiquement les risques et vous avez un plan de gestion connexe. Vous examinez tous les risques possibles, et vous vous penchez ensuite, comme l'a dit M. Jones, sur une approche à plusieurs niveaux. Pour moi, ces mesures font en sorte qu'il est très peu probable qu'un acteur malveillant déjoue notre système de sécurité. Pouvez-vous parler un peu plus de cette approche à plusieurs niveaux? Quels sont les niveaux?

M. Stéphan Aubé (dirigeant principal de l'information, Services numériques et biens immobiliers, Chambre des communes): Merci, madame la présidente.

Merci de poser la question, monsieur Turnbull.

Comme l'a dit M. Jones, pour nous, la sécurité à la Chambre des communes commence par les terminaux, par les utilisateurs finaux. Nous sommes très fiers de la façon dont nous sécurisons les terminaux. Nous tentons de rendre plus sûre la façon dont tous les députés contribuent à sécuriser le système. Nous imposons l'utilisation d'appareils gérés par la Chambre, pour que nous ayons les contrôles et le chiffrement nécessaires au transfert de données entre ces appareils et au sein de notre infrastructure.

Nous avons aussi une stratégie de surveillance. **********
****
****
****
****
****
****
****
****
**********.

(1245)

M. Ryan Turnbull: Merci de la réponse.

Combien y a-t-il eu d'atteintes à la sécurité depuis que le Parlement a commencé à siéger virtuellement?

M. Stéphan Aubé: Dans le contexte des séances virtuelles, il n'y en a eu aucune, monsieur.

M. Ryan Turnbull: Aucune. Bien. Merci.

La menace a toujours été là, mais personne ne s'est introduit dans notre système jusqu'à maintenant.

M. Stéphan Aubé: Pas à notre connaissance, et nous faisons sans aucun doute beaucoup de surveillance tous les jours.

M. Ryan Turnbull: Merci de faire ce travail. Cela me rassure, et je suis certain que c'est la même chose pour tout le monde ici.

Une autre chose. Je sais que le Royaume-Uni a mis au point un compte MemberHub pour voter à distance, et qu'il a recours à une identification multifactorielle. Je me demande, M. Jones ou M. Aubé – peu importe qui est le mieux placé pour répondre –, comment nous allons vérifier l'identité, d'un terminal à l'autre, des personnes qui pourraient voter à l'avenir.

M. Stéphan Aubé: Je peux en parler.

Nous sommes certainement au courant de ce que le Royaume-Uni fait dans le cadre de notre partenariat international. Nous sommes penchés là-dessus, monsieur. Cela dit, notre stratégie comprend 10 étapes pour sécuriser l'infrastructure.

Nous mettons l'accent sur la première partie, soit les avis. Nous devons faire en sorte que tout le monde est avisé et que les avis sont sûrs, c'est-à-dire entre la Chambre et les députés. C'est la première étape, monsieur.

La deuxième est l'identification des députés. L'accès à ces activités sera limité aux seuls députés et seulement à ceux **********, monsieur, et **********, d'autres mesures d'identification seront prises pour confirmer à 100 % ou à presque 100 % qu'une personne participe à la réunion, monsieur.

Nous allons aussi nous pencher sur le mécanisme de communication de toute l'information entre les terminaux. Nous assurons donc la sécurité, comme en a parlé M. Jones, au moyen du chiffrement entre les terminaux utilisés, et ce, jusqu'à notre centre de données.

Nous nous penchons aussi sur l'enregistrement et l'archivage des résultats pour faire en sorte que personne ne peut les modifier, monsieur.

Nous examinons également la procédure de vote, car au-delà du vote, il faut confirmer que la personne a voté, et nous devons donc chercher des moyens grâce à différents canaux – par exemple, au Royaume-Uni, une confirmation de vote chiffrée était transmise lorsque les députés votaient. C'est ainsi qu'on a procédé. Nous examinons et nous évaluons actuellement ces façons de faire en compagnie de nos homologues du CST.

Nous nous penchons aussi sur la publication des résultats…

La présidente: C'est malheureusement tout le temps que nous avions, monsieur Aubé.

M. Ryan Turnbull: Merci, monsieur Aubé.

La présidente: Merci.

C'est maintenant au tour de Mme Normandin.

[Translation]

Mme Christine Normandin: Merci beaucoup, madame la présidente.

Encore une fois, merci de votre présence.

Un peu comme mon collègue, M. Turnbull, je ne suis pas non plus très texte à vie. J'ose espérer que vous me corrigerez si jamais je disais des âneries.

Ma première question concerne l'identification visuelle. Un peu comme l'on vient de le faire avec le Comité. Jusqu'à quel point peut-il y avoir une menace par le biais de logiciels comme *Deepfake*? Est-ce une chose à considérer ou est-ce un peu farfelu que cela puisse être fait?

M. Stéphan Aubé: Dans le contexte de l'architecture que l'on a faite jusqu'à maintenant, c'est presque impossible que ces choses-là arrivent. Je dis toujours presque parce qu'il y a toujours un élément de risques dans tout ce que l'on fait, mais pour l'architecture que nous mettons en place, nous voulons nous assurer à 100 % que nous sommes capables d'identifier la personne qui participe à la rencontre et la personne qui, si on faisait un vote suite à votre demande, serait la bonne personne qui voterait aussi.

Mme Christine Normandin: Parfait.

Juste pour être sûre si j'ai bien compris. Par exemple, s'il y a un vote, l'authentification de la personne qui vote se ferait à plusieurs moments précis dans le temps. Cela fait partie des règles de sécurité que vous mettriez à la base. Au moment où le membre se présente, ensuite au moment où il vote et, après coup, une troisième fois pour s'assurer qu'on a la bonne personne.

M. Stéphan Aubé: Oui, je vous dirais que l'on commence même avant cela, c'est-à-dire au moment **********. Ce seraient des éléments qui valideraient l'identité de la personne.

(1250)

Mme Christine Normandin: Super.

On sait parfois que, lorsqu'il y a des votes soudainement, il y a une personne à la salle de bains parce qu'elle n'a pas le goût de voter sur un sujet quelconque. Si un membre arrivait en disant qu'il a eu un problème technique et qu'il n'a pas pu voter. S'il y a effectivement eu un problème de connexion Internet ou qu'un membre dit qu'il n'a pas pu exercer son droit de vote, le service informatique pourrait-il valider cette information par exemple si l'information est vraie?

M. Stéphan Aubé: Quand je parlais plus tôt à M. Turnbull, je regardais la liste des choses dont on parlait, mais une des choses que je n'ai pas mentionnée avant est toute la composante de l'audit du système.

On parlait des transactions possibles, et aussi de la réception des messages entre nous et le député. On va conserver une trace de toutes ces choses pour pouvoir bien valider que c'est bien la personne et qu'elle a pu participer.

S'il y a une chose qui arrive, on sera au courant. Par exemple, comme vous nous avez posé une question plus tôt [*inaudible*], sait-on combien de personnes sont déconnectées durant l'événement? Mais sur ce genre de trace que l'on garde actuellement pour essayer de travailler avec les gens après les rencontres pour améliorer le système. En même temps, cela va nous servir à valider que les résultats sont bien les bons.

Mme Christine Normandin: D'accord.

Par rapport à cela, on pourrait voir quel genre de problème il peut avoir eu. Est-ce le membre lui-même qui a décidé de se déconnecter parce qu'il ne souhaitait pas voter ou si c'est vraiment un problème technique qui a eu lieu? Il y aurait vraiment le moyen de le savoir.

M. Stéphan Aubé: Oui, c'est notre intention.

Comme idée, la première étape qu'on pourrait valider serait de savoir s'il y a reçu la notification de vote. Sur quel appareil l'a-t-il reçu? Sur sa tablette ou sur son téléphone? L'a-t-il lut en plus de cela pour compléter la deuxième étape.

Ensuite, a-t-il exercé son vote et quel est le résultat? Toutes ces choses seraient faites de façon sécuritaire dans le but de s'assurer qu'elles ne sont pas modifiées. On ne pourrait pas valider vraiment ce qui s'est passé.

Mme Christine Normandin: Merci.

Par rapport au choix de la plateforme qui va être utilisée pour le vote par exemple et le fait de passer cette information aux partis qui auront donc leur mot à dire, la façon dont vous allez établir le protocole pour expliquer aux membres quelle sera la plateforme, pour voir avec eux les recommandations et s'ils sont à l'aise ou pas, est-elle déjà prévue? Y a-t-il une chose déjà mise en place?

M. Stéphan Aubé: Actuellement, la façon dont on travaille est qu'on essaie de se positionner pour pouvoir avoir une infrastructure flexible pour répondre aux besoins des différents partis. C'est un premier résultat.

La deuxième chose est qu'on essaie d'utiliser des outils qu'on a déjà maintenant. Notre approche est de pouvoir utiliser des outils disponibles pour créer cette plateforme.

Par contre, dans le contexte appelé l'interface d'utilisateur, on s'assure que cela soit facile à utiliser. Ce serait des choses sur lesquelles on pourrait travailler avec un ensemble de députés pour pouvoir s'assurer qu'on ait la rétroaction nécessaire afin de la rendre plus facile possible.

Là, notre premier objectif est de s'assurer qu'on est capable de le faire de façon sécuritaire pour ensuite travailler avec vous pour s'assurer que l'aspect interface utilisateur rencontre les besoins. On veut rendre cela le moins complexe possible.

Mme Christine Normandin: Super.

J'ai une dernière question sur l'éventualité d'incidents futurs. Y a-t-il déjà un protocole mis en place pour savoir comment vous allez communiquer ces incidents? À qui cela sera-t-il communiqué? Est-ce à un service de la Chambre ou directement aux différents partis? Qui va recevoir cette information?

M. Stéphan Aubé: En ce qui concerne le vote, on n'a pas encore défini le protocole parce qu'on n'a pas reçu la demande officielle. Si on avait la demande officielle, il y aurait un protocole.

- Je vais vous donner l'exemple où il se produit un incident de sécurité à la Chambre. Si un incident de sécurité est découvert par notre équipe, à l'intérieur de la Chambre, **********
****
****
****
****
****
****
**********.

Dans le contexte où il s'agit d'un incident à l'extérieur de la Chambre, **********
****
****
****
****
****
****
****
**********.

(1255)

[Traduction]

La présidente: Je vous remercie, monsieur Aubé.

C’est maintenant Mme Blaney qui interviendra.

Mme Rachel Blaney: Je vous remercie.

Je pense que notre séance a été fort instructive jusqu'à présent et qu'il est toujours important de souligner l'excellent travail de tous ceux qui travaillent à maints égards pour s'adapter à la COVID-19. Je voudrais profiter de l'occasion pour vous remercier tous.

Je m'adresserai d'abord à M. Aubé. Vous avez commencé à énumérer 10 mesures que vous prenez. Je me demande si vous pouvez remettre cette liste de six mesures au Comité.

M. Stéphan Aubé: Oui, nous le pouvons.

Mme Rachel Blaney: Je vous remercie. Cette liste nous serait extrêmement utile.

Je suppose que ma question est la suivante. Un des points qui nous préoccupent le plus lorsque nous intervenons, c'est d'abord le fait que nous ne voulons pas remplacer le travail qui devrait être accompli à Ottawa, mais nous nous trouvons dans une situation qui nous oblige à faire les choses autrement. Je pense que la plupart d'entre nous le comprennent.

Je me demande si vous pourriez nous en dire un peu plus sur les modes de vote virtuel qui ont été envisagés et nous dire si nous devrions être au fait de certains problèmes de sécurité.

M. Stéphan Aubé: Je peux répondre à la première question, madame Blaney.

Il existe une panoplie de systèmes de vote, mais je tiens à circonscrire mon propos. Il n'est pas question ici d'un régime électoral, mais plutôt de séances ou de réunions s'apparentant à celles d'un conseil d'administration au sein d'une organisation précise. Vous constaterez qu'il existe un large éventail de systèmes de vote qui, par exemple, peuvent être utilisés pour tenir un vote par appel nominal, dans le cadre duquel chaque député est nommé et doit exprimer son vote. Ce serait l'exemple le plus simple possible.

Il faudrait aussi pouvoir voter à l'aide d'un système à la Chambre, comme quelqu'un l'a fait remarquer. J'ignore si les gens le savent, mais quand nous avons modernisé le système audio pour la dernière fois il y a 12 ans, nous avions prévu une fonction permettant de voter à la Chambre. Les câbles et les infrastructures étaient déjà installés dans l'édifice du Centre. Au consulat, nous prévoyions à un moment de pouvoir [*Inaudible*]. Il existe donc de tels systèmes de vote spécialisés intégrés.

En outre, pour les systèmes audios installés dans les salles de séance des comités, la plupart des fournisseurs comme Bosch ou Televic offrent habituellement d'y intégrer des capacités de vote.

Puis, l'an dernier, la technologie a réellement évolué. Les votes s'effectuent de plus en plus au moyen d'infrastructures mobiles, ce qui permet de tirer parti du coût de la mobilité pour voter.

Voilà ce qu'on pourrait appeler le spectre des systèmes de vote qui existent. L'approche dont nous parlons ici est plus complexe, car il s'agit d'un système de vote entièrement mobile. Si une personne qui n'est pas présente lors d'une séance est en mesure de voter, c'est ce que j'appelle

une infrastructure mobile. Ce sont là les 10 mesures que nous examinons pour le concept des systèmes de vote.

Cela étant dit, si vous vous intéressez principalement à un système de vote normal permettant de participer par vidéo, ce serait beaucoup plus simple. Il s'agirait d'utiliser essentiellement l'équipement dont vous disposez actuellement et d'étudier les procédures à utiliser pour pouvoir voter.

Nous examinons les divers modes de vote, ********** ********** ********** ********** ********** ********** ********** ********** ********** **********, lequel permet de tirer parti d'un environnement mobile qui est légèrement plus souple, mais qui est plus complexe et qui exige des échanges quotidiens avec nos partenaires du domaine de la sécurité.

Mme Rachel Blaney: Je vous remercie beaucoup de cette réponse.

Je pense, pour ma part, que le vote par vidéo atténue certaines des préoccupations que les députés ont à propos de l'identification, puisque nous pouvons voir la personne dire « oui » par vidéo. Je pense à ce qui s'est passé plus tôt au cours de la séance, quand on a pu voir les membres du personnel et vérifier de qui il s'agit. Je pense que c'est très important.

J'ai toutefois quelques interrogations. Je me demande d'abord si vous considérez que nous devrions envisager de commencer par le vote par vidéo. Si nous options pour cette solution, quel en serait le coût? Je présume que si nous utilisions la technologie déjà en place, l'investissement est déjà fait. Si nous agissons comme vous le proposez, quels seraient les coûts et comment pourrions-nous comprendre ce qu'il en est?

M. Stéphan Aubé: Je commencerai par le coût de l'option. Nous sommes d'avis que nous tirerions parti des investissements existants, de notre infrastructure de TI et de nos propres ressources ********** afin d'implanter toutes les solutions que vous voulez. Selon nous, nous pourrons mettre en œuvre toutes les solutions que vous demanderez avec des investissements minimaux à la Chambre parce que vous avez déjà l'infrastructure mobile nécessaire et que vous bénéficiez déjà d'une équipe de soutien **********. Toutes ces ressources n'entraînent aucuns frais supplémentaires pour l'instant. Les systèmes que nous entendons utiliser existent déjà à la Chambre des communes. Voilà en quoi consiste notre approche.

Si on utilise l'envoi de messages à titre d'exemple, nous espérons exploiter les outils existants, **********, une application mobile sécurisée figurant dans notre portefeuille d'applications que nous utiliserions pour aviser les députés. Cela n'entraînerait aucuns frais supplémentaires, car cette application existe déjà à la Chambre des communes.

Ce sont là les genres d'outils que nous envisageons d'utiliser, à un coût minimal. Le coût est un critère depuis le début de la pandémie. Nous voulons utiliser les outils dont nous disposons avant de dépenser de nouveaux fonds pour quelque chose d'autre.

(1300)

Mme Rachel Blaney: Je vous remercie de ces précisions. Je sais que les ordinateurs, les tablettes et les téléphones des députés sont dotés de fonctions biométriques. Je me demande si nous devrions penser à autre chose au chapitre de la sécurité.

M. Stéphan Aubé: Dans le cas des votes, nous discutons de la question avec ********. Je ne dirais pas que nous incluons ou excluons la biométrie. Nous n'en sommes pas là pour le moment. Nous voulons seulement nous assurer que les outils sont sécuritaires et peuvent combler tous les besoins. Si les fonctions biométriques s'avèrent nécessaires, nous les recommanderons au Comité, madame Blaney.

La présidente: Je vous remercie, monsieur Aubé.

Maintenant, pour les conservateurs, qui avons-nous? Est-ce M. Genuis?

Monsieur Doherty, vous avez la parole.

M. Todd Doherty: Je vous remercie, madame la présidente.

Ma question s'adresse à M. Jones et à M. Aubé, et concerne la plateforme Zoom proprement dite.

La sécurité et de la protection des renseignements personnels nous préoccupent-elles sur cette plateforme? Avons-nous conclu une entente officielle avec Zoom?

M. Stéphan Aubé: Je commencerai à répondre à cette question, madame la présidente.

Je vous remercie de poser cette question. Nous avons signé une entente avec Zoom lors de l'achat initial d'une licence de trois mois, monsieur. Là se limite l'entente que nous avons conclue. Comme je l'ai souligné en public, le coût mensuel que nous payons pour utiliser Zoom à huis clos ou en public est le même et s'élève encore à 3 000 $ actuellement, conformément à l'entente actuelle. Nous envisageons…

M. Todd Doherty: C'est très raisonnable.

M. Stéphan Aubé: En effet. C'est un des facteurs qui expliquent la raison pour laquelle nous nous sommes intéressés à cette solution, puisque nous souhaitions acheter à moindre coût.

Pour toute autre collaboration sur la Colline, nous préconisons d'autres approches, comme Microsoft teams, puisqu'ici encore, nous avons des contrats de licence à cette fin.

M. Todd Doherty: Dans des circonstances normales, nous savons que des acteurs étrangers cherchent quotidiennement à pirater nos systèmes. Je pense que vous avez répondu à la question de M. Turnbull en indiquant qu'à votre connaissance, il n'y avait eu aucun cas de piratage potentiel. Mais pas plus tard qu'en mars, des États ont lancé avec éclat des enquêtes sur les pratiques de Zoom en matière de protection des renseignements personnels et de sécurité. La

question nous préoccupe-t-elle, notamment au chapitre des politiques d'échange de données? Savez-vous si Zoom effectue du chiffrement de bout en bout?

M. Stéphan Aubé: Les séances publiques se déroulent sur l'infrastructure de Zoom, je tiens à le préciser. Je pense que vous n'avez pas assisté à la dernière séance lorsque je l'ai expliqué.

Pour nous, du point de vue de l'évaluation des risques, nous considérons qu'il s'échange très peu de renseignements sur les participants aux séances publiques tenues sur Zoom. C'est l'infrastructure de la Chambre qui est utilisée pour vérifier l'identité des utilisateurs. Nous ne leur demandons pas de créer un compte sur Zoom, utilisant plutôt les comptes de la Chambre. Ainsi, très peu d'informations sont communiquées à Zoom.

****
****
****
**********.

Seules des mégadonnées sont échangées entre la Chambre et Zoom. Il peut s'agir, par exemple, d'une confirmation indiquant qu'une personne a été authentifiée par la Chambre et sera autorisée à participer à la séance. Nous communiquons aussi la date et l'heure des séances, car le contrat de licence l'exige, mais c'est à peu près tout ce que nous communiquons à Zoom afin de régler les questions de nature délicate pour les séances.

(1305)

M. Todd Doherty: Comment pourrait-on éviter que des députés ne communiquent leur mot de passe au bureau du whip afin de voter?

M. Stéphan Aubé: Il existe diverses manières d'envisager l'authentification des personnes dans le contexte d'un vote. Comme je l'ai souligné, si nous empruntons cette approche, nous voudrions **********. C'est une autre solution que nous étudierons afin **********.

De plus, j'espère que les députés n'enfreindront pas la politique de la Chambre en communiquant le mot de passe personnel de leur compte à d'autres parties. C'est une autre précaution à prendre.

Nous envisageons aussi d'utiliser les données biométriques lors du processus de vote afin de nous assurer que c'est bien la personne concernée qui a pressé le bouton. Nous pourrions peut-être même capter une image de cette personne pour la comparer avec une photo existante, une photo publique que nous avons des députés. Je ne dis pas que c'est ce que nous ferons, mais nous envisageons divers mécanismes pour vérifier que c'est bien la personne concernée qui vote. S'il y a un risque, **********
**********.

M. Todd Doherty: Le risque que nos séances publiques sur Zoom soient infiltrées vous préoccupe-t-il?

La présidente: C'est tout le temps que nous avons, à moins que vous puissiez répondre en 10 secondes.

M. Stéphan Aubé: Je suis certain à 99,9 % que cela ne nous arrivera pas, à moins que quelqu'un ne fasse… [*inaudible*]. Il est plus risqué d'employer d'autres outils que celui que nous utilisons actuellement, compte tenu de la manière dont il a été configuré.

La présidente: Je vous remercie.

Monsieur Gerretsen, la parole est à vous.

M. Mark Gerretsen: Je vous remercie, madame la présidente.

Monsieur Aubé, j'ai une brève question. Il a été beaucoup question de la reconnaissance faciale et des images de gens que l'on voit. L'hypertrucage suscitant de plus en plus de préoccupations, n'est-il pas de plus en plus possible de modifier l'image des gens pour qu'ils ressemblent à quelqu'un, alors que ce n'est pas eux?

Quelle est votre méthode d'authentification préférée? Est-ce la biométrie ou quelque chose de plus fiable, de plus authentique ou de plus difficile à modifier?

M. Stéphan Aubé: Monsieur Gerretsen, je répondrai brièvement que c'est l'authentification multifactorielle, qui ne repose pas sur un seul facteur pour prévenir l'usurpation d'identité. Je commencerais par vous demander de voter et confirmerais votre identité en m'assurant qu'il s'agit bien de votre compte et de votre machine, mais je pourrais peut-être aussi vous envoyer une confirmation selon laquelle vous venez de voter en utilisant un ou deux autres mécanismes. Je pourrais vous faire parvenir un courriel pour vérifier que vous avez bien reçu le message et peut-être vous envoyer un message chiffré avec un outil différent pour m'assurer que vous l'avez bien reçu.

L'authentification multifactorielle permet mieux de vérifier l'identité qu'une seule approche.

M. Mark Gerretsen: Vous avez aussi indiqué que l'utilisation ********** pourrait empêcher le bureau du whip de voter à la place de quelqu'un. Ne craignez-vous pas qu'un bureau de whip, qui dispose de 60 ou 70 ordinateurs, puisse voter pour tout le monde?

M. Stéphan Aubé: J'espère que cela ne se produit pas, monsieur.

M. Mark Gerretsen: Je pense que l'intégrité de chaque député empêcherait pareille chose de survenir.

Je céderai le reste de mon temps à M. Turnbull, madame la présidente.

La présidente: Vous avez la parole, monsieur Turnbull.

M. Ryan Turnbull: Je vous remercie, monsieur Gerretsen.

La personne qui a présenté l'exposé a indiqué que l'équipe technique a élaboré une solution conceptuelle qui, selon ce que j'ai compris, utiliserait des outils existants, notamment des mesures de sécurité qui pourraient déjà être utilisées dans le cadre des activités quotidiennes de la Chambre.

Pourriez-vous nous décrire cette solution un peu plus en détail et peut-être expliquer clairement à quel point elle serait facile à mettre en œuvre?

🕐 (1310)

M. Stéphan Aubé: D'accord, monsieur Turnbull et madame la présidente. Je vous remercie de me poser la question.

Du point de vue conceptuel, monsieur Turnbull, nous pensons d'abord utiliser le système d'avis de vote de la Chambre et envoyer un message aux multiples appareils des députés pour les avertir de la tenue d'un vote. ** ** ** **.

C'est le premier processus. Vous le lanceriez de la même manière que vous faites retentir la sonnerie actuellement, mais l'avis serait aussi envoyé par voie électronique pour avertir les députés de la tenue d'un vote; nous envisageons la possibilité d'inclure la motion dans ce message. Vous verriez ainsi la motion qui est mise aux voix, dans la langue de votre choix. Ces outils seraient accessibles, et une fois que vous auriez lu le message, si vous voulez voter, nous vous dirigerions vers un portail sécurisé *****************, où vous seriez authentifié et où vous voteriez comme vous l'entendez.

Une fois que vous avez répondu par « oui », « non » ou « abstention », vous recevriez aussi une confirmation, monsieur. L'approche chiffrée multifactorielle [*Inaudible*] dont j'ai parlé, vous vous en souviendrez, valide votre identité à diverses étapes du processus. Ce serait une autre étape permettant de certifier que vous avez bel et bien envoyé un message, car vous avez reçu cette confirmation sur tous vos appareils et, sur celui que vous utilisez, vous pourriez confirmer que vous avez voté ou non. Si vous n'avez pas voté, un autre processus vous permettrait de signaler que quelqu'un d'autre utilise vos appareils. C'est un exemple que je vous donne, monsieur.

Nous enclencherions alors notre processus actuel de publication avec les outils dont nous disposons. Nous permettrions également le vote groupé et, comme je l'ai indiqué, nous avons des capacités en matière d'identité qui nous permettent de surveiller continuellement ce qu'il se passe, et ce, en utilisant le chiffrement pour nous assurer que la communication de messages, que ce soit lors du vote ou de l'avis, est chiffrée **********************. C'est essentiellement

l'approche que nous envisageons et dont nous discutons pour mettre en œuvre ces différentes mesures.

J'ajouterai enfin, puisque je n'ai pas eu l'occasion d'aborder le sujet, qu'il est très important de valider la chaîne d'approvisionnement. C'est un facteur qui doit être pris en compte. Si nous adoptons de nouveaux outils, nous devons savoir ce qui se trouve derrière afin de pouvoir suivre tous les changements et savoir comment ils sont effectués pour assurer la sécurité de l'outil.

La présidente: Je vous remercie, monsieur Aubé.

C'est maintenant M. Genuis, du Parti conservateur, qui prendra la parole. Merci.

M. Garnett Genuis: Je vous remercie beaucoup, madame la présidente.

Pourriez-vous nous fournir quelques explications pour faire la lumière sur la relation entre la plateforme technologique et la Chambre? La technologie est mise au point et exploitée par Zoom, mais vous affirmez que l'intervention de l'entreprise est minimale parce que ********** **********. Nous voyons tous Zoom en haut de notre fenêtre en ce moment même, mais certaines préoccupations ont fait surface par le passé, notamment sur le fait qu'on a appris après-coup que la technologie élaborée en Chine comportait des portes dérobées.

Aidez-moi à comprendre pourquoi vous ne semblez pas particulièrement inquiet dans le cas présent. Se peut-il que des renseignements puissent s'échanger au moyen de portes dérobées par une voie que vous ne voyez pas?

M. Stéphan Aubé: **********, je pourrais commencer à répondre, et vous pourriez étoffer ma réponse si vous le souhaitez.

********** **********
****
****
****
**********.

Le concept de porte dérobée que vous évoquez permet au logiciel de commencer à agir de lui-même pour ********** **********pour éviter que cela ne se produise. ********** **********.

M. Garnett Genuis : Si [*Inaudible*] une brève question de suivi pour commencer, vous avez dit que **********. Il semble y avoir un seuil sous **********. Est-ce exact?

M. Stéphan Aubé : Ce n'est pas comme cela que je l'expliquerais, monsieur. ********** **********. Il n'est pas seulement question de la

****
**********.

(1315)

M. Garnett Genuis : D'accord. Je ne veux pas vous mettre de mots dans la bouche; j'essaie simplement de comprendre ce que vous avez dit. Vous dites…

M. Stéphan Aubé : Je voulais donner un exemple, monsieur. Permettez-moi de me corriger.
****
**********.

M. Garnett Genuis : Il me semble que **********
*** serait une opération de faible envergure. Il est beaucoup plus probable que quelqu'un ***
**********.

****
****
****
****
****
**********. Est-ce exact? C'est ce que vous semblez dire.

M. Stéphan Aubé : Je ne dirais pas cela, monsieur Genuis, parce que nous avons en place de nombreux contrôles et nous effectuons un **********.

****
**********.

La deuxième chose, c'est que nous n'enregistrons pas les réunions. Ainsi, le contenu ne peut pas être utilisé à une date ultérieure. **********
****
*****.

M. Garnett Genuis : D'accord, si c'est vrai, alors c'est très bien. Je voulais simplement comprendre. Vous dites maintenant que **********
****
**********. Est-ce exact?

M. Stéphan Aubé : Tout à fait, monsieur.

M. Garnett Genuis : D'accord. Cela me semble différer de ce que vous avez dit au début, mais si c'est le cas, alors tant mieux. Je suis heureux d'avoir éclairci ce point.

M. Stéphan Aubé : Au moment de la discussion, nous étions centrés **********
**********.

M. Garnett Genuis : **********.

M. Stéphan Aubé : ********** **********.

M. Garnett Genuis : ********** **********.

M. Stéphan Aubé : **********.

La présidente : Nous n'avons plus de temps. Merci. Je vous ai accordé du temps pour cet échange et je suis heureuse que nous ayons pu répondre à cette question.

Madame Petitpas Taylor, vous avez la parole.

L'hon. Ginette Petitpas Taylor : Merci.

J'aimerais vous poser quelques courtes questions.

Monsieur Aubé, croyez-vous que les mesures de sécurité qui ont été mises en place nous permettent de tenir en toute sécurité des réunions hybrides et de procéder au vote à distance?

M. Stéphan Aubé : Je crois que nous pouvons assurer toute forme de participation à distance dans le cadre des séances. ********** **********.

L'hon. Ginette Petitpas Taylor : Merci.

Je crois vous avoir entendu dire plus tôt que les services sont hébergés dans l'infrastructure de la Chambre. C'est ce que j'ai compris.

M. Stéphan Aubé : C'est exact, pour les réunions à huis clos.

L'hon. Ginette Petitpas Taylor : Très bien. Quels contrôles de sécurité ont été mis en place à cette fin?

M. Stéphan Aubé : Comme je l'ai dit plus tôt, pour les réunions à huis clos, nous nous sommes surtout centrés sur les ********** ********** ********** ********** ********** **********.

Nous utilisons aussi ********** ********** ********** **********

**********.

(1320)

L'hon. Ginette Petitpas Taylor : J'aimerais vous poser une dernière petite question avant de céder la parole à M. Turnbull.

Quel est votre délai de réponse pour créer un correctif en cas d'infiltration du système?

Pouvez-vous nous répondre rapidement, s'il vous plaît?

M. Stéphan Aubé : Madame Petipas Taylor, j'essaie de comprendre la portée de votre question, à laquelle il est difficile de répondre. Tout dépend de l'infiltration.

Pour certains problèmes quotidiens, nous arrivons à trouver une solution en une heure; si le compte d'un député a été infiltré, par exemple. **********.
Nous effectuons une surveillance continue. **********.

C'est ce que je dis; tout dépend de l'ampleur du problème. Nous pouvons régler certains problèmes faciles instantanément. Il est difficile d'évaluer le temps nécessaire pour régler des problèmes plus graves qui toucheraient le centre. Cela étant dit, nous avons en place des mesures visant à tout arrêter de sorte qu'il n'y ait pas de fuite de renseignements. **********.

L'hon. Ginette Petitpas Taylor : Merci.

Monsieur Turnbull, je vous cède la parole.

M. Ryan Turnbull : J'aimerais vous poser une courte question.

En ce qui a trait à l'interférence dans le cadre du vote électronique, il semble que les mesures de sécurité en place rendent la chose très peu probable.

S'il y avait une forme d'interférence, est-ce que nous le saurions, monsieur Aubé, étant donné toutes les mesures de contrôle qui sont en place et que vous avez décrites?

M. Stéphan Aubé : Nous avons mis en place tous les outils nécessaires pour détecter l'interférence, monsieur Turnbull. C'est notre objectif.

Nous faisons preuve de diligence raisonnable et nous collaborons avec l'équipe de M. Jones pour détecter un tel problème. En cas d'interférence, nous pourrions trouver des façons pour permettre aux députés de maintenir leur participation à la séance.

M. Ryan Turnbull : Nous pourrions donc reprendre le vote, tout simplement?

M. Stéphan Aubé : Oui.

La présidente : Merci.

Nous n'avons plus de temps.

La présidente : Madame Normandin, vous avez la parole.

[Translation]

Mme Christine Normandin: Merci beaucoup.

Ma première question est sur l'utilisation de Zoom comme plateforme de vote en attendant qu'un système soit mis en place ou comme plan B advenant une faille technique ou un incident quelconque dans une autre plateforme et puis qu'on se rabatte sur Zoom comme plan B.

Quels seraient les principaux points négatifs à l'utilisation de Zoom comme plateforme de vote par appel nominal où la personne est identifiée et elle répond oui ou non et on passe à l'autre personne? En termes de temps, cela serait plus long que les 15 minutes qu'on a en Chambre. Avez-vous relevé des points négatifs?

M. Stéphan Aubé: Présentement, ce serait le choix des députés d'aller de l'avant avec cette méthode pour commencer, mais je demanderais à M. André Gagnon de répondre à cette question. Nous ne voyons pas d'enjeux techniques à le faire sauf que de prendre le temps nécessaire pour procéder au vote. Nous n'avons pas fait ces tests encore pour évaluer la durée de ce processus. Par contre, c'est quelque chose que nous allons examiner pour le faire de façon la plus efficace possible.

(1325)

Mme Christine Normandin: Je vois que le micro de M. Gagnon est allumé. Voulez-vous renchérir?

M. André Gagnon: À cause de Stéphan, je me sens obligé de répondre.

J'ajouterais que les deux méthodes auxquelles nous faisons référence ont chacune leur bon côté et leur mauvais côté. Le bon côté qu'aurait un vote auquel avait fait référence le président, c'est-à-dire que si on votait pendant que les cloches sonnent, les députés pourraient essentiellement voter de leur plateforme et, à partir des éléments qui sont devant eux, voter sur chacune des motions qui seraient présentes. Donc, il y a cette capacité de voter pendant la cloche de 30 minutes et même une capacité de voter sur différents items.

Comme vous le savez, à de nombreuses reprises, plusieurs votes ont lieu successivement, l'un après l'autre. Donc, cela serait une possibilité pour les députés de voter plus facilement sur les différentes motions. Aussi, ce serait sur une plus longue période. Donc, lorsque vient le moment de voter, s'il y avait des bris techniques, qui ne durent pas toujours 30 minutes, cela augmenterait la possibilité de voter, contrairement à un vote visuel auquel on fait référence parce que cela se fait à un moment bien précis. Alors, si les 338 parlementaires sont en ligne, cela rend les choses plus difficiles.

Mme Christine Normandin: Merci beaucoup.

[Traduction]

La présidente : Merci.

Madame Blaney, vous avez la parole.

Mme Rachel Blaney : Merci.

Monsieur Aubé, je reviens à vous. Vous avez dit, je crois, dans l'une de vos réponses, que vous souhaitiez mettre en place un groupe de travail chargé d'examiner certains de ces processus avec les députés. Je me demande comment vous procèderiez et si tous les partis reconnus pourraient y participer.

M. Stéphan Aubé : Excusez-moi, je n'ai pas bien compris le début de la question.

Mme Rachel Blaney : Je crois que vous avez dit dans l'une de vos réponses à nos questions qu'il y aurait un groupe de travail composé de députés, qui serait chargé d'examiner certains de ces processus, et je me demande si tous les partis reconnus y prendraient part.

M. Stéphan Aubé : Si c'est ce que j'ai dit, je tiens à me corriger. Ce que j'ai voulu dire, c'est que nous serions ouverts à une consultation avec les partis, s'ils nous le demandaient, au sujet de l'interface.

Lorsque nous demandons la participation des députés au sujet d'un système que nous développons pour eux, le processus habituel veut que tous les partis soient consultés. C'est ce que nous ferions si on nous le demandait.

Mme Rachel Blaney : Merci.

Aujourd'hui, nous avons beaucoup parlé de la façon dont on évalue les risques et dont on s'y adapte, surtout lorsqu'on songe à un Parlement virtuel pour l'avenir.

De quelle façon faites-vous part des risques possibles aux partis? Comment les évaluez-vous et comment transmettez-vous l'information aux députés?

M. Stéphan Aubé : La première étape consiste à évaluer et à documenter les risques. ****** **********. Une fois les risques documentés, nous les communiquons à la Présidence pour commencer. Le Président décide ensuite de la façon dont il veut en faire part aux partis politiques.

C'est l'approche que nous préconisons. Nous passons par le greffier, qui transmet l'information à la Présidence. En cas de risque, nous nous assurons d'aviser le Président de sorte qu'il puisse en faire part aux députés.

Mme Rachel Blaney : Merci.

Je n'ai pas d'autre question.

La présidente : Merci beaucoup, madame Blaney.

Je remercie tous les témoins.

Voilà qui met fin à nos séries de questions. Nous allons laisser le temps aux témoins de partir et poursuivre la réunion à huis clos afin de discuter des travaux du Comité. Je remercie une fois de plus toute l'équipe. Nous vous sommes très reconnaissants du temps que vous accordez au Comité.