Résumé de l'entrevue : John McKay[1]

John McKay, député fédéral, a été interrogé par les avocats de la Commission le 19 août 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. Contexte

[1] John McKay est le député fédéral de Scarborough—Guildwood. Il a été élu député pour la première fois en 1997. Il est membre du Parti libéral du Canada. Il est actuellement président du Comité permanent de la défense nationale de la Chambre des communes et a précédemment occupé les fonctions de secrétaire parlementaire du ministre de la Défense nationale et de porte-parole de l'opposition pour la défense. Avant d'être élu au Parlement, il travaillait comme avocat.

2. Les bureaux des députés et les services de TI

[2] M. McKay a expliqué comment les bureaux des députés étaient organisés et financés. Certaines dépenses sont financées directement par la Chambre des communes – comme les locaux des députés à Ottawa – tandis que d'autres sont couvertes par un budget attribué à chaque député.

[3] Les députés se procurent tous leurs appareils et services de TI auprès de la Chambre des communes. Cela inclut le service Internet dans les bureaux de circonscription et dans les bureaux d'Ottawa. Lorsque les députés se rendent à l'étranger, la Chambre

[1] Traduction.

des communes leur fournit un téléphone de voyage et leur donne des conseils sur les choses à faire et à ne pas faire en matière de sécurité.

[4] Les députés et leur personnel disposent d'un certain nombre de comptes de courriel standard fournis par la Chambre des communes. Il s'agit d'un compte général public, d'un compte pour le bureau de circonscription du député, de comptes pour le personnel des députés et d'un compte personnel pour le député.

[5] M. McKay a abordé les différents rôles des députés et leurutilisation des systèmes de TI. Les députés effectuent un travail à la fois parlementaire et partisan. Selon les règles de la Chambre des communes, les députés ne sont pas autorisés à utiliser les ressources de la Chambre – notamment les équipements de TI – pour effectuer des activités partisanes.

[6] Le personnel de M. McKay dispose d'appareils électroniques distincts pour les activités partisanes. M. McKay ne possède pas personnellement d'appareils distincts, mais il utilise un compte de courriel personnel qui n'est pas fourni par la Chambre des communes pour ses activités partisanes.

[7] M. McKay a indiqué que lui et son personnel veillent à respecter la règle interdisant d'utiliser le matériel de la Chambre pour des activités partisanes. Cependant, il a noté que la délimitation entre les activités parlementaires et partisanerie peut parfois être floue et qu'il arrive inévitablement que le matériel de la Chambre soit utilisé par inadvertance pour des activités qui pourraient être considérées comme partisanes.

[8] La Chambre des communes fournit une assistance TI pour les systèmes qu'elle met à la disposition des parlementaires et de leur personnel. M. McKay pense que cela inclut la surveillance de la cybersécurité. Ni la Chambre des communes ni le gouvernement du Canada ne fournissent d'assistance ni de services de cybersécurité pour les appareils ou systèmes de son personnel qui ne relèvent pas de la Chambre des communes.

3. L'Alliance interparlementaire sur la Chine (**IPAC**)

[9] L'Alliance interparlementaire sur la Chine (« **IPAC** ») est un groupe mondial de parlementaires partageant les mêmes idées et s'intéressant aux questions liées à la Chine, comme Taïwan, Hong Kong et le peuple ouïghours. Il s'agit fondamentalement d'un groupe de défense des droits de la personne.

[10] L'IPAC organise des activités dans le monde entier, qui peuvent mener ses membres à prendre des mesures dans les parlements nationaux. M. McKay a donné l'exemple d'une initiative à la Chambre des communes organisée par les membres canadiens de l'IPAC.

[11] Dans chaque pays où il opère, l'IPAC a des membres individuels, ainsi que des coprésidents nationaux, qui sont issus de différents partis politiques. Du point de vue de M. McKay, il n'y a pas de différence notable entre les rôles de coprésident et de membres individuels de l'IPAC vu que les parlementaires peuvent être plus ou moins actifs dans l'organisation à l'un ou l'autre titre.

[12] Quand l'IPAC a été mise sur pied vers 2020, les principaux Canadiens impliqués étaient Garnett Genuis [député du Parti conservateur du Canada] et Irwin Cotler [ancien député du Parti libéral du Canada]. M. Cotler a demandé à M. McKay d'assurer la coprésidence canadienne de l'IPAC aux côtés de M. Genuis. M. McKay a accepté. Il a travaillé sur des questions de droits de la personne liées à la Chine, notamment en tant que président du Groupe d'amitié Canada-Taïwan et en s'engageant dans la lutte contre le travail forcé dans les chaînes d'approvisionnement.

[13] M. McKay a dit que MM. Genuis et Cotler étaient plus actifs que lui dans l'IPAC.

4. Les cyberattaques menées par Advanced Persistent Threat 31

[14] M. McKay a expliqué comment il a été informé d'une cyberattaque visant M. McKay et d'autres membres de l'IPAC.

[15] Aux alentours du 24 avril 2024, M. McKay a eu un appel téléphonique avec M. Genuis et Luke de Pulford, le directeur exécutif de l'IPAC. M. de Pulford a informé MM. McKay

et Genuis que certains membres de l'IPAC avaient été la cible d'une cyberattaque menée par une entité appelée Advanced Persistent Threat 31 (« **APT31** »), incluant eux deux. M. de Pulford a indiqué à M. McKay qu'APT31 avait été identifié comme étant soutenu par le gouvernement chinois et que l'attaque avait eu lieu en janvier 2021. L'IPAC avait récemment obtenu cette information du Federal Bureau of Investigation (« **FBI** ») des États-Unis.

[16] Au cours de cet appel téléphonique, M. du Pulford a expliqué qu'APT31 avait mené une « attaque de reconnaissance par pixel », qui utilisait un courriel semblant provenir d'un site d'information pour collecter des informations de base sur le système informatique du destinataire, comme l'adresse IP et les informations relatives au système d'exploitation. Il a également indiqué que le système de la Chambre des communes n'avait pas été pénétré.

[17] M. de Pulford a également indiqué qu'en 2022, le FBI avait informé les gouvernements de tous les pays touchés – y compris le Canada. Toutefois, ni le gouvernement du Canada ni la Chambre des communes n'avait prévenu M. McKay à ce moment-là.

[18] M. McKay a d'abord été surpris d'apprendre qu'il avait été la cible d'une entité affiliée à la Chine. Auparavant, il n'avait pas accordé beaucoup d'importance aux questions de cybersécurité ni à la possibilité d'être une cible. Cependant, en y réfléchissant davantage, il a commencé à comprendre pourquoi il pouvait être ciblé : ses prises de position sur des questions liées à la Chine, associées à son rôle dans les matières de défense, comme la présidence du Comité permanent de la défense nationale, pourraient faire de lui un sujet d'intérêt pour la Chine.

[19] Un deuxième appel téléphonique a eu lieu, plus tard dans la journée, pour informer tous les membres canadiens concernés de l'IPAC. M. McKay n'y a pas participé, mais il a compris que M. de Pulford transmettrait les mêmes informations que celles qu'il avait fournies plus tôt dans la journée à MM. McKay et Genuis.

[20] Le 25 avril 2024, M. McKay et d'autres membres canadiens de l'IPAC ont reçu un courriel de M. de Pulford[2]. Ce courriel reprenait les mêmes informations que celles que M. McKay avait reçues par téléphone la veille.

[21] Fin avril ou début mai, M. McKay s'est entretenu avec le Président de la Chambre des communes au sujet de la cyberattaque. M. McKay a demandé au Président pourquoi lui et d'autres membres de l'IPAC n'avaient pas été informés par la Chambre des communes de ces cyberattaques. Le Président a indiqué que les systèmes de TI de la Chambre des communes étaient fréquemment la cible de cyberattaques. Si les députés étaient informés de chaque attaque de ce type, il y aurait un flux constant de notifications.

[22] Les membres canadiens de l'IPAC ont souhaité avoir une séance d'information avec le FBI. Celle-ci a été organisée avec l'aide du secrétariat de l'IPAC et a eu lieu au début du mois de mai 2024. Le FBI n'a pas fourni de détails supplémentaires sur la cyberattaque d'APT31, mais a discuté de l'ampleur de la menace de cyberattaque. Le FBI a indiqué qu'il disposait des ressources nécessaires pour enquêter que sur un très petit nombre des cyberattaques dont il avait connaissance.

[23] M. McKay n'a pas discuté des cyberattaques avec le sergent d'armes, le Service de protection parlementaire, le premier ministre, le SCRS, le CST ni les forces de l'ordre.

[24] M. McKay a été interrogé sur la manière dont les responsables canadiens ont été informés de la cyberattaque d'APT31. Il a indiqué qu'il ne disposait pas d'informations de première main, mais qu'il savait qu'en 2022, le FBI avait contacté le Service de protection parlementaire pour l'informer de la cyberattaque. Il a noté que les informations qu'il a reçues de l'IPAC indiquent que le FBI a également informé le gouvernement du Canada. Il n'était pas au courant de discussions entre la Chambre des communes et le gouvernement du Canada.

[2] COM0000485.

5. Les réflexions et les recommandations

[25] M. McKay a considéré les cyberattaques dans le contexte plus large de l'augmentation des menaces de sécurité auxquelles sont confrontés les députés. Au cours de sa carrière parlementaire, M. McKay a constaté que l'environnement politique est devenu de plus en plus toxique et que les menaces directes pour la sécurité des députés se sont multipliées. Cela a été particulièrement vrai au cours des cinq dernières années. Il considère que l'augmentation des menaces à l'encontre des députés a un effet corrosif sur la démocratie.

[26] Les cyberattaques qui le visent, bien qu'elles soient différentes des menaces de sécurité physique auxquelles les députés sont fréquemment confrontés, sont un autre exemple de l'environnement de plus en plus difficile dans lequel les députés doivent évoluer. Cela dit, M. McKay n'a pas indiqué que les cyberattaques comme telles avaient eu un impact considérable sur son travail parlementaire.

[27] Les avocats de la Commission ont demandé à M. McKay comment il évaluait la performance de l'administration de la Chambre des communes et du gouvernement du Canada dans la réponse aux cyberattaques. Il a indiqué qu'il n'avait pas suffisamment de connaissances personnelles pour dire s'ils avaient bien ou mal géré la situation, mais qu'il savait que le système de TI du Parlement n'avait pas été compromis. Il suppose que la situation a été gérée conformément aux protocoles et aux processus en vigueur en 2022. Il a indiqué que la question la plus importante était de savoir si ces protocoles ou processus reflétaient les réalités de 2024, y compris la question de savoir quand les députés devraient être informés qu'ils ont été ciblés.

[28] Il a indiqué que le seuil à partir duquel un député doit être informé qu'il est la cible d'activités d'un État étranger est une question complexe. S'il est fixé à un niveau trop élevé, les députés risquent de ne pas recevoir des informations importantes et de rester vulnérables. S'il est fixé à un niveau trop bas, ils risquent d'être informés d'événements mineurs – comme le flux régulier de cyberattaques ciblant le système parlementaire – ce qui nuirait à la valeur de la notification.

[29] Il a indiqué que, bien qu'il n'ait pas de réponse simple, il pensait qu'il fallait tenir compte à la fois de la nature de la menace et de la nature de la cible. À titre d'exemple, il a indiqué que, les députés jouant un rôle sensible par exemple en tant que membres d'un comité sensible sur le plan de la sécurité, pourraient avoir besoin d'être informés des menaces à un seuil plus bas que les autres.

[30] Il a été demandé à M. McKay qui devrait être responsable de prendre la décision d'informer les députés qu'ils ont été la cible d'un acteur étatique étranger. Il a indiqué qu'il s'agissait également d'une question complexe et qu'il n'avait pas de réponse claire, bien qu'il soit favorable à ce que cette responsabilité incombe à la Chambre elle-même.

[31] D'une part, le Parlement est une branche égale et indépendante du gouvernement. En tant que tel, il devrait être chargé d'assurer la sécurité de ses membres. Cette responsabilité entrainerait l'obligation d'avertir ces derniers des menaces qui pèsent sur leur sécurité. En confiant cette responsabilité à un organisme gouvernemental, on risque de porter atteinte à la séparation des pouvoirs.

[32] D'autre part, il s'est demandé si la Chambre des communes elle-même avait la volonté nécessaire de jouer un rôle de premier plan dans la lutte contre les menaces d'ingérence étrangère dirigées contre les députés. Il a souligné que l'esprit partisan était un obstacle important qui empêchait la Chambre elle-même de remplir cette fonction. Il estime que des responsables non partisans, comme le greffier de la Chambre des communes, devraient jouer un rôle dans la prise de décision à cet égard.

[33] M. McKay a souligné que son point de vue ne visait pas à diminuer le rôle de la communauté de la sécurité et du renseignement. Il a exprimé sa confiance envers les services publics, y compris dans des organismes comme le SCRS et le CST. D'un point de vue pratique, les informations sur les menaces proviendront probablement de ces organismes. Toutefois, il a estimé que les informations sur les menaces pesant sur les députés devraient probablement être transmises à la direction de la Chambre des communes, qui serait alors chargée d'alerter ses membres.

[34] Les avocats de la Commission ont renvoyé M. McKay aux Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et les

parlementaires[3]. M. McKay a indiqué qu'à son avis, l'approche exposée dans ce document serait adéquate dans les mains d'un bon ministre, mais mauvaise dans les mains d'un mauvais ministre. Il a souligné le pouvoir discrétionnaire conféré par les Directives pour déterminer ce qui constitue une menace suffisante justifiant une notification aux députés, ainsi que les circonstances dans lesquelles la notification peut ne pas avoir lieu pour des raisons de sécurité. M. McKay a fait référence à ce qu'il considère comme une approche trop prudente du secret de la part de certains responsables gouvernementaux.

[35] M. McKay a fait remarqué que les Directives ministérielles étaient utiles pour souligner le rôle unique et les vulnérabilités des parlementaires.

[36] On a demandé à M. McKay qui devrait être responsable de la cybersécurité des systèmes non parlementaires utilisés par les députés. Il a indiqué qu'il ne pensait pas que le gouvernement du Canada devrait s'en charger. Il a convenu que les activités partisanes ne devraient pas avoir lieu sur les appareils ni sur les comptes fournis par la Chambre des communes, mais il a suggéré que la Chambre des communes pourrait fournir des fonds aux députés pour qu'ils se procurent leurs propres services de cybersécurité pour leurs systèmes privés. M. McKay ne pense pas que les partis politiques seraient bien placés pour fournir ces services.

[37] M. McKay est d'avis qu'un plus grand nombre de députés devraient avoir une habilitation de sécurité, ce qui leur permettrait d'accéder à des informations classifiées relatives à d'éventuelles menaces d'ingérence étrangère à leur encontre. À titre d'exemple, il a suggéré que les membres de certains comités permanents, comme celui de la défense nationale ou des affaires étrangères, devraient vraisemblablement avoir une telle habilitation. Il a indiqué que les membres de ces comités pouvaient être des cibles attrayantes pour l'ingérence étrangère.

[3] CAN021931.