Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Résumé d'interrogatoire à huis clos : Caroline Xavier, Alia Tayyeb, Sami Khoury*

Les avocats de la Commission ont interrogé des responsables du Centre de la sécurité des télécommunications (« **CST** ») lors d'audiences à huis clos tenues en juillet et août 2024. L'avocat du procureur général du Canada a comparu au nom du gouvernement du Canada et a eu l'occasion d'interroger les témoins. L'audience s'est déroulée en l'absence du public et des autres participants. Le présent résumé présente les éléments de preuve qui, de l'avis de la Commissaire, ne porteraient pas atteinte aux intérêts essentiels du Canada ni de ses alliés, à la défense nationale ou à la sécurité nationale.

Note aux lecteurs :

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

1. Interrogatoire par les avocats de la Commission

1.1 Témoins et éléments de preuves

[1] Caroline Xavier a été nommée au poste de chef du CST et est entrée en fonction le 31 août 2022.

[2] Sami Khoury est le dirigeant principal du Centre canadien pour la cybersécurité (« **Centre pour la cybersécurité** ») et est entré en fonction en août 2021.

[3] Alia Tayyeb a été nommée chef adjointe du Secteur du renseignement électromagnétique (« **SIGINT** ») au CST en 2022. Elle est également responsable des opérations cybernétiques étrangères au CST.

* Traduction.

[4] Les témoins ont confirmé l'exactitude du résumé de leur entrevue et en ont adopté le contenu comme faisant partie de leur témoignage devant la Commission. Le rapport institutionnel non classifié et l'annexe classifiée du CST ont été déposés en preuve.

1.2 Le paysage des menaces : de 2013 à aujourd'hui

[5] M^me^ Xavier a déclaré que le CST publie des rapports sur les cybermenaces nationales, y compris l'IE, depuis au moins 2017. Le CST s'occupe de la collecte de renseignement étranger depuis près de 80 ans. Au cours de cette période, il a eu pour mandat de recueillir du renseignement étranger d'origine électromagnétique. La collecte de renseignement par le CST est guidée par les priorités du gouvernement du Canada en matière de renseignement, qui sont fixées par des décisions du Cabinet.

[6] Le CST observe depuis longtemps des cas d'ingérence étrangère (« **IE** ») dans les institutions démocratiques canadiennes. L'IE est une priorité en matière de renseignement depuis au moins 2016. M^me^ Xavier a déclaré que l'IE avait augmenté au cours des cinq à huit dernières années. Le CST a souligné ce fait dans ses rapports destinés au public, qui comprennent des évaluations nationales des cybermenaces réalisées par le Centre pour la cybersécurité, ainsi que quatre rapports intitulés *Cybermenaces contre le processus démocratique*[1].

[7] Le développement le plus marquant est que la République populaire de Chine (« **RPC** ») est devenue plus audacieuse et plus sophistiquée dans la manière dont elle effectue ses activités d'IE. Le CST en a fait état dans ses rapports sur les cybermenaces contre le processus démocratique. M^me^ Xavier a ajouté que la RPC a eu, et continue d'avoir, un intérêt stratégique important envers le Canada. La Russie, l'Iran et la Corée du Nord constituent également une menace sur le plan de l'IE, bien que le CST ait principalement observé la Russie et la RPC comme étant les deux principaux acteurs intéressés par le Canada. Ces principaux acteurs sont nommés dans les évaluations nationales des cybermenaces produites par le CST et destinées au public.

[1] La dernière édition des *Cybermenaces contre le processus démocratique* a été publiée en décembre 2023 et peut être consultée sur le site Web du CST.

[8] M^me^ Tayyeb a déclaré que l'IE dans les institutions démocratiques n'est pas un phénomène nouveau. Du point de vue du CST, avant 2015, la collecte d'informations sur les menaces d'ingérence et d'influence étrangère se concentrait sur les activités d'espionnage étranger, ainsi que sur la surveillance et l'influence exercées par des puissances étrangères sur les dissidents plutôt que sur l'IE dans les institutions démocratiques. À la suite des informations faisant état de l'ingérence de la Russie dans l'élection présidentielle américaine de 2016, l'IE dans les institutions démocratiques est devenue une priorité en matière de renseignement.

[9] M^me^ Tayyeb a noté que le CST a observé une augmentation des activités d'IE dans le cyberespace. Dans les années antérieures, les activités d'IE tournaient autour des ambassades et des intermédiaires humains. Les acteurs menaçants sont restés à peu près les mêmes depuis 2015, la RPC et la Russie étant les plus prolifiques, l'Inde et l'Iran opérant également dans cet espace. Elle a ajouté qu'un autre pays était plus actif dans la conduite de l'IE au Canada au cours des années antérieures, et qu'il l'est moins aujourd'hui.

[10] Le Canada est une cible moins prioritaire pour les cybermenaces de la Russie que certains de ses alliés, comme les États-Unis. M^me^ Xavier a ajouté que ces faits ont été réitérés dans le dernier rapport du CST sur les cybermenaces contre le processus démocratique.

[11] M. Khoury a déclaré que, bien que le Centre pour la cybersécurité ait été créé en 2018, le CST a été impliqué dans la cybersurveillance dès 2013. Il a décrit une cyberattaque détectée en 2013 contre le Conseil national de recherches du Canada. Cet incident a « ouvert les yeux » sur le fait que des nations étrangères pouvaient utiliser des techniques cybernétiques pour voler la propriété intellectuelle d'une organisation canadienne. Avant 2013, le CST était conscient de l'existence d'une cyberactivité, mais celle-ci était principalement dirigée par des États-nations vers d'autres États-nations (au lieu d'organisations non gouvernementales). Des incidents de ce type ont conduit à la création du Centre pour la cybersécurité. Ce dernier vise à mettre en commun les connaissances et l'expertise techniques du CST avec la société canadienne, en dehors du gouvernement.

[12] M. Khoury a déclaré qu'au fil des ans, le Centre pour la cybersécurité a constaté une évolution des techniques et des tactiques employées. Le CST a observé que des outils étatiques étaient dirigés contre des infrastructures non étatiques, des infrastructures provinciales et des infrastructures municipales. Le Centre pour la cybersécurité a également observé une augmentation de la sophistication des techniques cybernétiques utilisées. Si les quatre principaux acteurs restent les mêmes (Russie, Chine, Iran et Corée du Nord), le Centre pour la cybersécurité a également cité le Royaume d'Arabie saoudite (« RAS ») dans sa plus récente évaluation des cybermenaces destinée au grand public. Les techniques ont évolué, passant du simple espionnage au piratage et aux fuites, puis aux réseaux de zombies qui inondent les médias sociaux de désinformation, pour en arriver à l'utilisation de l'IA afin d'amplifier les récits et de récolter des données massives.

[13] M^me^ Xavier et M. Khoury ont convenu qu'en ce qui a trait au volume d'activité, la RPC est le principal acteur en matière de cybermenaces. M. Khoury a ajouté que cette activité s'est accrue au fil des ans.

[14] M. Khoury a déclaré que le Centre pour la cybersécurité suit les élections nationales dans le monde entier, y compris en ce qui concerne le rôle joué par l'IE dans ces élections. Le Centre pour la cybersécurité a constaté une augmentation constante du niveau d'activité de la menace d'IE lors des élections. M. Khoury a expliqué la complexité de l'attribution de ces activités, notamment en raison de l'utilisation d'intermédiaires.

[15] M^me^ Xavier a déclaré que les auteurs des cybermenaces liés à la RPC et qui ciblent le Canada ont la capacité de mener des activités cybernétiques malveillantes, souvent dans le but de maintenir un accès continu au réseau d'une cible. Des acteurs liés à la RPC ont ainsi été observés en train de tenter de compromettre divers cybersystèmes. La RPC est un adversaire coriace en raison de sa patience et du fait qu'elle est soumise à moins de contraintes qu'un État étranger opérant sous un gouvernement démocratique. M^me^ Xavier a estimé que le Canada et ses alliés étaient néanmoins bien positionnés pour répondre aux cybermenaces liées à la RPC.

1.3 Soutien au Centre pour la cybersécurité et menaces pesant sur les élections

[16] M. Khoury a expliqué que le Centre pour la cybersécurité est en mesure d'aider les paliers infranationaux de gouvernement, comme les gouvernements provinciaux, et qu'il est au courant des « incidents d'État-nation » qui ont été dirigés contre des provinces ou des territoires. Le Centre pour la cybersécurité a aidé les provinces et les territoires à atténuer ces incidents. Par exemple, il a contribué à atténuer une cyberattaque menée contre le réseau du gouvernement des Territoires du Nord-Ouest. Dans sa réponse, le Centre pour la cybersécurité a collaboré avec le commissaire au renseignement et le ministre de la Défense nationale pour mettre en œuvre un déploiement proactif des capacités cybernétiques afin de prévenir ce type d'incidents à l'avenir.

[17] Le Centre pour la cybersécurité a également travaillé avec d'autres gouvernements provinciaux pour déployer ses capacités et protéger leurs systèmes de manière proactive. M. Khoury a déclaré que le Centre pour la cybersécurité collabore actuellement avec une province canadienne pour atténuer les effets d'un grave incident cybernétique et pour aider au déploiement de capacités cybernétiques proactives et préventives.

[18] M. Khoury a déclaré que lorsque le CST a publié son quatrième rapport de la série *Cybermenaces contre le processus démocratique* en décembre 2023, le Centre pour la cybersécurité a organisé une séance d'information à l'intention de tous les directeurs généraux des élections (« **DGE** ») du Canada. Le Centre pour la cybersécurité est en mesure d'apporter son aide lors des élections provinciales à la demande du DGE d'une province. La première demande officielle est venue d'une province qui souhaitait donner une forme définitive à un partenariat entre le Centre pour la cybersécurité et l'organisme responsable des élections provinciales, afin de se préparer aux prochaines élections provinciales et d'évaluer son infrastructure de sécurité. Des discussions sont également en cours avec le DGE d'une autre province. Le Centre pour la cybersécurité participe à une rencontre annuelle des DGE du Canada pour faire le point sur les cybermenaces

qui pèsent sur les élections et voir s'ils souhaitent de l'aide pour défendre leur cyberinfrastructure électorale.

[19] M^me^ Xavier a déclaré que rien n'empêche le CST d'aider les provinces et les territoires. En fait, l'article 17 de la *Loi sur le CST* permet à celui-ci de fournir des conseils et un soutien à l'ensemble du Canada. Elle a souligné qu'une bonne hygiène informatique doit être un effort collectif. Il faut que tout le monde – le gouvernement comme les citoyens – veille à ce que les Canadiennes et les Canadiens restent résilients face aux cyberincidents et aux cyberattaques. Elle a ajouté que le CST travaille également avec Élections Canada pour renforcer l'infrastructure électorale canadienne depuis au moins 2015.

[20] Les avocats de la Commission ont fait référence à un document intitulé [TRADUCTION] « Lutte contre la mésinformation et la désinformation : Élaboration d'un programme émergent de protection de la démocratie »[2], qui indique que l'aire exposée à la menace est plus vaste au niveau des gouvernements infranationaux, parce que leurs processus électoraux ont tendance à s'appuyer davantage sur des moyens électroniques pour le vote. Le document indique également que le Centre pour la cybersécurité n'a pas la capacité de répondre à de multiples demandes parallèles émanant d'administrateurs électoraux de plusieurs provinces.

[21] M^me^ Xavier a déclaré que ce document était obsolète. Au cours des dernières années, le CST a reçu un afflux de financement pour le Centre pour la cybersécurité. Or, le document a été rédigé au cours d'un processus visant à déterminer les besoins du Centre pour la cybersécurité et ne reflète donc pas les ressources actuelles. Depuis le Budget 2022, on reconnaît que le CST est en croissance et qu'il remplit une fonction essentielle dans la défense contre les cybermenaces. En conséquence, le CST a bénéficié d'investissements importants dans le cadre de son mandat.

[22] M^me^ Xavier a déclaré que les solutions numériques pour les élections sont de plus en plus répandues et a recommandé aux utilisateurs d'intégrer des mesures de sécurité dans ces systèmes dès le départ. Le risque demeure, même si des couches de sécurité

[2] CAN019525

existent au sein d'une solution numérique. Toutefois, l'existence de couches de sécurité peut aider à prévenir les pires scénarios. Une approche fondée sur le papier permet de limiter les risques numériques, mais comporte ses propres risques.

[23] Les avocats de la Commission ont référé à nouveau au document [TRADUCTION] « Lutte contre la mésinformation et la désinformation : Élaboration d'un programme émergent de protection de la démocratie », qui traite également de la planification défensive du Centre pour la cybersécurité en relation avec la 43e élection générale (« 43 EG »). Le Centre pour la cybersécurité s'est appuyé sur un nouveau groupe de cyberplanification défensive pour élaborer un plan stratégique d'atténuation. Toutefois, le document indique que ce processus n'a pas été mené lors de la 44 EG en raison d'un manque de ressources disponibles.

[24] Mme Xavier a déclaré que le CST était habilité à mener des cyberopérations défensives pendant les 43 et 44 EG, mais qu'il n'a pas déclenché son plan de cyberdéfense parce qu'aucun incident ne l'y a obligé. Elle a suggéré qu'en raison de cette position défensive, le plan d'atténuation stratégique est devenu inutile pendant la 44 EG.

[25] M. Khoury a ajouté que les capacités défensives du CST étaient prêtes à être activées pendant la 43 EG, mais que cela n'a pas été nécessaire. Le CST a collaboré avec Élections Canada pour garantir la sécurité de son infrastructure.

[26] Mme Xavier a déclaré qu'elle serait surprise que la non-exécution du plan stratégique d'atténuation dans le cadre de la 44 EG soit due à un manque de ressources. M. Khoury partageait son point de vue. Il a ajouté qu'en période électorale, le CST maximise et réaffecte ses ressources à la protection des élections. Mme Xavier a suggéré que le plan stratégique d'atténuation n'a probablement pas été poursuivi parce que d'autres plans défensifs plus efficaces étaient disponibles. M. Khoury et Mme Xavier ont tous deux convenu qu'ils ne s'attendaient pas à ce que le CST se révèle incapable de protéger l'infrastructure électorale en 2025.

1.4 Capacités et menaces cybernétiques de la Chine

[27] Les avocats de la Commission ont fait référence à un document du Centre pour la cybersécurité datant de 2022 qui fournit une évaluation de base des menaces émanant

de la RPC. M. Khoury a confirmé que les capacités cybernétiques de la RPC ont considérablement évolué au cours des deux dernières années et qu'elles sont devenues plus sophistiquées. La RPC a mené des activités contre l'infrastructure infonuagique et se prépositionne sur l'infrastructure critique. Outre ses partenaires internationaux, le CST collabore également avec des organismes multinationaux et des organes de gouvernance pour faire face à la menace de la RPC. M^me^ Xavier a déclaré que la détermination du Canada et de ses alliés à travailler ensemble permettra au groupe de continuer à faire face à la menace posée par la RPC.

1.4.1 Comment les auteurs de menace accèdent-ils aux réseaux?

[28] M. Khoury a expliqué qu'il y a deux principales façons pour un auteur de menace d'accéder à un réseau : (i) il peut trouver une vulnérabilité dans le périmètre du réseau et le pirater directement, ou (ii) il peut utiliser des courriels comme moyen d'hameçonner quelqu'un ou de l'amener à cliquer sur un lien. Lorsque l'utilisateur ouvre un courriel ou clique sur le lien qu'il contient, l'auteur de la menace accède au réseau, franchissant ainsi la limite des défenses externes. Il a employé l'analogie de la porte d'entrée et de l'escalade d'une clôture pour décrire ces méthodes.

[29] M^me^ Xavier a expliqué qu'une fois qu'un adversaire pénètre dans un réseau, son objectif est généralement de voler la propriété intellectuelle ou d'autres informations. Dans d'autres cas, l'auteur de la menace peut ne pas agir immédiatement, mais tenter de se positionner en vue d'un objectif ultérieur.

1.4.2 Campagne ciblant l'Alliance interparlementaire sur la Chine

[30] [En janvier 2021, le CST a appris qu'un auteur, identifié comme étant APT31, menait une opération par courriel visant des parlementaires canadiens, notamment des parlementaires membres de l'Alliance interparlementaire sur la Chine (« **AIC** »), ainsi que l'infrastructure de la Chambre des communes.]

[31] M^me^ Xavier a déclaré que le Centre pour la cybersécurité avait rapidement informé les responsables de la sécurité informatique de la Chambre des Communes de l'opération et qu'il avait collaboré avec eux pour poursuivre l'enquête et recueillir davantage d'informations sur ce qui s'était passé. Il s'agissait de la procédure normale. M^me^ Xavier

a souligné que le CST entretenait de bonnes relations avec les services informatiques de la Chambre des communes et qu'il avait conclu un protocole d'entente avec ces derniers en 2016. Les témoins ont entrepris d'établir une chronologie de l'incident et des communications connexes. Cette chronologie a été fournie et est accessible au public. Elle est intitulée : « Chronologie des événements – Campagne de pistage ciblant des parlementaires canadiens »[3].

[32] Grâce à de multiples conversations et à la mise en commun des connaissances entre le Centre pour la cybersécurité et le personnel informatique de la Chambre des communes, ce dernier a pu identifier les parlementaires qui avaient été ciblés. M[me] Xavier a précisé qu'il était rare que le Centre pour la cybersécurité connaisse le nom exact des personnes visées par une cyberattaque. Elle n'a pas pu dire pourquoi le personnel informatique de la Chambre des communes n'a pas informé les parlementaires qu'ils avaient été ciblés. Toutefois, le risque a été atténué.

[33] M. Khoury a expliqué que la nature de cette campagne consistait à envoyer des courriels aux parlementaires et à leur faire parvenir un lien destiné à exploiter une certaine vulnérabilité. Le personnel informatique de la Chambre des communes a pu supprimer les courriels contenant le lien des boîtes de réception des utilisateurs avant que la plupart des parlementaires n'y aient accès. Dans d'autres cas, les courriels en question ont été bloqués par un pare-feu, ce qui a permis d'atténuer la menace.

[34] M[me] Xavier n'a pas été en mesure de dire ce qui a été fait, le cas échéant, en ce qui concerne les courriels de la sorte envoyés aux adresses électroniques personnelles des parlementaires ciblés (plutôt qu'à celles de la Chambre des communes). Il est interdit au CST de diriger ses opérations vers les Canadiennes et les Canadiens et les personnes se trouvant au Canada, et il ne peut donc pas déployer ses capacités à l'endroit d'une adresse électronique non gouvernementale. Le CST peut fournir des conseils et des orientations en matière de cybersécurité aux Canadiennes et aux Canadiens. Il dispose également d'une ligne d'assistance que les utilisateurs peuvent contacter pour signaler leurs préoccupations et les incidents cybernétiques.

[3] CAN047441. [CAN047442 (version française)]

[35] Les avocats de la Commission ont fait référence à une mise à jour de 2022 du Centre pour la cybersécurité sur les opérations de messagerie électronique de la RPC menées contre les Canadiennes et les Canadiens. Selon cette mise à jour, il est presque certain que les opérations de courriel d'APT 31 continueront à cibler les Canadiennes et les Canadiens, en particulier ceux qui participent à la politique étrangère et à la prise de décision politique du Canada, au moins au cours de l'année à venir. Les avocats de la Commission ont également fait référence à une chaîne de courriels concernant les activités d'APT 31 menée contre l'AIC. En ce qui concerne cette chaîne de courriels, un employé du CST estime qu'APT 31 [TRADUCTION] « n'essayait pas, selon toute vraisemblance, d'interférer *directement* dans les processus démocratiques par le biais du cyberespace (à moins que le terme "interférence" n'englobe l'espionnage) ». L'employé suppose que les renseignements recueillis dans le cadre de ce type d'opération pourraient être utilisés pour éclairer les efforts d'ingérence.

[36] M^{me} Xavier a expliqué que les hommes et les femmes politiques, les électeurs et les infrastructures électorales sont tous des cibles d'ingérence électorale de la part d'acteurs étatiques étrangers, ce que le CST a indiqué dans sa série de rapports *Cybermenaces comme le processus démocratique*, et ce dès le premier rapport publié. Les opérations d'information pourraient être l'une des tactiques utilisées pour faire avancer ces efforts. Le CST considère APT 31 comme un acteur plus largement omniprésent, qui ne se concentre pas spécifiquement sur les élections. Les activités de cybermenace d'APT 31 visent l'espionnage de manière plus vaste et l'ingérence en général. Il est difficile d'affirmer catégoriquement que cette opération de courriel était spécifiquement destinée à interférer dans un processus démocratique.

[37] Elle a ajouté que le Canada peut être une cible involontaire en raison de son rôle dans l'OTAN ou de sa proximité avec les États-Unis.

[38] M. Khoury a déclaré qu'il était difficile de discerner l'intention d'un auteur de menace qui agit sur le plan cybernétique. Un courriel frauduleux peut être un moyen de mettre le pied dans un réseau. Pour évaluer l'intention, il faut examiner les informations techniques en même temps que le contexte.

[39] Les avocats de la Commission ont fait référence à la chaîne de courriels concernant l'activité d'APT 31 menée contre l'AIC. L'un des courriels décrit le compte rendu d'une réunion tenue entre divers organismes de sécurité nationale. Les participants à cette réunion ne savaient pas si les parlementaires concernés avaient été informés du ciblage des membres de l'AIC par APT 31.

[40] M^me^ Xavier a déclaré qu'il y a eu des conversations générales sur le désir de mettre les parlementaires au courant des informations qui les concernent. Des séances d'information à l'intention des parlementaires ont lieu tout au long de l'année. M^me^ Xavier n'a pas pu dire si les parlementaires visés par l'incident de l'AIC avaient été informés.

1.4.3 Directives du ministre sur les breffages à l'intention des parlementaires

[41] M^me^ Xavier a déclaré que le CST considérait les opérations de courriel d'APT 31 menées contre les membres de l'AIC comme le type d'activité visé par les Instructions du ministre à l'intention du SCRS, qui stipulent que le premier ministre, le cabinet du premier ministre (« **CPM** ») et les ministres doivent être mis au courant de manière proactive des informations relatives aux menaces à la sécurité nationale qui pèsent sur les parlementaires et leur famille et que, dans la mesure du possible, les parlementaires ciblés doivent être informés de ces menaces[4].

[42] M^me^ Xavier a fait remarquer qu'à la suite des directives du ministre, elle a également émis une directive au CST demandant que toutes les informations concernant les parlementaires soient signalées afin qu'elles tombent entre les bonnes mains au bon moment pour éclairer la prise de décision du gouvernement. Si ce type d'incident se produisait aujourd'hui, les directives du ministre au SCRS s'appliqueraient probablement et les parlementaires concernés seraient sans doute informés. Le CST n'informerait probablement pas directement les personnes concernées, car il fournit généralement des informations classifiées à des prestataires de services autorisés ou indique les mesures à prendre. Les séances d'information proviendraient probablement

[4] Voir CAN027809. Il convient de noter que les Instructions mentionnées ont été données au SCRS le 16 mai 2023.

du Service canadien du renseignement et de la sécurité (« **SCRS** »), de la Gendarmerie royale du Canada (« **GRC** ») ou du Bureau du Conseil privé (« **BCP** »).

1.4.4 Menaces à l'encontre de députés canadiens

[43] Les avocats de la Commission ont fait référence à un document datant de 2023. M^me^ Xavier a confirmé que cette information serait prise en compte par les Instructions du ministre et la directive du chef. M^me^ Tayyeb a ajouté que la directive du chef exige également que le CST informe immédiatement tous les organismes gouvernementaux responsables, ce qui a été fait dans ce cas. Les témoins ont confirmé que le document a été envoyé à des centaines de clients canadiens, dont le SCRS et la GRC, et qu'il a été signalé au BCP peu de temps après sa publication. M^me^ Xavier a précisé que le CST n'a pas pour rôle d'informer directement les parlementaires d'une quelconque menace. En général, le rôle du CST est d'interagir avec les systèmes et leurs fournisseurs de services. Si le CST recueille des informations révélant une menace envers les parlementaires ou dispose d'informations sur une cybercampagne visant les parlementaires, il veille à ce que ces informations soient communiquées aux responsables, ministères et/ou organismes concernés, qui peuvent déterminer la réponse appropriée. Par exemple, le SCRS pourrait vouloir prendre une mesure de réduction de la menace ou demander l'émission d'un mandat, ou la Gendarmerie royale du Canada (« **GRC** ») pourrait souhaiter enquêter. D'autres organismes s'occupent des affaires intérieures. On a rappelé qu'il est interdit au CST de diriger ses actions vers le Canada.

[44] M^me^ Xavier a déclaré que le CST aurait informé le SCRS, le BCP, la GRC et d'autres partenaires d'informations, comme les responsables de la sécurité de la Chambre des communes, concernant les menaces contre les parlementaires, ainsi que les raisons pour lesquelles une action est justifiée. Il appartiendrait ensuite au SCRS ou à la GRC de déterminer les étapes suivantes.

1.4.5 Progression des capacités cybernétiques de la RPC

[45] L'activité d'influence étrangère en ligne de la RPC est devenue plus sophistiquée ces dernières années. Parfois, la RPC réussit à contourner les mécanismes de détection des faux contenus mis en place par certaines plateformes de médias sociaux.

[46] M. Khoury a déclaré que, selon lui, la RPC dépasse désormais la Russie en ce qui a trait au volume de cyberactivité. M^me^ Tayyeb a fait remarquer qu'il est difficile de comparer les deux pays du point de vue de l'ingérence étrangère.

[47] M^me^ Xavier a déclaré que la RPC s'infiltre dans de multiples espaces, en ligne et autres, auxquels on ne s'attend pas nécessairement, et a décrit la RPC comme jouant à un « jeu de longue haleine ». En ce qui a trait au volume, la RPC pourrait dépasser les activités de la Russie, mais cela est difficile à quantifier. La RPC est fortement impliquée dans le développement de logiciels, la fabrication de téléphones et la mise au point d'applications comme TikTok.

[48] M^me^ Tayyeb a fait remarquer que la RPC réagit à la surveillance mondiale parce qu'elle tient à sa réputation et cherche à éviter l'embarras sur la scène internationale. Ces dernières années, les activités de la RPC au Canada et dans d'autres pays ont fait l'objet d'une plus grande publicité. En conséquence, la RPC a pris davantage de mesures pour mettre ses activités à l'abri de la surveillance.

1.5 Capacités et menaces cybernétiques de la Russie

[49] M^me^ Tayyeb a expliqué que, par le passé, la Russie ne semblait pas avoir l'intention d'interférer directement dans les élections canadiennes. Cependant, la Russie mène depuis longtemps une campagne visant à discréditer les États-Unis et leurs alliés, ainsi que la démocratie occidentale en général. Cela a une incidence sur le Canada et d'autres alliés. M^me^ Tayyeb a ajouté que le CST a observé la présence de cybermenaces russes au Canada, mais qu'elles n'étaient pas dirigées contre les institutions démocratiques canadiennes.

[50] M^me^ Xavier a ajouté que le CST a acquis des connaissances sur d'autres tactiques et techniques russes en observant l'invasion russe en Ukraine.

[51] M. Khoury a ajouté que le paysage cybernétique de la Russie est vaste et complexe. La Russie en tant qu'État est un acteur menaçant, mais il y a aussi des États affiliés, des intermédiaires, des groupes de rançongiciels et des cyberactivistes qui opèrent à partir de la Russie. Ce pays dispose de capacités cybernétiques très avancées dont le Canada doit se méfier. Par exemple, il y a dix ans, la Russie a mis hors service le réseau électrique de l'Ukraine.

1.6 Capacités et menaces cybernétiques de l'Inde

[52] Les avocats de la Commission ont fait référence à un rapport de 2023 du Centre pour la cybersécurité sur la détection des cybermenaces des États émergents. Ils ont également fait mention d'un rapport du Centre pour la cybersécurité de 2023 sur l'Inde. Selon ce document, l'Inde dispose d'un programme cybernétique national de niveau de sophistication moyen. M. Khoury a reconnu que cette évaluation restait exacte.

[53] M^me^ Xavier a déclaré que le CST reconnaît l'Inde comme un État qui aspire à mettre en place un programme cybernétique modernisé. Par exemple, lorsque le premier ministre a évoqué l'assassinat de M. Hardeep Singh Nijjar ou lorsqu'il s'est rendu en Inde, le CST a relevé de la mésinformation et de la désinformation (« **MIDI** »). Le CST est conscient que l'Inde tente de contrer les récits à son encontre et à l'encontre de son gouvernement.

[54] M^me^ Tayyeb a précisé que le CST est au courant des activités menées par l'Inde au Canada. Le Canada est l'une des cibles de l'Inde en raison de l'importance de la diaspora indienne au Canada.

1.7 Mise en commun du renseignement étranger

[55] M^me^ Tayyeb a indiqué que le renseignement recueilli dans le cadre du volet « renseignement étranger » du mandat du CST doit être communiqué au gouvernement du Canada. La *Loi sur le CST* ne prévoit pas de mécanisme permettant au CST d'informer directement les Canadiennes et les Canadiens du renseignement précis qu'il recueille, mais le CST utilise des mécanismes comme son rapport public annuel et

d'autres documents publics pour fournir des évaluations et des avis découlant des rapports de renseignement, des activités de cyberdéfense et de la recherche.

[56] Seules les personnes désignées ayant le mandat d'agir recevront les informations supprimées portant sur l'identité de Canadiens et de Canadiennes. Les intéressés peuvent en demander la liste par le biais d'une procédure particulière. Ils doivent alors justifier les raisons pour lesquelles ils la demandent et doivent prouver qu'ils sont légalement autorisés à la recevoir. M^me^ Xavier a ajouté que ces demandes sont parfois refusées.

1.8 Produits du SIGINT

[57] Les avocats de la Commission ont fait référence à un document du CST intitulé « 2021 – 2023 END Cycle Update Tasking Response » qui décrit une nouvelle catégorie de rapports appelée « produits de renseignement personnalisés » (« Tailored Intelligence Products », ou **TIP**).

[58] M^me^ Tayyeb a expliqué que le CST s'efforce toujours de rendre ses produits de renseignement plus accessibles aux clients, de les adapter aux besoins et d'intégrer le retour d'information des clients.

1.9 Outils de lutte contre l'IE et les cyberincidents

1.9.1 La lutte contre la MIDI dans les environnements nationaux

[59] Les avocats de la Commission ont fait référence à un échange de courriels concernant le travail du CST sur la MIDI. L'un des courriels indique que la recherche sur les campagnes de désinformation, et en particulier l'élaboration d'outils et de techniques pour les détecter, a été limitée en raison de préoccupations réelles ou perçues concernant l'alignement du mandat. Les campagnes de désinformation ne sont généralement pas considérées comme des activités de « cybersécurité ». Par conséquent, les campagnes d'influence malveillantes visant les Canadiennes et les Canadiens et mises en œuvre sur les réseaux sociaux qu'ils utilisent ont été considérées comme « hors du champ d'application ».

[60] M^me^ Xavier a rappelé que le CST ne peut pas orienter son équipement vers des Canadiennes ou des Canadiens ou des personnes se trouvant au Canada. Le CST s'efforce de respecter cette restriction et d'éviter de capter involontairement des données canadiennes. Étant donné que le CST ne peut diriger son équipement vers les Canadiennes et les Canadiens, il n'est pas le mieux placé pour surveiller et éliminer la MIDI dans les environnements nationaux. En revanche, le CST peut donner des conseils sur la MIDI, éduquer les Canadiennes et les Canadiens sur la menace qu'elle représente et mener des actions éducatives pour encourager l'esprit critique au sujet de la consommation d'informations en ligne. Ce point est lié à l'article 17 de la *Loi sur le CST*, qui définit l'aspect cybersécurité et assurance de l'information du mandat du CST. M^me^ Xavier a déclaré que les organismes de renseignement canadiens ne devraient pas diriger leur équipement contre les Canadiennes et les Canadiens qui expriment légalement des points de vue ou des opinions. Les Canadiennes et les Canadiens jouissent d'un droit à la liberté d'expression protégé par la *Charte*. M^me^ Xavier fait remarquer qu'il pourrait être utile de confier à une tierce partie ou à une organisation non gouvernementale le soin d'identifier et de rectifier la MIDI.

[61] M^me^ Xavier a déclaré que le CST peut jouer un rôle dans l'attribution technique de la MIDI en ligne, en particulier lorsque l'identification technique est nécessaire pour déterminer l'origine d'un acteur malveillant. Cependant, il ne peut le faire que lorsque certains indices pointent vers une source de nature étrangère.

[62] M^me^ Tayyeb a ajouté que le CST pourrait être appelé à clarifier la source s'il avait connaissance qu'un acteur étranger se livrait à des activités de MIDI. Toutefois, si les activités proviennent du Canada, le CST n'en aura pas connaissance, à moins qu'il n'y ait du renseignement étranger autour de la MIDI. Le CST ne peut pas enquêter sur une piste nationale, car cela l'obligerait à diriger ses efforts contre une Canadienne ou un Canadien. S'il soupçonne un État étranger d'être impliqué, le CST ne peut qu'examiner le renseignement d'origine électromagnétique étranger pour voir s'il confirme ou infirme le soupçon, et ne peut pas prendre de mesures contre des Canadiens.

[63] M^me^ Xavier fait remarquer que le CST est également en mesure de fournir un soutien technique dans le cadre de son mandat d'assistance. Lorsque ce mandat est activé, le

CST peut offrir une assistance en vertu du mandat et des pouvoirs de l'organisme demandeur. Suite à l'interrogatoire, en réponse à un engagement, le CST a informé la Commission qu'il n'avait reçu aucune demande au titre de son mandat d'assistance en vertu de l'article 20 pour l'attribution technique d'une campagne de MIDI dans le contexte des élections générales ou des processus démocratiques de manière plus générale.

1.9.2 Programme de cyberopérations du CST

[64] Les avocats de la Commission ont fait référence à un document non daté résumant le programme de cyberopérations du CST. Ce document indique que le Canada dispose d'un avantage grâce à ses cyberopérateurs de calibre mondial, mais que [TRADUCTION] « nos alliés et nos adversaires nous dépassent rapidement, tant en termes de portée que d'échelle ».

[65] M^{me} Xavier a expliqué que le Budget 2024 allouait près d'un milliard de dollars au CST au cours des cinq prochaines années, dont une partie est destinée au renseignement étranger et une autre aux opérations cybernétiques à l'étranger. Cette allocation de fonds est en partie due au fait que les nouveaux pouvoirs du CST requièrent une augmentation proportionnelle de ses ressources.

1.9.3 Opérations par courriel

[66] M. Khoury a précisé qu'en ce qui concerne les opérations par courriel, le fait de cliquer sur le lien contenu dans un message permet à un adversaire de pénétrer dans le serveur. Cependant, il arrive qu'un système présente des vulnérabilités faisant en sorte que le simple fait de télécharger le courriel permet la pénétration (c'est ce qu'on appelle une vulnérabilité de type « zéro clic »). Les vulnérabilités de ce type peuvent se manifester par l'entremise de courriels ou de messages textes malveillants. La réception seule peut créer une vulnérabilité, en fonction de la plateforme et de la nature de l'attaque. La rapidité est essentielle pour résoudre ces problèmes.

[67] M^{me} Xavier a expliqué que le CST s'efforce de trouver des moyens de se protéger contre ces acteurs malveillants. Le CST déploie des capteurs sur les systèmes

gouvernementaux qui empêchent les messages malveillants d'atteindre l'utilisateur. Voilà pourquoi il est important de disposer de plusieurs couches de cybersécurité.

1.10 Sensibilisation du public

1.10.1 Sensibilisation des partis politiques

[68] Les avocats de la Commission ont fait référence à un échange de courriels concernant la ligne d'assistance cybernétique. Un courriel indique qu'un seul problème a été signalé à la ligne d'assistance pendant la 43 EG. Aucun problème n'a été signalé à la ligne d'assistance pendant la 44 EG. Le Centre pour la cybersécurité n'a pas demandé aux partis politiques de lui faire part de leurs commentaires sur le service d'assistance téléphonique.

[69] En réponse à une question de la Commission sur le sujet, M^{me} Xavier a déclaré qu'elle ne savait pas pourquoi il n'y avait pas plus d'utilisation de la ligne d'assistance cybernétique. Elle explique que bien que le CST ait communiqué l'existence de la ligne d'assistance avec les membres des partis politiques et les ministres, en 2019, cette ligne était encore une nouveauté. En 2021, elle était mieux connue, mais les gens étaient aussi davantage sensibilisés à la cybersécurité et entretenaient de meilleures pratiques à cet égard. Elle a émis l'hypothèse que les personnes éprouvant des problèmes pouvaient les atténuer elles-mêmes ou s'adresser directement à des plateformes logicielles ou à des plateformes de médias sociaux.

[70] M^{me} Xavier n'a pas pu expliquer pourquoi le CST n'a pas sollicité la rétroaction des partis politiques et a suggéré qu'on y accorde plus d'attention avant les prochaines élections. Elle a ajouté que la ligne d'assistance était disponible en dehors des périodes électorales et qu'elle avait été utilisée entre les élections. Le CST a ainsi reçu des appels entre les élections.

[71] M^{me} Xavier a déclaré que la ligne d'assistance n'a pas été mise à la disposition des candidats aux élections provinciales et territoriales. Le CST et le Centre pour la cybersécurité ont entrepris d'autres initiatives pour faciliter la communication directe avec les provinces et les territoires. Par exemple, le Centre pour la cybersécurité a organisé de nombreuses réunions sur les élections avec les provinces et les territoires.

1.10.2 Sensibilisation du grand public

[72] M^me^ Xavier a expliqué que le CST publie des rapports publics destinés à l'ensemble de la société civile. Il s'efforce de rendre ces rapports les plus accessibles possibles, mais l'objectif premier est d'aider ceux qui travaillent dans le domaine des systèmes d'information à s'assurer qu'ils pratiquent une hygiène de base et qu'ils renforcent la cyberrésilience dans le cyberespace. Le public du CST évolue en même temps que le paysage des menaces.

[73] M. Khoury explique que le CST a également remanié son site Web en fonction des commentaires du public afin de le rendre plus accessible. En outre, le CST a lancé une campagne de sensibilisation du public intitulée « Pensez cybersécurité », destinée à s'adresser aux Canadiennes et aux Canadiens d'une manière non technique. Le CST mène également d'autres campagnes et recueille des données sur l'intérêt accordé au contenu et le succès de chacune d'entre elles. M^me^ Xavier explique que des données récentes sur une campagne de sensibilisation à la MIDI ont montré qu'elle avait été couronnée de succès.

[74] Les avocats de la Commission ont fait référence à un document qui détaille les différents rôles que le CST pourrait jouer dans le cadre du Plan pour protéger la démocratie canadienne, et qui détaille un certain nombre de propositions relatives à la sensibilisation des partis politiques et du public. Par exemple, une proposition suggère que le CST traduise ses documents d'information dans les langues les plus parlées au Canada, notamment le mandarin, le punjabi, le cantonais, l'espagnol et l'arabe.

[75] M^me^ Xavier explique que ce document a été rédigé par une personne travaillant à un niveau plus opérationnel. Il visait à recueillir les suggestions des employés sur les mesures que le CST pourrait prendre pour mieux protéger la démocratie canadienne. Certaines de ces idées ont déjà été mises en œuvre ou sont des points que le CST espère améliorer. Par exemple, le CST a mené des actions de sensibilisation auprès des journalistes et a organisé une séance de « cybersécurité 101 ». Le CST a également traduit des conseils dans les langues autochtones pour informer ces communautés des cybermenaces. M^me^ Xavier a estimé que le CST pouvait faire plus et qu'il continuerait à apporter des améliorations.

2. Interrogatoire par le procureur général du Canada

[76] M^me^ Tayyeb explique que, dans le cadre de son mandat relatif au renseignement étranger, le CST fournit des informations aux organismes gouvernementaux. M. Khoury a ajouté qu'en ce qui concerne la cybersécurité et l'assurance de l'information, le CST procure du soutien en matière de cybersécurité aux systèmes fédéraux ou à d'autres systèmes désignés comme étant importants pour le gouvernement du Canada. Les systèmes des gouvernements provinciaux et territoriaux sont désignés comme étant importants, ce qui permet au CST de les soutenir sur le plan de la cybersécurité.

[77] M^me^ Tayyeb a comparé la facilité d'attribution des cyberincidents et des campagnes de MIDI. Lorsqu'il s'agit d'attribuer un incident ou une activité cybernétique, le CST est en mesure de consulter des services de renseignement étrangers et d'obtenir des détails techniques sur la compromission. Ce renseignement étranger et ces informations techniques peuvent être comparés à la connaissance qu'a le CST des différents acteurs étrangers pour faciliter l'attribution. En ce qui concerne la MIDI, le CST n'est généralement pas en mesure d'obtenir les informations techniques nécessaires à l'attribution parce qu'elles n'existent pas ou n'ont pas été fournies par une plateforme de médias sociaux. Si un acteur étranger utilise des intermédiaires au Canada pour diffuser des messages de MIDI, cela peut compliquer encore davantage la capacité du CST à attribuer la campagne.

[78] M^me^ Xavier a confirmé que le rôle principal du CST est l'attribution technique. Même s'il ne peut identifier un acteur d'un point de vue technique, il peut tout de même émettre une alerte, formuler une orientation ou donner un conseil pour informer les clients des indicateurs de compromission.