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'entrevue : Centre de la sécurité des télécommunications (Caroline Xavier, Rajiv Gupta, Alia Tayyeb)*

Des hauts fonctionnaires du Centre de la sécurité des télécommunications (« **CST** ») ont été rencontrés en entrevue par les avocats de la Commission le 14 juin 2024. L'entrevue s'est déroulée dans un environnement sécurisé et comportait des références à des informations classifiées. Le présent document est la version publique du résumé de l'entrevue classifié déposé en preuve au cours d'audiences à huis clos tenues en juillet et août 2024. Ce résumé divulgue la preuve pertinente qui, selon la Commissaire, ne porterait pas préjudice aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale.

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. Témoins

[1] Caroline Xavier a été nommée cheffe du CST le 31 août 2022. À ce titre, elle est responsable de la gestion et des opérations du CST.

[2] Rajiv Gupta a été nommé dirigeant associé, Centre canadien pour la cybersécurité (« **CCC** »), en juillet 2021. Dans le cadre de ses fonctions de dirigeant associé, M. Gupta est chargé de faire progresser la vision stratégique du CCC afin de sécuriser le Canada sur le plan numérique.

[3] Alia Tayyeb a été nommée cheffe adjointe du Secteur du renseignement

* Traduction.

électromagnétique (« **SIGINT** ») au CST en 2022. Elle est également responsable des cyberopérations étrangères liées au mandat du CST.

2. Évolution du portrait de la menace

2.1 Acteurs clés et mandat du CST

[4] Mme Xavier a expliqué que l'ingérence étrangère est une priorité en matière de renseignement depuis de nombreuses années. Depuis 2017, le CCC a publié quatre rapports publics sur les cybermenaces qui pèsent sur les institutions démocratiques[1]. Ces publications identifient quatre principaux auteurs de menaces : la République populaire de Chine (« **RPC** »), la Russie, l'Iran et la Corée du Nord. La RPC et la Russie mènent la plupart des cyberactivités dont la responsabilité a été attribuée et qui ciblent les élections étrangères. Toutefois, en 2022, 85 % de ces cyberactivités malveillantes n'avaient pas été attribuées.

[5] Comme il a été souligné dans le dernier rapport sur les menaces contre le processus démocratique, publié en décembre 2023, Mme Xavier a déclaré que la mésinformation et la désinformation sont omniprésentes. Les politiciens, les candidats et les électeurs sont les principales cibles de la mésinformation et de la désinformation exacerbées par l'intelligence artificielle (« **IA** »). La cybersécurité revêt une importance particulière. Le CST a indiqué dans ses diverses publications que les infrastructures essentielles [dont les processus, les systèmes, les installations, les technologies, les réseaux, les biens et les services essentiels à la santé, à la sûreté, à la sécurité et au bien-être économique des Canadiens et au fonctionnement efficace du gouvernement] sont vulnérables aux cyberattaques et à d'autres cyberincidents. La protection des infrastructures essentielles fait partie du mandat de cyberassurance

[1] Le plus récent s'intitule « Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023 » et se trouve sur le site Web du CST. Il s'agit de la quatrième version du rapport du CST sur les cybermenaces qui pèsent contre le processus démocratique du Canada, et il fournit une mise à jour des rapports de 2017, 2019 et 2021. Le CCC publie aussi régulièrement une évaluation des cybermenaces nationales. Il l'a fait en 2018, en 2020 et, plus récemment, en 2023-2024

du CST.

[6] Mme Xavier a expliqué que le CST avait acquis une meilleure connaissance de la gamme des cybertactiques étrangères en observant celles employées par la Russie pendant la guerre en Ukraine, de même que grâce aux renseignements exploitables du CST. Ce faisant, le CST a enrichi sa base de connaissances sur les cybertactiques et techniques. Mme Xavier a indiqué que certains auteurs de cybermenaces de la RPC se « pré-positionnent » en piratant les systèmes des infrastructures essentielles et en conservant l'accès à ces systèmes afin d'en affecter ultérieurement le fonctionnement. Cette technique, parfois appelée « attaque hors sol », consiste à utiliser des outils et des processus légitimes pour s'intégrer aux activités normales du système et mener à bien ses opérations discrètement, réduisant ainsi la probabilité de détection ou de blocage. Mme Tayyeb souligne que le CST a observé un auteur de menaces, « Volt Typhoon », utiliser cette tactique.

[7] M. Gupta a expliqué que, pour lutter contre les cybermenaces dans le contexte des institutions démocratiques, le CST fournissait des conseils et des directives sur l'infrastructure électorale. Il a lui aussi indiqué que la mésinformation et la désinformation, qui circulent au moyen de techniques d'intelligence artificielle comme le clavardage synthétique, les hypertrucages et d'autres types d'activités de « réseau de zombies », étaient devenues courantes.

[8] M. Gupta a précisé que les systèmes fédéraux n'étaient pas les seuls systèmes ciblés. Les provinces, les territoires, les municipalités et les gouvernements autochtones sont également exposés à un tel risque. Dans certains contextes, le CST aide à protéger d'importants systèmes provinciaux, territoriaux et municipaux, comme l'infrastructure électorale provinciale et territoriale, à condition que ces systèmes fassent partie des infrastructures essentielles, lesquelles s'inscrivent dans le mandat de cybersécurité du CST.

[9] Mme Xavier a ajouté que les provinces, les territoires et les municipalités disposaient de moins de ressources pour faire face aux cybermenaces. Elle a déclaré que le CST

collaborait avec les provinces et les territoires pour fournir des conseils et des directives. Le CST a obtenu une autorisation ministérielle pour fournir un soutien technique aux territoires et a épaulé d'autres entités non fédérales qui ont été désignées comme étant des systèmes d'importance. Bien que le CST ait obtenu cette autorisation récemment, il avait déjà aidé les territoires dans le cadre de son mandat de cyberassurance. Le CST déploie des efforts afin d'intervenir en cas de cyberincidents et de prévenir de tels incidents. Le CST a commencé à diffuser des directives dans les langues autochtones, en plus du français et de l'anglais.

2.2 Tactiques et techniques particulières

[10] Mme Tayyeb a expliqué que le CST se concentrait actuellement sur la surveillance des activités d'ingérence étrangère menées par la RPC, la Russie, l'Inde et l'Iran. En réponse à une question sur les nouvelles tendances et techniques en matière d'ingérence étrangère, elle a indiqué qu'outre les cybertechniques traditionnelles, le CST avait observé des auteurs de menaces effectuer la collecte de mégadonnées pour des campagnes d'influence et tirer parti des ressources de leur propre appareil gouvernemental et d'autres organismes de communication. Mme Xavier a expliqué que les acteurs étatiques et non étatiques étaient de plus en plus difficiles à distinguer, car les cybercriminels agissent au nom des États en tant que cybermandataires.

[11] En ce qui concerne les autres nouvelles tendances, Mme Tayyeb a souligné le recours croissant de la Russie aux médias d'État internationaux aux fins de l'amplification de ses campagnes d'influence. De plus en plus, la RPC exerce ses activités au moyen de réseaux non traditionnels en sous-traitant à des acteurs non étatiques, dont des entités affiliées au Département du travail sur le front uni. Mme Tayyeb a également fait référence aux tactiques employées par la RPC, comme la manipulation de l'information, l'élaboration de faux récits et la propagation de mésinformations et de désinformations.

[12] Mme Xavier a déclaré que la dernière évaluation des cybermenaces nationales

réalisée par le CST, publiée en 2022, montre que les groupes de diaspora sont de plus en plus pris pour cible, notamment au moyen de la surveillance du contenu des applications étrangères et des activités liées aux médias sociaux. Elle a expliqué que le but des évaluations des cybermenaces publiées par le CST était de cerner les tendances et d'aider les Canadiens à comprendre l'environnement de menace lié à l'ingérence étrangère. M. Gupta a souligné que le Citizen Lab, un groupe de recherche indépendant, avait publié des travaux sur l'ingérence étrangère et les diasporas au Canada.

3. Cybermenaces et programmes

3.1 Cyberprogramme de la RPC

[13] Les participants ont confirmé que le Cyberprogramme de la RPC, une vaste initiative qui s'appuie sur la capacité collective des services de renseignement de la RPC de même que sur un écosystème plus vaste d'acteurs étatiques et non étatiques, possédait des capacités qui posent une grande menace pour le Canada et ses alliés. M. Gupta a décrit le caractère incessant des activités de menace menées par le Cyberprogramme. Il a affirmé que les efforts du Cyberprogramme, compte tenu de la participation d'acteurs étatiques et non étatiques, étaient considérables et continus. Le CST a observé que la RPC menait des cyberactivités persistantes contre les systèmes canadiens.

[14] En réponse à cette situation, le CST tire parti de ses pouvoirs pour mener des cyberopérations actives (« **COA** ») ainsi que des cyberopérations défensives (« **COD** »). Les cybertechniques utilisées par la RPC éclaireront la façon dont le CST défendra l'infrastructure du Canada contre les menaces futures prévues.

[15] M. Gupta a indiqué qu'un auteur de cybermenaces lié à la RPC était l'un des plus importants et des plus sophistiqués qui ciblent actuellement le Canada. Cet auteur de menaces a la capacité de mener des cyberactivités malveillantes, souvent dans le but de maintenir un accès continu au réseau d'une cible. Cet auteur de menaces a été

observé en train de tenter de compromettre les systèmes des gouvernements fédéral, provinciaux et territoriaux et de prendre pour cible des représentants du gouvernement, des chercheurs, des politiciens et d'autres personnes. Le CST a récemment publié un document non classifié au sujet de cet auteur de menaces, bien qu'il ne le nomme pas.

[16] Mme Xavier a souligné que le programme de cybersécurité du CST était efficace. À l'heure actuelle, par exemple, le CST met fin quotidiennement à près de six milliards de cyberattaques malveillantes contre les systèmes du gouvernement fédéral. Chaque action représente une occasion de découvrir des renseignements sur l'activité menaçante.

3.2 Défense des systèmes du gouvernement fédéral

[17] M. Gupta a déclaré que le CST utilisait divers capteurs automatisés sophistiqués pour défendre les systèmes du gouvernement du Canada. Ces capteurs surveillent les flux d'information qui entrent dans les systèmes gouvernementaux et qui en sortent. Les capteurs aident à détecter les activités suspectes et les cyberattaques. Le programme a été déployé sur un certain nombre d'années et couvre maintenant la plupart des ministères fédéraux. Le CST a récemment commencé à installer ces capteurs sur des ordinateurs portables fournis par le gouvernement, ce qui a accru la couverture des menaces du CST.

[18] M. Gupta a ajouté que, depuis 2019, le CST utilisait également des capteurs pour surveiller l'infrastructure d'Élections Canada afin d'appuyer cette organisation et d'assurer l'intégrité de ses systèmes.

[19] Toutefois, M. Gupta a précisé que le fait d'avoir plus de capteurs n'éliminait pas tous les risques de cyberactivité malveillante. La meilleure façon d'atténuer les risques consiste à mettre en place de multiples niveaux de protection, ce qui inclut un public averti. M. Gupta a fait remarquer que le CST avait relevé des cyberattaques dans 26 % des élections internationales observées à l'échelle mondiale en 2022, ainsi que de

la mésinformation ou de la désinformation dans 100 % de ces élections.

3.3 Défense des systèmes des gouvernements provinciaux et territoriaux

[20] Mme Xavier a indiqué que le CST collaborait également avec les gouvernements provinciaux et territoriaux, notamment en plaçant des capteurs dans leurs systèmes quand ceux-ci sont considérés comme des systèmes importants et quand cela est jugé approprié. Le CST effectue de telles interventions en vertu d'une autorisation ministérielle qui lui permet d'aider les provinces et les territoires sur demande.

[21] M. Gupta a parlé d'un cyberincident qui a touché les systèmes gouvernementaux des Territoires du Nord-Ouest. Le CST a exercé les pouvoirs qui lui étaient conférés par l'autorisation ministérielle afin de lutter contre l'incident cybernétique. Bien que le CST puisse indiquer la meilleure marche à suivre, il revient ultimement au territoire de mettre en œuvre les solutions proposées par le CST. M. Gupta a ajouté que le CST recevait de plus en plus de demandes d'aide de la part des provinces et des territoires.

[22] M. Gupta a également décrit une cyberattaque menée contre des systèmes de TI essentiels qui soutiennent les fournisseurs de soins de santé à Terre-Neuve-et-Labrador. Le CST a aidé la province à contenir et à contrer l'attaque.

4. Autres incidents précis liés au renseignement

4.1 Postes de police étrangers

[23] Les avocats de la Commission ont présenté aux témoins des documents classifiés concernant la présence de postes de police chinois au Canada.

[24] Mme Tayyeb a affirmé que le CST était au courant de l'existence de ces postes de police, dont le mandat consiste officiellement à fournir de l'aide d'ordre administratif aux citoyens de la RPC et aux personnes d'origine chinoise vivant à l'étranger, mais qui se livrent également à des activités de répression transnationale.

4.2 Accès des acteurs étrangers aux réseaux du gouvernement du Canada

[25] Les avocats de la Commission ont présenté aux témoins un courriel dans lequel un employé du CST exprime son désaccord à l'égard d'une déclaration du Service canadien du renseignement de sécurité (« **SCRS** ») concernant des campagnes menées par des acteurs étrangers pour accéder aux réseaux du gouvernement du Canada. Mme Xavier a expliqué qu'il n'était pas rare que des personnes au sein du CST et du SCRS ne soient pas d'accord ou aient des interprétations ou des évaluations différentes de certains renseignements, compte tenu de leurs différents points de vue opérationnels.

4.3 Suivi du signalement d'une potentielle activité d'ingérence étrangère en 2021

[26] Mme Tayyeb a déclaré que le CST n'avait pas de mise à jour à présenter au sujet des renseignements détaillant de l'ingérence étrangère potentiellement commise par un représentant d'un État étranger, qui ont été recueillis et signalés au Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections après les élections de 2021.

4.4 Collecte de renseignements par les organismes affiliés au Département du travail sur le front uni

[27] Le CST sait que les organismes affiliés au Département du travail sur le front uni souhaitent recueillir des renseignements sur les parlementaires canadiens afin d'exercer une influence sur eux.

5. Rôle du CST dans l'attribution des cyberincidents

[28] Mme Xavier a précisé que l'attribution de la responsabilité à l'égard des incidents faisait partie de la trousse d'outils employée par le CST pour traiter l'ingérence étrangère. Lorsqu'un cyberincident survient, la priorité absolue du CST est de le

contenir et de l'arrêter. En général, le CST ne prend pas de mesures actives pour attribuer la responsabilité d'un incident jusqu'à ce que celui-ci soit maîtrisé. Le processus d'attribution exige beaucoup de travail technique.

[29] M. Gupta a ajouté que plus le CST disposait de renseignements sur l'environnement de menaces, les techniques courantes et le cyberincident lui-même, plus il est facile d'attribuer la responsabilité de celui-ci. Si un incident concerne un comportement nouveau, il faudra peut-être plus de temps au CST pour en attribuer la responsabilité.

[30] Mme Tayyeb a établi une distinction entre l'attribution de cyberévénements et l'attribution de campagnes de mésinformation et de désinformation. Souvent, le CST ne dispose pas de suffisamment de renseignements sur l'environnement de source ouverte ou les données techniques pour attribuer en toute confiance la responsabilité de campagnes de mésinformation et de désinformation. Il est également difficile d'attribuer la responsabilité de cyberévénements, mais quand le CST peut obtenir des renseignements techniques auprès de la partie touchée, ceux-ci peuvent être utilisés pour apporter des correctifs afin de contrer les tactiques et les techniques de cyberacteurs connus. Le CST peut également disposer de renseignements étrangers sur les activités et les intentions des auteurs de menaces, ce qui peut faciliter le processus d'attribution.

[31] Mme Xavier a fait la distinction entre l'attribution technique et l'attribution publique. Le CST s'occupe de l'attribution technique, c'est-à-dire de déterminer qui est à l'origine du cyberévénement. L'attribution publique relève du portefeuille d'Affaires mondiales Canada (« **AMC** ») et de Sécurité publique Canada (« **SP** »). Ces organisations ont élaboré un cadre d'attribution des cyberincidents pour déterminer s'il convient d'attribuer publiquement la responsabilité d'un cyberévénement et comment procéder, le cas échéant.

[32] Mme Xavier a expliqué qu'elle pouvait exprimer un point de vue sur la question de savoir si l'attribution publique était souhaitable, mais qu'elle n'était pas responsable de la décision finale quant à l'attribution publique d'un cyberévénement. Il peut être

souhaitable d'attribuer publiquement la responsabilité d'un cyberévénement pour sensibiliser le public, ou pour des raisons de sécurité. Dans d'autres circonstances, l'attribution publique peut ne pas être souhaitable en raison de conséquences diplomatiques ou parce que cela révélerait les techniques ou les tactiques du CST, ou même d'autres renseignements sensibles en matière de sécurité nationale.

[33] Mme Xavier a fait aussi remarquer que les rapports publics du CST constituaient également une forme d'attribution. Dans la mesure du possible, les cyberacteurs sont identifiés dans les rapports du CST. Le CST attribue également les mesures aux auteurs de menaces et nomme des États étrangers précis dans ses rapports publics. Il s'agit là aussi d'une forme d'attribution, appelée « attribution avec un petit "a" ».

6. Collecte, diffusion et suivi des renseignements

6.1 Nouveau processus pour les hauts fonctionnaires

[34] Les avocats de la Commission ont présenté aux témoins un courriel de M. Dan Rogers, actuellement conseiller adjoint à la sécurité nationale au Bureau du Conseil privé (« **BCP** »), dans lequel il affirme que le rapporteur spécial indépendant (« **RSI** ») a relevé des lacunes dans la façon dont la communauté de la sécurité nationale diffuse les renseignements et en assure le suivi, et propose de mettre sur pied un groupe de travail pour évaluer les solutions.

[35] Mme Xavier a déclaré qu'à la suite du rapport du RSI, le CST avait redoublé d'efforts afin de veiller à ce que les renseignements soient bien reçus et compris. Elle a indiqué que le CST faisait déjà une grande partie de ce qui était recommandé dans le rapport, mais qu'il avait participé à un groupe de travail chargé d'examiner la manière dont les renseignements sont transmis aux clients gouvernementaux et dont était effectué le suivi à cet égard. L'objectif du groupe de travail était de déterminer les pratiques exemplaires. Mme Xavier a indiqué que le groupe avait donné suite à diverses recommandations, ce qui a permis au SCRS et au CST de mieux savoir qui

lisait quels renseignements ainsi que de tirer parti des outils dont ils disposaient pour s'assurer que les renseignements atteignaient les publics appropriés. Le travail du groupe a abouti à la mise en place d'un nouveau système de diffusion et de suivi des renseignements transmis aux hauts fonctionnaires, lequel est décrit dans un document intitulé « Diffusion et suivi des renseignements pour les hauts dirigeants et le personnel politique ».

[36] Mme Tayyeb a expliqué que le nouveau processus tenait compte du fait qu'un groupe central de ministres responsables de la sécurité et du renseignement avait besoin d'un soutien spécialisé. Le nouveau processus permet également au SCRS d'utiliser la plateforme de diffusion et de suivi du renseignement du CST. Enfin, le nouveau processus continue de miser sur les agents des relations avec la clientèle (« **ARC** »)[2]. Le SCRS a également affecté à Sécurité publique un agent d'information chargé d'aider à gérer la diffusion des renseignements.

[37] Le réseau d'ARC continue de s'agrandir. Mme Tayyeb explique que le CST cherche toujours des solutions pour accroître la capacité des ARC et répondre aux besoins des clients du gouvernement.

6.2 Critères de diffusion aux hauts fonctionnaires

[38] Mme Tayyeb a déclaré que les renseignements étaient transmis aux hauts fonctionnaires du gouvernement en fonction d'une analyse des priorités en matière de renseignement et de la rétroaction des ministères et des fonctionnaires au sujet de leurs besoins et préférences à cet égard. Habituellement, c'est le sous-ministre compétent qui détermine quels renseignements seront transmis à son ministre. Au CST, la cheffe ou son délégué décide quels renseignements sont transmis au ministre de la Défense nationale. Dans tous les cas, la décision quant aux renseignements qui devraient être communiqués est guidée par les besoins du Canada en matière de

[2] Les employés du CST hébergés dans d'autres ministères, chargés de communiquer les renseignements du CST aux fonctionnaires de ces ministères.

renseignement.

[39] Mme Tayyeb a précisé que le CST ne choisissait pas unilatéralement les renseignements fournis aux hauts fonctionnaires. Ce sont plutôt les hauts fonctionnaires et d'autres clients qui déterminent les domaines d'intérêt et demandent des renseignements précis au CST. Le CST répond à ces besoins. Le CST fait le suivi des demandes et utilise la rétroaction des clients pour ajuster ses activités de collecte et de diffusion de renseignements afin de mieux répondre aux besoins des clients du gouvernement. Le CST dresse une liste des renseignements qu'il juge intéressants ou pertinents, en fonction de ce qu'il sait, et la distribue aux sous-ministres responsables de la sécurité et du renseignement, dont le conseiller à la sécurité nationale et au renseignement.

6.3 Séances d'information et renseignements concernant les députés

[40] Les avocats de la Commission ont présenté aux témoins la note de service CAN027809 datant de mai 2023 qui indique que le CST et d'autres organismes du portefeuille de la sécurité publique élaborent des mesures internes pour veiller à ce que leurs ministres respectifs soient informés de manière proactive de toute menace pour la sécurité des députés et des membres de leur famille, cela en réponse à une directive du premier ministre selon laquelle lui-même et les ministres doivent être informés de manière proactive de telles menaces.

[41] Mme Xavier a expliqué que le CST fonctionnait déjà selon les directives du premier ministre. Tous les renseignements de grande importance sont signalés au ministre, y compris les renseignements relatifs aux députés ou les menaces à leur endroit. Néanmoins, Mme Xavier a émis une directive enjoignant expressément au CST de signaler tout renseignement recueilli qui touche des parlementaires.

7. Cyberopérations

7.1 Cyberopérations actives et défensives en général

[42] Mme Xavier a expliqué que les modifications législatives de 2019 avaient permis au CST de mener des COA et des COD (ensemble, désignées sous le terme de « cyberopérations étrangères », ou COE). Les COE visent à protéger le bien-être des personnes vivant au Canada. Mme Xavier a déclaré que les COA étaient plus utiles pour combattre l'ingérence étrangère.

[43] Mme Tayyeb a indiqué que le CST devait obtenir des autorisations ministérielles pour mener des COA. À l'heure actuelle, le CST détient un certain nombre d'autorisations ministérielles, dont une qui lui permet de mener des COD contre toute activité visant des systèmes du gouvernement fédéral ou des systèmes désignés comme étant d'importance (tels que définis par le gouvernement fédéral).

7.2 COE particulières

[44] Mme Tayyeb a fait savoir que le CST avait mené une cyberopération particulière contre un adversaire et fourni des détails sur cette opération.

7.3 Limites sur le plan des ressources

[45] Mme Xavier a affirmé que la cyberguerre était devenue un élément essentiel de la défense nationale. En 2022, le CST a reçu une injection de fonds du gouvernement pour lutter contre les cyberactivités hostiles.

[46] Les avocats de la Commission ont présenté à Mme Xavier le document CAN041952, intitulé « Cyberopérations canadiennes », publié en mars 2024. Ce document offre un tour d'horizon du cyberespace canadien ainsi qu'un résumé de la capacité du CST à mener des cyberopérations; il fait état d'un manque de capacité. Mme Xavier a déclaré que la capacité du CST à mener des cyberopérations avait augmenté depuis la préparation du document. Mme Xavier a expliqué que, le CST ayant démontré ce qu'il était capable de faire, des ressources supplémentaires lui avaient été accordées

dans le Budget de 2024, ce qui a augmenté sa capacité de mener plus de cyberopérations à la fois. Le taux de croissance a été jugé raisonnable, surtout compte tenu du défi que doit relever le CST pour attirer des employés possédant les connaissances spécialisées nécessaires et les maintenir en poste.

7.4 Autres contraintes

[47] La Loi sur le CST prévoit que, pour obtenir une autorisation du ministre de la Défense nationale pour mener des COA ou des COD, le ministre doit être convaincu que l'objectif de la cyberopération ne peut être atteint par d'autres moyens raisonnables. Les avocats de la Commission ont demandé si cette condition préalable constituait un obstacle pour le CST. Mme Tayyeb est d'avis qu'il ne s'agit pas d'un obstacle, car le CST n'interprète pas cette disposition comme exigeant que la cyberopération soit une mesure de « dernier recours » ou le seul moyen disponible pour atteindre un objectif. Les autres participants n'ont pas relevé d'autres problèmes ou lacunes sur le plan législatif.

[48] Mme Tayyeb a fait valoir que la contrainte législative qui influe le plus sur l'efficacité opérationnelle du CST est le fait que ses activités ne doivent pas viser les Canadiens ou l'infrastructure au Canada. Elle n'a pas suggéré de supprimer ou de modifier cette contrainte. Celle-ci limite la capacité du CST de recueillir des renseignements et de défendre le cyberespace canadien. Cependant, Mme Tayyeb a expliqué que ce type de limitation à l'égard du renseignement électromagnétique et des cyberopérations était courant dans d'autres pays. Elle comprend que d'autres pays se ont des règles différentes régissant les cyberopérations, par opposition à la collecte de renseignements étrangers. Elle a souligné que le CST devait toujours tenir compte des répercussions sur les Canadiens et veiller à ce que ses activités soient conçues de manière à ce que leurs effets ne soient pas dirigés contre les Canadiens. De plus, les identités canadiennes sont supprimées dans les rapports de renseignement du CST et ne peuvent être divulguées qu'au moyen d'une procédure officielle gérée par une équipe spécialisée du CST.

[49] Interrogé sur la capacité du CST à exploiter des renseignements de sources ouvertes (« **OSINT** »)[3], M. Gupta a expliqué que, dans le cadre du volet cybersécurité du mandat du CST, sa capacité à acquérir des renseignements de source ouverte ou des renseignements commerciaux sur les menaces à la cybersécurité était limitée dans une certaine mesure par le fait que le CST ne peut pas acquérir directement les renseignements sans autorisation ministérielle, si cela porte atteinte aux attentes raisonnables en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

[50] Mme Xavier n'a relevé aucun problème concernant le fait que le CST relève du ministre de la Défense nationale. Mme Xavier a souligné que le mandat du CST consistait à protéger les Canadiens. Les participants ont expliqué que le CST vivait dans « trois mondes », et que son mandat décrivait clairement sa participation aux affaires internationales, à la défense et à la sécurité. Compte tenu des liens opérationnels et historiques entre le CST et les Forces armées canadiennes, ainsi que de l'importance du renseignement électromagnétique pour les capacités de défense nationale du Canada, il est logique que le CST relève du ministre de la Défense nationale.

8. Sensibilisation

8.1 Sensibilisation du public

[51] Mme Xavier a indiqué que le CST menait régulièrement des activités de sensibilisation du public au moyen de publications comme les évaluations des cybermenaces nationales, les visites dans des écoles secondaires et des centres communautaires dans le but d'interagir avec les jeunes, ou l'organisation d'événements comme des marathons de programmation. Elle a mentionné que le CST avait commencé à publier certains de ses documents destinés au public en

[3] Renseignements qui ne sont pas classifiés et qui peuvent être trouvés en ligne, par exemple.

langues autochtones, en plus du français et de l'anglais.

[52] M. Gupta a expliqué que le CST avait collaboré avec des équipes de marketing pour s'assurer que ses publications atteignent les auditoires canadiens. Le CST assure un suivi régulier de son lectorat. Il aimerait recevoir des recommandations sur la façon de mieux faire connaître les publications et les documents d'orientation qu'il produit auprès du public.

8.2 Communications et collaboration avec des partenaires internationaux

[53] Mme Tayyeb a déclaré que le CST faisait face à peu ou pas d'obstacles à l'interaction avec des partenaires internationaux. Le CST a besoin d'un protocole d'entente (« **PE** ») pour échanger des renseignements et entretenir des relations avec des partenaires internationaux. Le CST a déjà conclu un certain nombre de ces protocoles d'entente. De nouveaux centres de cybersécurité voient le jour partout dans le monde. Il est dans l'intérêt du CST de communiquer avec ces centres et d'apprendre d'eux, dans la mesure du possible.

[54] M. Gupta a ajouté que le CST collaborait également à l'échelle internationale avec les équipes d'intervention en cas d'incident de sécurité informatique (comme le Réseau international de veille et d'alerte) pour échanger des renseignements sur les menaces.

9. Mot de la fin

[55] Mme Tayyeb a affirmé que le CST disposait de ressources et de pouvoirs législatifs adéquats pour remplir son mandat, ainsi que des autorisations ministérielles nécessaires. Il n'est pas urgent d'apporter de nombreux changements. L'un des plus grands défis que doit relever la collectivité en général consiste à concevoir des mécanismes pour réagir de façon coordonnée à l'ingérence étrangère dans l'ensemble du gouvernement. Mme Xavier a expliqué qu'il était important que les Canadiens comprennent que les cybermenaces comportent toujours un risque.