Résumé de l'entrevue : Garnett Genuis[1]

Garnett Genuis, député fédéral, a été interrogé par les avocats de la Commission le 15 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] Garnett Genuis est le député fédéral de Sherwood Part—Fort Saskatchewan. Il représente cette circonscription électorale depuis 2015. Il est membre du Parti conservateur du Canada. Avant son élection au Parlement, il a travaillé comme membre du personnel politique au fédéral, dans un organisme politique sans but lucratif et dans une société de recherche sur l'opinion publique. Il est diplômé de l'Université Carleton et de la London School of Economics.

[2] Tout au long de sa carrière parlementaire, M. Genuis s'est investi dans les questions internationales relatives aux droits de la personne, en particulier celles touchant la République populaire de Chine (« **RPC** ») et le Parti communiste chinois.

[1] Traduction.

2. L'organisation des bureaux des députés

2.1 L'organisation générale

[3] Les députés disposent d'une grande souplesse dans l'organisation de leur bureau. Tous les députés ont un budget et décident de sa répartition entre leur bureau d'Ottawa et celui de leur circonscription.

[4] Le bureau d'Ottawa de M. Genuis est chargé de l'appuyer dans son travail parlementaire, comme la participation aux comités permanents, les communications sur les questions nationales et les projets de loi d'initiative parlementaire. Son bureau de circonscription s'occupe quant à lui de divers dossiers (aide aux électeurs qui ont des problèmes avec le gouvernement fédéral) et des consultations avec les électeurs. Il n'y a pas de cloisonnement entre ces activités, et le député tient à ce qu'il y ait une bonne communication entre ses deux bureaux.

[5] Le bureau d'Ottawa de M. Genuis est composé de deux à trois employés permanents, soutenus par des stagiaires et des bénévoles. Son bureau de circonscription est composé d'un chef de bureau, d'une réceptionniste et d'un employé à temps partiel.

2.2 Les technologies de l'information (« **TI** »)

[6] La Chambre des communes fournit des services et des équipements de TI aux députés et à leur personnel. Elle fournit à M. Genuis et à ses bureaux des appareils (ordinateurs, téléphones portables, etc.) et le service Internet, et assure une assistance TI en cas de problème technique. Elle est responsable de la cybersécurité liée à ces systèmes.

[7] M. Genuis a expliqué que chaque député effectue à la fois un travail parlementaire et un travail partisan. Le travail partisan ne fait pas partie du mandat en tant que tel, mais chaque député effectue un travail partisan dans une certaine mesure, ce qui inclut des activités comme la collecte de fonds, le maintien des relations avec l'association de sa circonscription électorale et la préparation de la réélection. Bien que son travail partisan soit lié à son statut de député, il ne serait pas approprié, et même contraire aux règles parlementaires, d'utiliser le matériel de TI de la Chambre des communes pour le

réaliser. M. Genuis dispose donc de son propre équipement privé, comme un téléphone portable personnel, pour son travail partisan, ainsi que pour d'autres activités personnelles. La façon dont cette séparation est structurée peut varier d'un député à l'autre, et M. Genuis a souligné qu'il ne pouvait parler que de sa propre expérience, qui peut différer de la manière dont d'autres gèrent cette distinction.

[8] Le service de TI de la Chambre des communes ne fournit pas de soutien pour les appareils ou services de TI privés de M. Genius, y compris son Internet à domicile. M. Genuis effectue certains travaux parlementaires à domicile en utilisant des appareils fournis par la Chambre des communes.

[9] Le Parti conservateur ne fournit pas d'appareils aux parlementaires ni de services de TI pour les appareils personnels. Par contre, il fournit une assistance TI en relation avec des applications particulières du parti.

[10] M. Genuis a dit ne pas avoir connaissance de services particuliers fournis par le Centre canadien pour la cybersécurité aux députés en ce qui concerne la sécurisation de leurs systèmes ou la réponse aux cyberattaques.

[11] Il peut arriver que les travaux parlementaires soient discutés sur des canaux ou des appareils personnels. M. Genuis peut recevoir des communications d'électeurs sur des questions législatives pendant une campagne électorale. En dehors des campagnes électorales, il reçoit également des appels d'électeurs concernant les travaux parlementaires par le biais de canaux personnels, de la même manière que quelqu'un pourrait l'aborder dans une épicerie ou à l'église pour discuter de questions parlementaires. De nombreuses communications peuvent avoir des aspects à la fois partisans et parlementaires, comme un appel avec un donateur potentiel qui implique une discussion sur les projets de loi actuellement à l'étude au Parlement.

[12] M. Genuis a également évoqué une situation dans laquelle un électeur pourrait envoyer un courriel partisan à son compte de courriel parlementaire, qu'il redirigerait ensuite vers son compte de courriel non parlementaire. Il a également expliqué que certaines communications parlementaires qu'il a avec ses électeurs et ses collègues peuvent avoir lieu sur des systèmes de messagerie sécurisés comme Signal, qu'il a installé sur ses appareils personnels.

[13] M. Genuis ne donne pas son numéro de téléphone portable de la Chambre des communes à ses électeurs, mais leur communique de temps à autre son numéro de téléphone portable personnel. Il reçoit donc des appels téléphoniques et des messages textes parlementaires liés à son travail en circonscription sur un appareil privé.

3. Les groupes, les associations et les organisations interparlementaires

3.1 Généralités

[14] Les députés peuvent participer à différents groupes internationaux, associations et organisations de parlementaires.

[15] Certaines organisations, comme les associations parlementaires et les groupes interparlementaires, sont des organismes officiels reconnus par la Chambre des communes. Ces groupes sont soumis à des règlements et reçoivent du financement de la Chambre des communes.

[16] D'autres organisations interparlementaires existent en dehors des structures officielles de la Chambre des communes, auxquelles les députés peuvent adhérer.

[17] L'Alliance interparlementaire sur la Chine appartient à cette dernière catégorie.

3.2 L'Alliance interparlementaire sur la Chine (« **AIC** »)

[18] L'AIC est une organisation internationale composée de parlementaires de tous horizons idéologiques. Elle a été fondée en 2020.

[19] Ce qui unit les membres, c'est la thèse selon laquelle le Parti communiste chinois (PCC) constitue une menace pour la sécurité mondiale et les normes internationales en matière de droits de la personne. Bien que les membres de l'AIC aient des opinions diverses sur la Chine, ils s'accordent à dire qu'il est nécessaire d'élaborer des politiques et des stratégies qui tiennent compte de la menace que représente le PCC, et de répondre à cette menace avec plus de fermeté et d'attention par rapport au risque.

[20] L'AIC est organisée autour d'un secrétariat international qui dispose de son propre budget et de son propre personnel. Dans chaque pays, l'AIC compte à la fois des membres et des coprésidents nationaux, qui sont tous des parlementaires actuels ou anciens. Les coprésidents d'un pays doivent être issus de partis ou de groupements politiques différents.

[21] L'AIC sert de forum pour l'échange d'informations entre ses membres. Elle organise des conférences nationales et internationales, publie des déclarations communes et assure la communication avec les parlementaires membres. M. Genuis a souligné l'intérêt pour les parlementaires d'échanger des idées, des points de vue et des propositions de politiques. Il a noté qu'une bonne idée dans un territoire de compétence peut déboucher sur une action dans d'autres pays grâce à cet échange d'idées.

3.3 La participation de M. Genuis à l'AIC

[22] M. Genuis participe à l'AIC depuis sa création en 2020.

[23] Il entretenait déjà des relations avec Luke de Pulford, cofondateur de l'AIC, dont il est le directeur exécutif. Ian Duncan Smith – un parlementaire conservateur britannique que M. Genuis respecte – a également participé à la mise sur pied de l'AIC. M. Genuis a pensé que l'AIC lui convenait parfaitement, compte tenu de ses activités de défense des droits et de l'attention qu'il porte aux droits de la personne à l'international et à la Chine à titre de député.

[24] M. Genuis a participé à l'AIC à titre de coprésident du Canada, avec deux membres du Parti libéral du Canada : John McKay et Irwin Cotler.

[25] M. Genuis conserve aujourd'hui son rôle de coprésident canadien de l'AIC.

[26] M. Genuis estime qu'il y a environ 20 à 25 membres canadiens de l'AIC.

[27] Invité à décrire son rôle de coprésident, M. Genuis a indiqué que la fonction de coordination y était plus importante par rapport aux autres membres. Il considère que son rôle de coprésident consiste à faciliter l'accès des députés fédéraux canadiens au réseau de l'AIC. En tant que coprésident, il était plus susceptible d'être invité à prendre la parole lors des conférences organisées par l'AIC.

[28] M. Genuis a confirmé qu'à titre de coprésident, il communiquait régulièrement avec le secrétariat international de l'AIC.

[29] M. Genuis a indiqué que les communications de l'AIC étaient généralement envoyées sur son compte courriel personnel, et non sur celui du Parlement. Il pense que c'est le cas en raison de sa relation préexistante avec M. de Pulford, avec qui il communique en utilisant sa messagerie personnelle. M. Genuis a toutefois noté que l'AIC communiquait également avec son personnel en utilisant les comptes de courriel parlementaire.

4. Les cyberattaques menées par le groupe Advanced Persistent Threat 31

[30] Les avocats de la Commission ont interrogé M. Genuis sur sa compréhension d'une cyberattaque coordonnée menée contre les membres de l'AIC au Canada en 2021 par une entité liée à la RPC, et désignée sous le nom de Advanced Persistent Threat 31 (« **APT 31 »**). La discussion a porté à la fois sur la manière dont M. Genuis a eu connaissance des attaques et sur sa compréhension de la manière dont en ont été informés les responsables du gouvernement du Canada et du Parlement.

4.1 La notification des membres de l'AIC

[31] Le 25 mars 2024, une mise en accusation[2] a été rendue publique par un tribunal de district des États-Unis (district Est de New York), accusant sept personnes de s'être livrées à une série de cyberattaques pour le compte du ministère de la Sécurité de l'État du Hubei en RPC. L'acte d'accusation décrit les accusés comme des membres d'APT 31. Il indique que, vers 2021, les accusés ont ciblé les comptes de courriel de différents membres de gouvernements du monde entier qui faisaient partie de l'AIC.

[32] L'AIC a pris connaissance de l'acte d'accusation et a contacté le Federal Bureau of Investigation des États-Unis (« **FBI** »). Grâce à ces communications, l'AIC a confirmé la liste de ses membres dont les adresses électroniques avaient été ciblées par APT 31.

[2] COM0000380.

[33] Au cours du week-end du 19 au 21 avril 2024, M. Genuis a reçu un appel téléphonique de M. de Pulford. Ce dernier a informé M. Genuis qu'il avait été pris pour cible dans le cadre d'une cyberattaque et que l'AIC était encore en train de consulter le FBI pour savoir quelles informations pouvaient être divulguées. Les deux hommes ont convenu qu'il était important que les membres canadiens de l'AIC soient informés et ont organisé deux séances d'information le 24 avril : la première pour les coprésidents de l'AIC et la seconde pour tous les membres canadiens de l'organisation.

[34] Le 24 avril, M. de Pulford a organisé une séance d'information plus détaillée avec M. Genuis et M. McKay. Ils ont été informés, entre autres, de ce qui suit :

a. les cyberattaques ont été menées par APT 31;

b. les États-Unis et le Royaume-Uni avaient tous deux attribué les attaques à la Chine;

c. les attaques ont pris la forme d'une « attaque de reconnaissance par pixel », dans laquelle un « pixel de suivi » avait été incorporé dans une image contenue dans un courriel. Lorsque le courriel est ouvert et que l'image se charge, le pixel renvoie quelques informations limitées, notamment l'adresse IP du destinataire, l'heure et quelques données limitées sur l'appareil, comme le système d'exploitation utilisé;

d. le FBI n'avait pas informé directement les parlementaires concernés en raison de ses propres règles relatives à la souveraineté des États;

e. le FBI avait toutefois notifié les gouvernements des membres de l'AIC concernés en 2022.

[35] M. de Pulford a également fourni des informations sur les mesures qui pourraient être prises pour mieux protéger les appareils des membres de l'AIC.

[36] M. Genuis a été informé que c'était son adresse électronique personnelle qui avait été visée par APT 31.

[37] M. Genuis n'a pas été particulièrement surpris d'apprendre que la RPC l'avait pris pour cible, compte tenu de ses prises de position affirmées sur les questions liées à la Chine. En revanche, il a été surpris d'apprendre que le gouvernement du Canada avait été

informé par le FBI en 2022 et que lui-même n'a été mis au courant des attaques qu'en 2024. Il a noté que le défaut d'informer ne se limitait pas à un seul parti : des membres de divers partis politiques avaient été affectés, y compris le Parti libéral du Canada, mais aucun d'entre eux n'avait été averti. Il a également estimé qu'il y avait une ressemblance entre l'absence d'information donnée aux membres de l'AIC concernés et le fait de ne pas avoir révélé au député Michael Chong qu'il était visé par la RPC.

[38] Plus tard dans la journée du 24 avril 2024, M. Genuis, M. McKay et M. de Pulford ont tenu une séance d'information en ligne pour les membres canadiens concernés de l'AIC. M. de Pulford et d'autres membres du personnel de l'AIC ont dirigé la séance d'information et ont transmis les mêmes informations que celles ayant été fournies à M. Genuis et à M. McKay plus tôt dans la journée. M. Genuis a indiqué que, de manière générale, les parlementaires qui ont assisté à cette séance d'information en ligne étaient déçus du gouvernement du Canada, qui ne les avait pas informés plus tôt de l'incident.

[39] Tous les parlementaires concernés n'étaient pas présents à la séance d'information. Afin de s'assurer qu'ils étaient informés, l'AIC a envoyé un courriel[3] à tous les membres canadiens concernés le 25 avril 2024, contenant les informations fournies lors des séances d'information du 24 avril.

[40] Le 29 avril 2024, M. Genuis a soulevé une question de privilège à la Chambre des communes concernant à la fois les cyberattaques elles-mêmes et le fait que les responsables canadiens n'avaient pas informé les parlementaires touchés. Cette question de privilège est actuellement sous examen au Comité permanent de la procédure et des affaires de la Chambre (PROC).

[41] Le 9 mai 2024, le FBI a organisé une séance d'information en ligne à l'intention des membres de l'AIC du monde entier ayant été touchés. Cette séance n'a pas fourni d'informations supplémentaires sur les attaques elles-mêmes. Le FBI a toutefois donné des conseils supplémentaires sur les mesures de cybersécurité que les membres de l'AIC pouvaient prendre.

[3] COM0000485.

[42] M. Genuis a indiqué qu'il n'avait eu aucune discussion de fond sur les cyberattaques ou le risque d'ingérence étrangère d'origine technologique avec l'administration de la Chambre des communes, les services de police, de sécurité et de renseignement, ou d'autres ministères et organismes gouvernementaux, en dehors de sa participation aux audiences qui se déroulent actuellement au sein du PROC.

4.2 La notification des responsables canadiens

[43] Il a été demandé à M. Genuis de préciser à quel moment il pensait que les responsables canadiens ont eu connaissance des cyberattaques.

[44] M. Genuis a indiqué qu'il croyait savoir que le FBI avait informé le gouvernement du Canada en 2022, et que ce dernier avait informé le service de TI de la Chambre des communes.

[45] M. Genuis comprend également qu'il existe une suggestion selon laquelle le gouvernement du Canada était au courant des cyberattaques en 2021, mais il n'est pas au fait de ce que les représentants du gouvernement ont déclaré savoir à ce moment-là. De même, il ne connaît pas la nature ni la portée des informations échangées par le gouvernement du Canada avec les services de TI de la Chambre des communes, et ne sait pas si cette dernière était autorisée à divulguer ces informations plus avant.

4.3 Les répercussions des cyberattaques

[46] M. Genuis a indiqué que les cyberattaques n'avaient pas eu de répercussions visibles importantes sur sa vie personnelle ou professionnelle, car il supposait déjà que des États étrangers – en particulier la Chine – surveillaient ses activités. Il ne pense pas qu'il soit plausible que la Chine le prenne pour cible en menaçant sa sécurité ou son bien-être sur le sol canadien, bien qu'elle puisse essayer de perturber ou d'influencer son travail d'une autre manière. Toutefois, il utilise davantage les canaux de communication sécurisés qu'auparavant, même s'il le faisait déjà avant d'être informé des attaques. Les conséquences réelles de ces attaques restent inconnues.

[47] M. Genuis comprend également que les cyberattaques ont été infructueuses pour l'essentiel. Il n'a pas connaissance que des membres canadiens de l'AIC aient été visés

par d'autres attaques d'APT 31, et il sait que l'administration de la Chambre des communes a confirmé que les systèmes informatiques de la Chambre n'ont pas été compromis. Les appareils personnels et le système de messagerie privé de M. Genuis n'ont pas fait l'objet d'un examen par la police scientifique visant à déterminer s'ils étaient compromis par l'APT 31.

[48] M. Genuis estime toutefois que le fait que lui et ses collègues n'aient pas été prévenus les a privés de la possibilité de prendre des mesures défensives en temps utile. M. Genuis a suivi les conseils de l'AIC et du FBI en matière de cybersécurité, notamment en désactivant le chargement d'images dans ses courriels. S'il avait été informé des cyberattaques en 2021 ou 2022, il aurait pris ce type de mesures des années plus tôt.

5. Les réflexions sur les cyberattaques et les recommandations

[49] M. Genuis estime que les parlementaires ciblés auraient dû être informés par le gouvernement du Canada des cyberattaques dès que les responsables canadiens en ont eu connaissance. L'administration de la Chambre des communes n'est pas un organisme de sécurité et de renseignement et n'avait donc pas la responsabilité d'avertir les députés. Même lorsque l'administration parlementaire a été informée par le gouvernement, les informations qu'elle a reçues ont pu faire l'objet de réserves, ce qui aurait limité ou empêché la divulgation d'informations aux parlementaires concernés. La responsabilité d'informer les parlementaires aurait dû incomber aux organismes de sécurité et de renseignement comme le Service canadien de sécurité et de renseignement (« **SCRS** »).

[50] M. Genuis a noté les récentes modifications apportées à la *Loi sur le SCRS* dans le projet de loi C-70, qui, selon lui, renforceraient la capacité du SCRS à communiquer des informations en dehors du gouvernement du Canada. M. Genuis a indiqué que seul le temps nous dira si ces amendements seront réellement utiles. Il a fait remarquer qu'il existe un problème culturel au sein du gouvernement canadien en ce qui concerne la déclassification des informations. Il estime qu'une plus grande divulgation des informations peut être un outil efficace pour contrer l'ingérence étrangère.

[51] Lorsqu'il s'agit d'informations classifiées ou sensibles, M. Genuis pense qu'il convient de soupeser l'intérêt public lorsqu'on envisage la divulgation des informations. Il estime également que, dans certaines situations, les cibles de l'ingérence étrangère devraient avoir le droit absolu de savoir. Il a déclaré que les informations précises à fournir dépendaient des circonstances. Il peut être approprié de ne pas divulguer certaines informations, à condition qu'elles soient suffisantes pour permettre à la cible de prendre des mesures pour se protéger. Il serait dans l'intérêt public de permettre aux gens de se protéger contre l'ingérence étrangère, ce qui nécessite d'informer rapidement les personnes visées par les activités d'ingérence.

[52] M. Genuis a été interrogé sur la question de savoir qui des ministres ou des hauts fonctionnaires devraient être responsables des décisions en matière de divulgation. M. Genuis a indiqué que les deux options présentaient des défis. Dans un système de gouvernement responsable, il y a de bonnes raisons de penser que ce sont les ministres qui devraient prendre ces décisions. D'un autre côté, il existe un conflit d'intérêts inhérent au fait que les ministres sont également des acteurs politiques. Les hauts responsables de la sécurité et du renseignement ne sont pas des acteurs partisans, mais peuvent avoir d'autres motifs de non-divulgation. Il est clair que le gouvernement en place est responsable en dernier ressort du bon fonctionnement du système, et que, si le système ne fonctionne pas, la responsabilité ministérielle impose au gouvernement d'en assumer la responsabilité.

[53] M. Genuis a indiqué qu'il serait préférable qu'il y ait des règles ou des lignes directrices claires sur le moment et la manière dont la divulgation d'informations sensibles à des personnes ciblées devrait avoir lieu.

[54] M. Genuis a passé en revue les Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires de mai 2023[4]. Il a confirmé qu'il n'avait pas été informé des cyberattaques en vertu des Directives, et a noté qu'on n'y mentionnait pas si elles s'appliquaient aux événements survenus avant mai 2023. M. Genuis a indiqué que les Directives devraient s'appliquer à tout incident

[4] CAN021931.

passé qui pourrait encore avoir des répercussions actuelles sur le Parlement ou les parlementaires.

[55] Les avocats de la Commission ont renvoyé M. Genuis au paragraphe 3 des Directives, qui traite de la notification des parlementaires lorsque des menaces à la sécurité du Canada sont dirigées contre eux. Les avocats de la Commission ont interrogé M. Genuis sur le fait que l'obligation de divulguer était limitée aux circonstances où la notification était faite « dans la mesure du possible et dans le respect de la loi et tout en protégeant la sécurité et l'intégrité des opérations et des enquêtes de sécurité nationale et de renseignement ». M. Genuis a indiqué que cette formulation laissait une grande marge de manœuvre et pouvait avoir pour conséquence qu'aucune notification ne soit faite dans des circonstances où elle devrait l'être. Il a estimé que la question de la culture du secret du gouvernement était un aspect important qui aurait probablement une incidence sur l'application des Directives.

[56] M. Genuis a évoqué les défis posés par les États étrangers qui ciblent les appareils personnels des particuliers. Il a noté que ce type de ciblage présentait des risques non seulement liés à l'exposition de travaux parlementaires ou d'informations politiquement sensibles, mais aussi à l'exposition des cibles au chantage. Actuellement, le soutien en matière de sécurité pour ces appareils – par rapport aux appareils de la Chambre des communes – est limité.

[57] Il a été difficile de déterminer qui devrait être responsable de la fourniture d'un soutien supplémentaire. Les organismes gouvernementaux auraient les capacités nécessaires pour s'en charger, mais l'accès des acteurs gouvernementaux à des systèmes politiquement sensibles suscite des inquiétudes. Les partis politiques pourraient fournir des appareils ou un soutien, mais des problèmes similaires se poseraient si ces appareils étaient utilisés pour des compétitions internes au sein des partis, comme les courses à la direction ou les courses à l'investiture. Les parlementaires pourraient être autorisés à utiliser leurs appareils de la Chambre des communes pour participer à des activités partisanes, mais cela impliquerait dans les faits une subvention publique pour ce type d'activités. Cependant, M. Genuis a fait remarquer qu'il existe d'autres

domaines dans lesquels des subventions publiques pour des activités de campagne partisane existent déjà.