Résumé de l'entrevue : Administration de la Chambre des communes (Patrick McDonell et Benoît Dicaire)*

Les avocats de la Commission ont mené une entrevue avec Patrick McDonell, sergent d'armes, et Benoît Dicaire, dirigeant principal de l'information à la Chambre des communes, le 3 septembre 2024.

Notes aux lecteurs :

- Les segments de texte entre crochets sont des notes explicatives fournies par les avocats de la Commission pour aider le lecteur.

1. Introduction

[1] Patrick McDonell est l'actuel sergent d'armes et directeur de la sécurité institutionnelle à la Chambre des communes (la « **Chambre** » ou la « **CdC** »). En plus d'exercer de nombreuses fonctions protocolaires, il est responsable de la sécurité de la Chambre et de ses membres pendant qu'ils sont à la Chambre et lorsqu'ils se trouvent à l'extérieur de la Cité parlementaire. Cette responsabilité comprend les bureaux de circonscription et les résidences privées des députés**.** Il supervise une équipe d'environ 114 employés.

[2] Il a été officiellement nommé à son poste en juillet 2019, après avoir déjà occupé le poste de sergent d'armes par intérim, à la suite de la nomination de Kevin Vickers à titre d'ambassadeur en Irlande en 2015. Il s'est joint à la GRC en 1980, où il a occupé divers postes avant de passer au Sénat du Canada, où il était directeur du Service de sécurité du Sénat.

[3] Benoît Dicaire occupe actuellement le poste de dirigeant principal de l'information (« **DPI** »), Services numériques et Biens immobiliers (« **SNBI** »), de la Chambre. Il dirige une équipe de 760 employés qui supervise et fournit l'infrastructure de sécurité, ainsi que les applications informatiques et le soutien connexe à la Chambre, à ses

* Traduction.

membres et à ses employés. Il est aussi responsable de la politique de sécurité des technologies de l'information (TI) et de la cybersécurité, en plus de veiller à l'intégration de la technologie dans les installations de la CdC et pour la radiotélédiffusion et la diffusion sur le Web lorsque la CdC est en session. Une partie du mandat du DPI consiste à protéger l'information parlementaire.

[4] M. Dicaire travaille pour la CdC depuis 24 ans et a été nommé à son poste actuel en 2024. Il est titulaire d'un baccalauréat en commerce de l'Université d'Ottawa.

2. Structure de l'Administration de la Chambre des communes

[5] Le Bureau de régie interne (« **BRI** ») est l'entité responsable de toutes les questions financières et administratives pour la CdC, ses locaux, ses services et ses employés, ainsi que les députés. Il est créé par la *Loi sur le Parlement du Canada*. Le BRI est présidé par le Président de la Chambre des communes, qui est choisi par tous les députés. La composition du BRI est divisée également entre les députés du gouvernement et de l'opposition. Le nombre de députés change en fonction du nombre de partis reconnus à la Chambre. À l'heure actuelle, il y a quatre partis reconnus. L'opposition officielle a deux députés, et chaque autre parti de l'opposition a un député chacun. Le parti au pouvoir a donc quatre membres.

[6] Le BRI établit les règlements administratifs concernant la gestion des ressources de la CdC par les députés. Le BRI applique ses propres règlements administratifs, mais l'Administration de la Chambre des communes joue un rôle actif dans leur mise en œuvre. Par exemple, le service des finances traite les demandes de remboursement de tous les députés. Le service doit déterminer si les dépenses dont les députés demandent le remboursement se rapportent à des travaux parlementaires, ce qui peut parfois être difficile. L'Administration de la CdC traite plus de 100 000 demandes par année.

[7] Il n'y a pas d'unité au sein des bureaux du sergent d'armes ou du directeur de l'information qui s'occupe spécifiquement de l'ingérence étrangère, mais celle-ci est

pertinente pour le travail de certaines unités, telles que l'unité de gestion des risques et des enquêtes.

[8] Le Programme de veille des sources ouvertes relève également de la responsabilité du sergent d'armes. Ce programme comprend une équipe d'analystes qui surveille le renseignement de sources ouvertes (« **OSINT** ») pour détecter les menaces et le harcèlement envers les députés. Si les analystes constatent un comportement qui pourrait être criminel, ils communiquent avec la GRC ou les services de police compétents concernés. Une collaboration régulière existe entre l'équipe du sergent d'armes et les services de TI de la CdC.

[9] Le Bureau du sergent d'armes dispose d'une unité d'enquête, composée principalement d'anciens policiers, qui enquête sur les cas de menaces et de harcèlement à l'encontre des députés. Une autre équipe au sein du Bureau mène des enquêtes contre-techniques, notamment la surveillance des signaux et le dépistage de mouchards [dispositifs de surveillance clandestine].

[10] Le Service de protection parlementaire (« **SPP** ») est une entité distincte de l'Administration de la CdC et relève à la fois des Présidents de la CdC et du Sénat. Le directeur du Service est membre de la GRC. Il a un mandat spécifique pour les institutions du Parlement, pas seulement la Chambre. Il est responsable de la sécurité physique des députés pendant qu'ils se trouvent dans la Cité parlementaire.

3. Mesures et politiques de sécurité des TI

[11] M. Dicaire a expliqué que d'un point de vue technologique, il existe diverses règles qui régissent ce que les députés ont et ce qu'ils peuvent faire sur leurs dispositifs électroniques de la CdC. Le BRI a une politique d'utilisation acceptable remontant à 2014 qui dicte le comportement acceptable et inacceptable, et une politique de sécurité des TI depuis 2016. Le BRI a également une politique sur la gestion de l'information qui a été récemment mise à jour en 2024 et qui s'applique actuellement au personnel de la CdC, mais pas aux députés, car le BRI ne l'a pas encore approuvée officiellement.

[12] Le programme de sécurité des TI est fondé sur des mesures proactives et réactives, qui comprennent à la fois la surveillance des incidents et la production de rapports provenant de diverses sources, y compris les plaintes. Il adopte une approche à plusieurs niveaux fondée fondée sur les normes et les meilleures pratiques du secteur visant à réduire les risques à tous les niveaux et à s'assurer que les députés peuvent mener leurs activités efficacement, que ce soit au caucus, dans leur bureau de circonscription ou à la Chambre. Des mesures de contrôle au niveau du dispositif et de l'utilisateur, ainsi que des contrôles de périmètre, sont en place.

[13] M. Dicaire a expliqué que, en ce qui concerne les TI, la Chambre a sa propre infrastructure et gère ses propres réseaux. Les contrôles de périmètre veillent à ce que l'infrastructure elle-même soit protégée sur le périmètre, y compris aux points de contact avec Internet ainsi que sur les réseaux du gouvernement du Canada. Le réseau de la CdC est conçu de manière à se conformer aux normes internationales.

[14] Les députés ont l'obligation de faire rapport à l'Administration de la Chambre lorsqu'ils voyagent à l'étranger avec un appareil électronique de la CdC, quel que soit le but du voyage. Tous les dispositifs de la CdC sont suivis, et SNBI peut voir quand un dispositif se trouve à l'étranger. Si un député ne transporte pas d'appareil parlementaire à l'étranger, il n'est pas tenu d'en informer l'Administration de la Chambre. Des rapports sont générés tous les matins pour savoir où se trouvent les différents députés dans le monde lorsqu'ils voyagent avec un appareil parlementaire.l

[15] Il est possible de prendre diverses mesures lorsqu'un député se rend à l'étranger avec un appareil parlementaire sans en informer l'Administration de la Chambre. On peut communiquer avec le député non conforme pour lui rappeler les règles ou de de porter la situation à la connaissance du whip du parti concerné. SNBI a la capacité d'interrompre l'accès du dispositif, en particulier lorsque le député visite un pays préoccupant pour le Canada. Le DPI a l'obligation et le pouvoir discrétionnaire d'interrompre l'accès s'il croit qu'il y a un risque particulier.

3.1 Appareils électroniques de la Chambre fournis aux députés et la cybersécurité

[16] M. Dicaire a expliqué que les députés se font remettre trois ordinateurs pour les bureaux sur la Colline parlementaire. Pour les bureaux de comté, ils peuvent avoir jusqu'à 10 appareils électroniques fournis par la Chambre des communes (la « **Chambre** » ou « **CC** »). Les députés ne peuvent pas utiliser des appareils non autorisés par l'administration de la Chambre. Des dispositions sont prévues pour certains appareils personnels (p. ex. MacBook). Ils peuvent se brancher sur un réseau « invité », qui est également sécurisé. En ce qui concerne les appareils portables, il peut y en avoir un par employé.

[17] Lorsque les députés voyagent à l'étranger, ils bénéficient du programme « ParlVoyage ». Ce programme prévoit une évaluation du risque effectuée en fonction de la destination du voyageur et des personnes qui l'accompagnent. Suivant cette évaluation, le droit de voyager avec les appareils électroniques parlementaires est soit accordé ou, s'il existe un risque à la sécurité, l'appareil est restreint avec une différente configuration de sécurité. L'expérience utilisateur demeure néanmoins similaire et le député conserve l'accès à ses courriels des 60 derniers jours. L'administration de la Chambre fournit également des sacs de protection pour les appareils portables. Le Sénat a ses propres appareils et utilise les services de Services partagés Canada (« **SPC** »).

[18] M. Dicaire a signalé que son département n'a aucune autorité sur l'utilisation des ordinateurs personnels par les députés, mais offre plusieurs formations sur les types d'appareils électroniques qui peuvent être utilisés. Il fait remarquer qu'on ne peut pas savoir si un appareil personnel d'un député a été compromis à la suite d'une cyberattaque. Cependant, si un député soupçonne que l'un de ses appareils personnels a été piraté, celui-ci peut faire appel aux services informatiques de la Chambre en vue d'effectuer une analyse du contenu informatique.

[19] M. Dicaire a précisé que la protection des parlementaires s'applique aussi aux comptes informatiques. Il existe plusieurs moyens technologiques pour assurer la sécurité informatique des comptes, incluant l'authentification multifactorielle. Par ailleurs, il y a une politique en place qui interdit aux employés de la Chambre l'utilisation des comptes parlementaires sur les médias sociaux à des fins non professionnelles.

[20] En cas de problème de cybersécurité, il existe un service disponible 24 heures sur 24, sept jours sur sept pour les parlementaires. La cybersécurité de la Chambre passe par les opérations de sécurité, le programme de sécurité, incluant la politique de sécurité, le respect des règles, la détection des menaces, ainsi que la sensibilisation et la formation du personnel.

[21] M. Dicaire a souligné qu'au cours d'une année donnée la Chambre est confrontée à un nombre faramineux de cyberattaques qui peuvent prendre plusieurs formes (p. ex. logiciels malveillants, hameçonnage, rançongiciel, spamouflage, etc.). La plupart du temps, les mécanismes de défense détectent et bloquent ce qui essaie de pénétrer dans le système, mais parfois, quelque chose réussit à passer. Dans ces cas, son équipe fait enquête et cherche à colmater les brèches dans le système. Il réaffirme que son mandat porte la continuité des opérations au Parlement.

[22] Lorsque les responsables de la sécurité des TI de la Chambre détectent une attaque, ils ne divulguent pas nécessairement qu'elle a eu lieu. Cela dépend des circonstances. Si une attaque vise un parlementaire en particulier, cette information lui est divulguée. S'ils doivent communiquer des informations relatives à une cyberattaque à des services de renseignement et de sécurité, le député concerné en est avisé. Mais en cas de cyberattaque infructueuse, ils ne préviennent personne. Le nombre de cyberattaques qui échouent est énorme.

[23] Le président de la Chambre est avisé d'une cyberattaque lorsque celle-ci a un impact sur les activités du Parlement ou pose un risque d'atteinte à la réputation de la Chambre.

4. Relations avec le gouvernement du Canada et d'autres intervenants

4.1 Relations avec les ministères, organismes et comités du gouvernement

[24] Les avocats de la Commission ont posé des questions sur la relation entre la CdC et le gouvernement du Canada. M. McDonell a expliqué que le Bureau du sergent d'armes a conclu avec le SCRS et la GRC des protocoles d'entente (« **PE** ») qui prévoient un échange d'information. Il indique que le Bureau a des communications régulières avec la GRC et le SCRS. Il a également des PE avec le Bureau du Conseil privé (« **BCP** »), notamment pour la surveillance des dispositifs de surveillance clandestine aux réunions du Cabinet.

[25] Le DPI a un PE avec le Centre de la sécurité des télécommunications (« **CST** »), avec lequel il entretient une relation de longue date. Des réunions se tiennent régulièrement avec le CST, à la fois planifiées et en réponse à des incidents spécifiques.. Le rôle du CST s'est accru au fil des ans, mais aujourd'hui, il se concentre sur l'aide à la protection de l'infrastructure de la CdC au périmètre et sur l'aide à la gestion des incidents. Il y a également échange d'information entre l'équipe du DPI et le CST concernant la sensibilisation, les pratiques exemplaires et les nouvelles tendances. Des réunions sont prévues à intervalles réguliers entre la Chambre et le CST, et certaines sont ponctuelles, en fonction d'incidents précis. M. Dicaire a qualifié le partenariat avec le CST de collaboration fructueuse.

[26] M. Dicaire indique que la CdC entretient une relation informelle avec Services partagés Canada (« **SPC** ») [SPC est l'institution fédérale responsable de la prestation de services numériques non classifiés aux organisations du gouvernement du Canada]. La Chambre peut utiliser ses services au besoin, mais elle n'est pas tenue de le faire. Ils font tous deux partie d'une communauté de pratique avec d'autres ministères. Il est invité à des réunions trimestrielles à SPC.

[27] M. Dicaire a ajouté que la CdC fournit une infrastructure de TI à tous les partenaires parlementaires, y compris le Sénat, la Bibliothèque du Parlement et le SPP. Les

équipes de TI de la Chambre et du Sénat travaillent en collaboration sur la même infrastructure.

[28] Le Bureau du sergent d'armes participe à INTERSECT, une communauté de premiers intervenants de la région d'Ottawa, qui comprend les services d'application de la loi, d'incendie et d'urgence. Cet organisme communique divers produits de renseignement à ses membres, y compris la CdC. La communication d'informations par l'intermédiaire d'INTERSECT a augmenté depuis les manifestations du « convoi de la liberté » [en 2022].

[29] M. McDonell siège également au Comité des sous-ministres sur la protection ministérielle. Ces réunions ont lieu dans une installation classifiée.

4.2 Échange d'information entre le gouvernement et la CdC

[30] M. Dicaire a expliqué que les circonstances dans lesquelles il reçoit de l'information du CST concernant les cybermenaces sont assez formelles. Le CST produit des bulletins techniques conformément à un protocole officiel, à la suite d'une demande de prise de mesures ou d'une recommandation. M. Dicaire a indiqué que le CST est généralement à la recherche d'une « pièce du casse-tête ». L'information est de niveau « Protégé B » et de nature générale ou technique. Il a expliqué que ces informations ne concernaient que très rarement des personnes et porte plus souvent sur les activités d'une adresse IP en relation avec un réseau particulier.. Le CST examine le périmètre de l'infrastructure de TI de la CdC, mais n'a aucune visibilité à l'intérieur de son réseau. Le CST demande de l'aide pour interpréter les informations , et l'équipe de M. Dicaire peut fournir de l'aide ou de la visibilité en enquêtant sur l'information technique. Les informations fournies par le CST étant de nature technique, le COH ne sait pas si la cybermenace est le fait d'un gouvernement étranger ou de toute autre personne disposant d'une connexion à l'internet.

[31] M. Dicaire ne se souvient pas que le CST lui ait jamais parlé d'un cas d'ingérence étrangère. S'il l'a fait, c'était uniquement à propos d'informations techniques dépourvues de contexte, de sorte qu'il n'aurait pas su que cela se rapportait à

l'ingérence étrangère. La seule fois où il se souvient de quelque chose se rapportant spécifiquement à l'ingérence étrangère, c'était lors d'un breffage du SCRS.

[32] Les avocats de la Commission ont demandé s'il serait utile de recevoir des renseignements contextuels du CST. M. Dicaire a répondu par l'affirmative. Certains des bulletins qu'il reçoit contiennent des recommandations peu claires. Le contexte pourrait aider à reconstituer le casse-tête. Il s'est toutefois demandé dans quelle mesure le CST pouvait communiquer efficacement cette information. L'important est que les informations transmises permettent au DPI d'enquêter sur la menace et de s'assurer que les systèmes de la CdC sont stables. Si l'augmentation des renseignements contextuels entraîne une réduction de l'information technique communiquée en raison de problèmes de sécurité, ce serait un problème. M. Dicaire a souligné que le DPI et le CST ont des mandats très différents : le DPI a principalement pour fonctions de protéger les systèmes parlementaires, de s'assurer que les députés ont accès au réseau, et de faire en sorte que le réseau ne soit pas compromis pour permettre aux travaux parlementaires de se poursuivre. Il n'a pas de mandat en matière de sécurité nationale.

[33] M. McDonell a expliqué que son bureau et la GRC produisent tous les matins, du lundi au vendredi, des rapports sur les menaces à l'encontre des députés. Les rapports de la GRC contiennent la contribution du département de Sécurité et renseignement du BCP. Les deux entités s'échangent leurs rapports, qui fournissent des informations actualisées sur les menaces apparues au cours des 24 heures précédentes. Pendant les week-ends, des personnes sont disponibles si un événement préoccupant se produit.

[34] Le sergent d'armes et la GRC préparent conjointement des évaluations de la menace pour tous les types d'activités et de lieux publics où les députés sont présents.

[35] La GRC produit des rapports sur les manifestations dans tout le pays, qui sont communiqués au sergent d'armes. L'OSINT du sergent d'armes surveille également les manifestations et en fait rapport.

4.3 Habilitations de sécurité et installations sécurisées

[36] Comme les députés sont élus par les Canadiens, ils n'ont pas besoin d'une habilitation de sécurité pour siéger à la Chambre. Certains députés peuvent en avoir besoin selon la fonction ou la responsabilité particulière qu'ils exercent. C'est le cas des députés qui exercent certaines fonctions de secrétaire ministériel ou parlementaire, ou des députés qui siègent à certains comités comme le Comité des parlementaires sur la sécurité nationale et le renseignement (« **CPSNR** »). Cette responsabilité incombe au gouvernement.

[37] Le Président n'a pas besoin d'une habilitation de sécurité pour s'acquitter de ses fonctions. Toutefois, le Président actuel, l'honorable Greg Fergus, en a une en raison de ses rôles antérieurs au Parlement.

[38] M. McDonell et M. Dicaire ont tous deux une habilitation de sécurité de niveau très secret. Le Bureau du sergent d'armes compte un certain nombre d'employés qui ont une habilitation de sécurité de niveau très secret en raison de la nature de leurs fonctions, qui comprennent des interactions avec le SCRS et la GRC.

[39] M. Dicaire détient également une habilitation de sécurité de niveau très secret parce qu'il rencontre régulièrement le CST. Certains analystes de M. Dicaire ont une habilitation de sécurité de niveau très secret en raison de la nature de leur travail.

[40] La Chambre des communes dispose dans ses locaux d'une salle où l'on peut échanger de l'information classifiée au niveau secret, en discuter et la stocker, et d'une autre salle qui peut accueillir des séances d'information de niveau secret et très secret. Les représentants de l'Administration de la Chambre assistent également à des réunions à l'extérieur dans un local isolé pour l'information sensible cloisonné (« **LIISC** »). Pour M. Dicaire, ces réunions ont lieu au CST.

[41] M. McDonell indique qu'il est actuellement prévu de construire un LIISC dans la nouvelle Cité parlementaire dans le cadre des travaux de rénovation en cours.

5. Questions de sécurité liées aux députés, au caucus et au personnel

5.1 Questions de sécurité liées aux députés

[42] En cas de préoccupation concernant un député, ils communiqueront directement avec le député en question. Il existe des voies de communication directes avec les députés et il est rarement nécessaire de passer par un groupe parlementaire ou un membre du personnel.

[43] M. McDonell a expliqué qu'il existe diverses façons pour son bureau de détecter les menaces à la sécurité physique des députés, notamment au moyen du renseignement de sources ouvertes, de rapports provenant de députés et de membres du personnel, ainsi que de la GRC ou du service de police compétent.

[44] Les menaces à la sécurité physique sont communiquées directement au député concerné. Dans certains cas, le sergent d'armes avisera le whip ou le leader parlementaire du parti du député. Il avisera également la GRC et, dans certains cas particuliers, le BCP et les organismes de sécurité et de renseignement. M. McDonell souligne que les menaces et le harcèlement à l'égard des membres se produisent quotidiennement.

[45] La Chambre fournit aux députés des systèmes de sécurité à domicile qui sont mis à leur disposition pour leurs résidences principale et secondaire (c.-à-d. la région de la capitale nationale). Les bureaux de circonscription peuvent également être équipés de systèmes de sécurité.

[46] Les députés et leurs conjoints reçoivent des dispositifs d'alarme personnels portatifs. Dans certains cas plus graves, des gardes de sécurité peuvent être fournis pour protéger un député ou sa résidence. Les députés peuvent demander une sécurité statique ou fixe pour leur domicile ou leur bureau de circonscription. Le sergent d'armes peut également fournir une équipe de sécurité personnelle aux chefs de parti. Cela se fait généralement au cas par cas.

[47] L'Administration de la Chambre a peu d'interactions liées à la sécurité avec les anciens députés. Il existe une association d'anciens députés qui a un petit bureau dans la Cité parlementaire. Le sergent d'armes a des contacts réguliers avec cette organisation, mais à part les questions liées aux privilèges d'accès aux édifices, il n'y a essentiellement aucune interaction liée à la sécurité avec ce groupe. M. McDonell ne se souvenait d'aucun cas mettant en cause son bureau où un ancien député avait été la cible d'un acte d'ingérence étrangère.

[48] M. Dicaire a indiqué que la protection des anciens députés contre les cybermenaces d'ingérence étrangère ne fait pas partie de son mandat. S'il était informé d'une telle menace, il en informerait l'organisme national compétent. Cela ne s'est jamais produit jusqu'à présent.

5.2 Enquête de sécurité sur le personnel des députés

[49] Le Bureau du sergent d'armes est chargé d'effectuer les enquêtes de sécurité sur le personnel de la Chambre. Il effectue des vérifications des antécédents criminels et des enquêtes sur la « loyauté envers le Canada », avec l'aide de la GRC et du SCRS.

[50] Les enquêtes sur la loyauté envers le Canada comprennent un examen des antécédents des cinq dernières années. Ces enquêtes peuvent être difficiles, surtout si le candidat a résidé à l'étranger, s'il est nouveau au Canada ou vient d'un pays qui soulève des préoccupations pour Canada. Les enquêteurs du sergent d'armes peuvent mener des entrevues « préventives » (‘*resolution of doubt*’) avec des candidats à l'emploi. Le nombre d'entrevues « préventives » menées aujourd'hui a connu une augmentation considérable par rapport à ce qui se faisait en 2019 environ; les entrevues sont également plus approfondies qu'elles ne l'étaient auparavant. Lorsque les renseignements soumis par le candidat à l'emploi sont incomplets, son bureau veut veiller à prendre les mesures appropriées pour protéger ses réseaux et ses institutions. La plupart des enquêteurs du sergent d'armes sont des anciens policiers ayant une grande expérience des entrevues. L'unité du renseignement de sources ouvertes recueille autant de documents de sources ouvertes que possible sur le candidat à l'emploi.

[51] L'enquêteur qui mène l'entrevue « préventive » recommande au sergent d'armes d'accorder ou non l'accréditation. Le sergent d'armes a le dernier mot. Il existe un processus d'appel informel dans le cas où le député employeur potentiel, qui a un pouvoir discrétionnaire sur les per3sonnes qu'il embauche, n'est pas d'accord avec le refus par le sergent d'armes d'octroyer l'accréditation. En générale, le candidat à l'emploi doit communiquer avec le sergent d'armes pour interjeter appel de la décision. Dans un cas, le député et le candidat à l'emploi ont rencontré le sergent d'armes.

[52] M. McDonell a indiqué qu'au cours des dix années écoulées, à son poste, il n'a refusé qu'un petit nombre d'accréditations en raison de préoccupations liées à l'ingérence étrangère.

5.3 Préoccupations en matière de sécurité liées au caucus et à son personnel

[53] En cas de préoccupations, liées à la sécurité ou d'autre nature, concernant les membres actuels du personnel du caucus, le sergent d'armes communique avec le bureau du whip du parti en question.

[54] Certaines questions peuvent être abordées avec les whips ou les chefs de parti, lorsque la question est de nature plus collective. M. McDonell a indiqué que, dans certains cas, cela peut être aussi informel qu'une conversation de couloir.

[55] Lorsqu'on lui a demandé si l'Administration de la CdC gardait contact avec les anciens députés, M. McDonell a indiqué que c'était le cas, soulignant qu'il existe une « association d'anciens parlementaires » qui maintient un petit bureau sur les lieux. L'association se concentre sur la transition des députés vers la vie post-parlementaire. Il est en discussion régulière avec l'association. Il n'a pas encore eu connaissance d'un cas où un ancien député aurait soulevé des préoccupations concernant l'ingérence étrangère dans son bureau. Les anciens députés conservent un accès privilégié à la Colline du Parlement après leur mandat.

6. Breffages à l'intention des députés et du personnel sur l'ingérence étrangère

[56] L'Administration de la Chambre des communes assure la coordination avec les partenaires de la sécurité, du renseignement et de l'application de la loi pour offrir aux députés et au personnel des breffages non classifiées sur l'ingérence étrangère. Ces breffages sont élaborées par la GRC, le SCRS, le CST et Sécurité publique Canada (« **SPC** »), qui en prend les rênes. Des breffages ont été offertes au cours de la dernière année aux divers caucus en tant que groupe, ainsi qu'à différents secteurs de l'Administration de la CdC. Ces breffages portent sur le paysage actuel des menaces et sur les précautions possibles à prendre.

[57] Le Bureau du sergent d'armes compte de nouveaux postes liés à la sensibilisation à la sécurité. Ils portent davantage sur l'information des députés sur la sécurité, dont l'ingérence étrangère est un aspect important. L'un des objectifs de ce travail d'information commencera avec la prochaine législature dans le cadre du processus d'intégration des députés. Les breffages aborderont de nombreux sujets, y compris l'ingérence étrangère.

[58] M. McDonell a indiqué qu'il voulait que le programme de sensibilisation à la sécurité soit à jour en tout temps et que les députés soient tenus informés en continu.

[59] M. Dicaire a indiqué que son bureau ferait de même en ce qui concerne la cybersécurité, car la sensibilisation est un pilier important d'une cybersécurité saine.. La composante de l'ingérence étrangère dans les breffages sur la cybersécurité à l'intention des députés sera élargie.

[60] Son équipe envoie actuellement des bulletins de cybervigilance sur les questions d'actualité telles que TikTok et les courriels d'hameçonnage.

[61] M. McDonell a indiqué que ces mesures n'étaient pas nécessairement en réponse aux recommandations formulées dans le rapport du Comité de la procédure et des affaires

de la Chambre (« PROC ») déposé à la Chambre l'an dernier, notant qu'il avait plaidé en faveur de ce type de breffages bien avant cela.

[62] Lorsque le SCRS veut rencontrer un député, le sergent d'armes et son bureau aident à coordonner et à faciliter la réunion. Ils ne demandent pas de détails sur les raisons pour lesquelles le SCRS souhaite rencontrer le député.

7. Lutte contre la mésinformation et la désinformation

[63] Les avocats de la Commission ont demandé si la lutte contre la mésinformation et la désinformation faisait partie du mandat de l'Administration de la Chambre, qui consiste à soutenir les députés dans leurs fonctions parlementaires. M. Dicaire a noté qu'il s'agissait d'un sujet dont il était plus conscient et qu'il surveillait de plus en plus, en particulier avec l'avènement de l'IA et de l'hypertrucage. Bien que l'Administration de la Chambre n'ait pas le mandat de corriger la mésinformation et la désinformation et qu'elle ne devrait pas être perçue comme intervenant dans le débat politique, elle met l'accent sur la sensibilisation et les meilleures pratiques. L'Administration de la Chambre prend soin de ne pas intervenir dans le débat politique.

[64] Il y a eu de nombreux cas de faux comptes de médias sociaux se faisant passer pour des députés et de sites web d'immigration frauduleux utilisant les images des députés.. Dans ce cas, la CdC intervient auprès des adminstrateurs de la plateforme et prend des mesures pour faire retirer le contenu. Elle obtient généralement l'autorisation du député concerné d'agir en son nom, mais cela n'est pas toujours nécessaire, car le contenu enfreint généralement les modalités de la plateforme.

[65] M. Dicaire a décrit une campagne de « Spamouflage » liée à la RPC sur les médias sociaux ciblant les comptes des députés, qui impliquant robots publiant de la désinformation et de la propagande en 2023. Cette campagne a été portée à son attention par Affaires mondiales Canada (« **AMC** »). Une communication aux députés les a informés de cette campagne particulière.

[66] L'Administration de la CdC ne gère pas la mésinformation ou la désinformation liée à la Chambre elle-même. Elle tente plutôt de positionner le site Web de la Chambre comme

la source légitime d'information sur la Chambre. La plus grande préoccupation de l'équipe de M. Dicaire est la protection de l'équipement et des systèmes de TI.

8. Incidents particuliers

8.1 La cyberattaque du groupe APT31 ciblant les députés de l'IPAC

[67] Les avocats de la Commission ont présenté aux personnes interrogées un document non classifié préparé par le CST décrivant une chronologie des événements liés à la campagne de lien de suivi par courriel du groupe APT31 en 2021, qui ciblait les députés membres de l'Inter-Parliamentary Alliance on China (« **IPAC** »). Les avocats de la Commission ont sollicité leur point de vue sur la chronologie des événements, plus particulièrement pour aborder les nombreux cas dans le rapport indiquant que la sécurité des TI de la CdC ne répondait pas ou ne fournissait pas de rétroaction aux demandes du Centre canadien pour la cybersécurité (« **CCC** »).

[68] M. Dicaire indique que les services de TI de la Chambre reçoivent régulièrement des rapports du CCC qui sont de nature très technique. Dans ce cas, le CCC demandait de l'aide concernant des adresses IP précises. Lorsque la CdC reçoit de tels rapports, elle est tenue d'en accuser réception dans le cadre de son protocole. En ce qui concerne l'incident décrit dans le rapport, seules des informations très techniques ont été fournies. Le rapport contenait de vagues recommandations sur ce qu'il fallait faire, comme demander de vérifier si des courriels précis étaient parvenus à leurs destinataires. Le CCC n'a communiqué que des adresses IP. Après enquête, le service de TI de la CdC a découvert que les courriels en question n'étaient pas parvenus à leur destinataire et avaient été mis en quarantaine par leur passerelle de sécurité. Par conséquent, il n'y avait aucune menace pour le Parlement ou son infrastructure.

[69] M. Dicaire a expliqué qu'il reçoit de nombreux rapports de ce genre. Lorsque son bureau détermine qu'il n'y a pas de menace pour l'infrastructure parlementaire, il n'en fait pas plus. Dans ce cas, il a signalé au CCC le 3 février 2021 que la situation avait été « traitée à l'interne » parce que leur système l'avait gérée.

[70] La puce du 17 février 2021 indique que le service de TI de la CdC a évalué que certaines adresses courriel personnelles de députés pourraient avoir reçu les messages. M. Dicaire a fait remarquer que les comptes de courriel personnels ne relèvent pas de la compétence de la CdC. Les renseignements originaux reçus concernaient les adresses IP des députés, qui, selon lui, n'avaient pas été compromises. Il a indiqué qu'aucune information contextuelle n'avait été communiquée dans le rapport du CCC, de sorte que le bureau n'avait aucun moyen de savoir s'il s'agissait d'une attaque parrainée par un État ou non. Il a noté que la source de la cyberattaque ne faisait aucune différence du point de vue de la CdC, si ce n'est le fait qu'il s'agit d'informations contextuelles qui pourraient éclairer la compréhension du profil de menace par la CdC.

[71] M. Dicaire a mentionné que lorsque le bureau a reçu le rapport original, la CdC n'avait pas encore compris que les courriels en question avaient été mis en quarantaine. Il a envoyé un courriel aux huit députés concernés pour savoir s'ils recevaient des courriels des domaines en question. Aucun d'entre eux n'a répondu qu'ils en avaient reçu. Dans leur réponse écrite, deux députés ont indiqué qu'ils resteraient à l'affût.

[72] Malgré une demande du CCC le 24 février 2021 pour obtenir des copies des courriels, le service de TI de la CdC ne les a pas fournis, car ils n'avaient pas le consentement des députés pour le faire. Il n'a pas demandé le consentement, car les courriels ne sont jamais parvenus à leurs destinataires. Cela dit, le service de TI de la CdC a fourni au CCC des informations, y compris des métadonnées, sur les courriels le 26 février 2021. M. Dicaire a établi un contraste avec la campagne Spamouflage où l'on craignait que les courriels n'aient atteint des députés ciblés. Dans ce cas, le service de TI de la CdC a collaboré avec le Bureau du sergent d'armes pour obtenir le consentement des députés de pourvoir vérifier leurs courriels.

[73] En réponse à la puce du 17 mars 2021 faisant référence à un 8e rapport dans lequel le CCC a demandé à l'analyste de la sécurité des TI de la CdC d'autres informations techniques ou contextuelles, M. Dicaire a fait remarquer que si une demande se rapporte à une menace qui a été écarter, il est possible que l'analyse n'ait pas répondu

parce que le problème a été géré. Il a dit que cela aurait été communiqué au CCC, soulignant que le protocole entre le CCC et le service de TI de la CdC est très collaboratif.

[74] En examinant les informations contenues dans le rapport en question, M. Dicaire a expliqué que le CCC a demandé d'enquêter sur des informations très spécifiques et techniques. Répondre à ce type de demande prend du temps, car cela nécessite une analyse criminalistique de la part de la CdC. En l'espèce, l'analyse de la CdC a indiqué que les renseignements demandés par le CCC concernaient un appareil personnel ou invité qui se trouvait sur le réseau d'invités de la CdC. Étant donné que l'appareil en question n'était pas un appareil de la CdC, toute menace à son intention ne constituait pas une menace pour l'infrastructure parlementaire. Ces renseignements ont d'ailleurs été communiqués au CCC.

[75] M. Dicaire a indiqué que SNBI n'était pas au courant que le FBI avait informé le gouvernement en juin 2022 que l'activité mentionnée dans les rapports du CCC était liée à une attaque liée à la RPC contre des parlementaires qui étaient membres de l'IPAC.

[76] Il a expliqué que la CdC avait effectivement reçu un bulletin du CCC en juin 2022 sur les cyberattaques sur lesquelles la CdC avait précédemment enquêté. Le bulletin ne mentionnait pas le groupe APT31. Il ne mentionnait pas non plus le FBI, faisant seulement référence à un partenaire de confiance. Il mentionnait que seules les adresses courriel de personnes qui s'étaient exprimées ouvertement sur des sujets liés au Parti communiste chinois (« **PCC** ») ont été ciblées. Le bulletin portait sur des détails techniques.

[77] De plus, le bulletin de juin 2022 faisait référence à une attaque en janvier 2022, et non en janvier 2021. M. Dicaire a expliqué que le service de TI de la CdC pensait que le bulletin faisait donc référence à un incident différent du numéro de janvier 2021. Toutefois, lorsque le service de TI de la CdC a enquêté sur l'affaire, il n'a pas pu trouver d'informations pertinentes relatives à la plage de dates citée par le CCC dans le

bulletin. Après avoir informé le CCC de ce fait, celui-ci s'est corrigé pour indiquer que le bulletin aurait dû faire référence à 2021, et non à 2022.

[78] Lorsque le CCC a corrigé les dates pertinentes, le service de TI de la CdC a compris que le bulletin se rapportait à la même affaire de 2021 qu'il avait déjà traité avec le CCC.

[79] Les parlementaires ciblés n'ont pas été informés par l'Administration de la CdC en 2022, parce que la cybermenace ne les a jamais atteints. Le CCC n'a pas non plus recommandé de les en informer. Si le service de TI de la CdC avait su qu'il s'agissait d'une campagne parrainée par un État, ils auraient peut-être examiné la situation avec une plus grande vigilance, dans une perspective de surveillance et de continuité des activités.. Mais une fois qu'il a conclu qu'il n'y avait pas de menace réelle, il n'a informé personne, conformément à sa pratique habituelle.

8.2 Ciblage du député Michael Chong

[80] En ce qui concerne le rapport de 2023 indiquant que le député Michael Chong a reçu un exposé du SCRS indiquant qu'il était la cible d'une campagne d'ingérence de la RPC, le sergent d'armes n'a reçu aucun produit de renseignement relativement à cet incident et n'avait pas de détails sur le but de la réunion.

[81] Les personnes interrogées ne savaient pas si les commentaires ou la rétroaction de la CdC avaient été sollicités avant l'adoption des *Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires* peu de temps après cette séance d'information. Elle les informe toutefois que le seuil d'information des députés est abaissé. Depuis les directives, la fréquence de l'échange d'information est restée à peu près la même, mais il y a eu des améliorations dans la coordination et la communication de l'information aux députés. Le sergent d'armes est un point de contact centralisé.