Résumé public d'entrevue classifiée : Shelly Bruce, Alia Tayyeb et Dan Rogers[1]

Le 8 février 2024, les avocats de la Commission ont mené une entrevue en groupe de cadres du **Centre de la sécurité des télécommunications (« CST »)**. L'entrevue s'est déroulée dans un environnement sécurisé et traitait notamment d'informations classifiées. Le présent document constitue la version publique du résumé classifié de l'entrevue déposé en preuve au cours des audiences à huis clos de la Commission qui ont eu lieu en février et mars 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.
- La rédaction du présent résumé s'appuie sur la sous-division (a)(iii)(C)(II) du mandat de la Commission. Ce résumé divulgue la preuve pertinente aux fins des divisions (a)(i)(A) et (B) du mandat de la Commission qui, selon la Commissaire, ne porteraient pas préjudice aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale.
- Le présent résumé contient de l'information qui concerne les divisions (a)(i)(A) et (B) du mandat de la Commission. L'information fournie au cours de l'entrevue se rapportant à d'autres aspects du mandat de la Commission a été omise de ce résumé, mais pourrait être présentée en preuve par la Commission à un stade ultérieur des procédures.
- Le présent résumé doit être lu conjointement avec le rapport institutionnel non classifié du CST.

[1] Traduction.

Contexte et mandat

Le CST est l'organisme qui s'occupe de la cryptographie et des renseignements électromagnétiques au Canada. Son mandat général est décrit dans la *Loi sur le CST*. Le CST analyse l'infrastructure mondiale de communication de manière à collecter des renseignements étrangers, principalement sous forme d'informations ou signaux électromagnétiques (renseignement électromagnétique ou **« SIGINT »**), qu'il utilise ensuite pour rédiger des rapports de renseignement.

Shelly Bruce a été nommée cheffe du CST en 2018. Elle a occupé le poste jusqu'en août 2022 et a pris sa retraite par la suite. En tant que cheffe, M^me^ Bruce était la dirigeante principale du CST et s'occupait de la gestion et des activités de l'organisation.

Alia Tayyeb a été nommée cheffe adjointe du Renseignement électromagnétique du CST en 2022. Elle est également responsable des cyberopérations à l'étranger, conformément au mandat du CST.

Dan Rogers a été nommé chef adjoint du Renseignement électromagnétique du CST en 2018. Il a par la suite été nommé chef adjoint du CST en janvier 2022. Il a occupé ce poste jusqu'en mai 2023.

Définition de l'ingérence étrangère selon le CST

M^me^ Bruce a expliqué qu'en vertu de la *Loi sur le CST*, la collecte par le CST de renseignements étrangers d'origine électromagnétique est dictée par les priorités du gouvernement du Canada en matière de renseignement, qui comprennent l'ingérence étrangère (**« IE »**). M^me^ Tayyeb a expliqué que, même si CST connaît bien et accepte la définition de l'IE utilisée par le **Service canadien du renseignement de sécurité (« SCRS »)**, le CST est guidé par les priorités en matière de renseignement, qui comprennent à la fois l'influence étrangère et l'ingérence étrangère. La notion d'influence

est plus large que celle d''ingérence et englobe les intentions, les activités et les capacités d'États étrangers.

M[me] Bruce a discuté du mandat du CST en ce qui concerne l'IE. Elle a relevé cinq aspects du mandat du CST :

1) Le mandat lié au renseignement étranger;
2) Le mandat lié à la cybersécurité et à l'assurance de l'information;
3) Le mandat lié aux cyberopérations étrangères;
4) Le mandat lié aux cyberopérations défensives;
5) Le mandat lié à l'assistance.

Elle a expliqué que les cinq aspects du mandat du CST sont tous pertinents dans le cadre des enquêtes en matière d'IE. À titre d'exemple, le mandat du CST lié au renseignement étranger inclut la collecte de renseignements afin de déterminer les intentions et les capacités d'entités étrangères, ainsi que les motifs qui les animent, en fonction des priorités du Canada en matière de renseignement. Le CST peut fournir ces renseignements à des partenaires en vertu de l'article 16 de la *Loi sur le CST*. Les clients qui reçoivent ces renseignements peuvent les utiliser pour prendre des mesures. Si un client détermine qu'une mesure doit être prise, il est tenu de demander la permission au CST afin de veiller à ce que les renseignements soient utilisés de manière à protéger la sécurité nationale et à ne pas compromettre les intérêts du CST.

M[me] Bruce a souligné que le CST traite également d'affaires relatives à l'IE dans le cadre de son mandat lié à la cybersécurité et à l'assurance de l'information. À titre d'exemple, le CST travaille avec des partenaires afin d'aider à protéger les composantes électroniques d'infrastructures, comme celles qui sont nécessaires pour organiser et mener des élections générales.

M[me] Bruce a expliqué que le CST, par l'entremise du Centre canadien pour la cybersécurité (le **« CCC »**) sensibilise également les partis politiques et offre des conseils et recommandations aux gestionnaires des TI [technologies de l'information] pour les campagnes électorales afin de promouvoir la sécurité de celles-ci. De plus, Le CCC a

établi une ligne téléphonique pour répondre à des questions, mené des évaluations des menaces pour le public et produit deux fois par année une évaluation des menaces en matière de cybersécurité. Le CCC a aussi communiqué avec Postes Canada, notamment, concernant la sécurité des systèmes permettant de traiter les bulletins de vote soumis par la poste pendant l'élection de 2021.

M[me] Tayyeb a ajouté que, en ce qui concerne les menaces pour les institutions démocratiques et la sécurité des élections, il était utile de concevoir que le mandat du CST lié à la cybersécurité et à l'assurance de l'information visait à protéger trois entités : les électeurs, les partis politiques et l'infrastructure électorale. Afin de protéger les électeurs, le CST, par l'entremise du CCC, communique des avis publics, fait de la sensibilisation concernant les bonnes pratiques en matière de sécurité informatique et informe le public au sujet des activités des acteurs malveillants. Afin de protéger les partis politiques, le CCC offre des conseils et des recommandations au sujet des pratiques exemplaires en matière de sécurité. Pour protéger l'infrastructure électorale, le CCC travaille avec Élections Canada et aide à protéger l'infrastructure de vote électronique contre les cyberattaques.

M[me] Bruce a discuté du mandat du CST lié aux cyberopérations étrangères. Elle a expliqué que, pendant les élections de 2019 et de 2021, une autorisation ministérielle était en vigueur afin de permettre au CST, au besoin, de prendre des mesures visant à perturber les attaques menées contre l'infrastructure électorale.

Enfin, M[me] Bruce a abordé l'aspect du mandat du CST lié à l'assistance. Elle a souligné que, sur demande, le CST peut fournir de l'assistance opérationnelle et technique à d'autres organismes. Ces organismes comprennent le SCRS, la **Gendarmerie royale du Canada** (**« GRC »**), le **ministère de la Défense nationale** et les **Forces armées canadiennes** (le **« MDN »** et les **« FAC »**), et l'Agence des services frontaliers du Canada. Lorsqu'il prête assistance à ces ministères et organismes, le CST agit conformément au mandat et aux politiques du ministère ou de l'organisme qui fait la demande, et ceux-ci sont les seuls qui détiennent les résultats de cette assistance.

Lorsque le CST agit conformément à son propre mandat, il lui est interdit de mener des activités visant des Canadiens ou des personnes au Canada. Le mandat du CST est axé sur des activités ou des informations qui sont de nature étrangère.

Aspects du mandat du CST

M. Rogers a fait remarquer que certains aspects du mandat du CST fonctionnent conjointement. À titre d'exemple, l'information recueillie dans le cadre du mandat du CST lié au renseignement étranger d'origine électromagnétique est utilisée pour éclairer l'établissement de rapports dans le cadre du mandat du CST lié à la cybersécurité et à l'assurance de l'information.

M[me] Bruce a réitéré que tous les aspects du mandat du CST s'éclairent l'un l'autre. La mission du CST liée au renseignement étranger d'origine électromagnétique alimente la mission liée à la cybersécurité et à l'assurance de l'information, et appuie également les cyberopérations étrangères du CST. De même, l'information obtenue dans le cadre de la mission liée à la cybersécurité alimente la mission liée au renseignement étranger d'origine électromagnétique. L'information est échangée de manière naturelle et dynamique par l'entremise de mécanismes de partage de l'information établis au sein du CST.

M. Rogers a utilisé l'exemple d'une **attaque par déni de service distribué** [un type de cyberopération qui empêche temporairement un site Web de fonctionner en l'inondant de niveaux de trafic importants, de telle sorte qu'il devient incapable de répondre aux demandes normales] pour expliquer la manière dont cet échange d'information fonctionne en pratique. Si une telle attaque survient, le CCC pourrait trouver des indices tendant à montrer que l'opération est menée par des acteurs étrangers. Ensuite, les personnes impliquées dans le mandat lié au renseignement étranger d'origine électromagnétique pourraient mener une enquête. Enfin, dans certaines circonstances, les personnes impliquées dans au mandat lié aux cyberopérations étrangères pourraient prendre des mesures pour perturber l'opération.

Mme Tayyeb a signalé que le CST mène des enquêtes sur des acteurs étrangers afin de déterminer leurs intentions. Si l'équipe du renseignement étranger d'origine électromagnétique du CST découvre de l'information qui indique qu'un acteur lancera une cyberattaque, elle en informe les personnes responsables des cyberopérations étrangères. À cette étape, les personnes participant aux cyberopérations étrangères pourraient prendre des mesures appropriées pour perturber l'attaque.

Mme Tayyeb a aussi souligné la différence entre les cyberopérations actives et les cyberopérations défensives, aux termes des articles 18 et 19 de la Loi sur le CST. Une cyberopération défensive a lieu lorsqu'une cyberattaque est en cours contre les systèmes du gouvernement du Canada, ou d'autres systèmes jugés importants, et que le CST doit défendre contre cette cyberattaque. Une cyberopération active a lieu lorsque le CST prend des mesures en ligne pour perturber les capacités d'acteurs malveillants étrangers et réduire leur capacité à cibler le Canada.

Coordination entre groupes

Mme Tayyeb a souligné qu'il existe de nombreuses procédures en place pour faciliter la coopération et la coordination entre les divers groupes et sections au sein du CST. Tout le monde connaît bien son rôle. Ces procédures peuvent être de nature officielle ou informelle. À titre d'exemple, les personnes qui travaillent dans le SIGINT pourraient échanger de l'information avec des collègues de la cybersécurité et des cyberopérations par l'entremise de rapports officiels, et assurer un suivi dans le cadre de réunions, d'échanges de courriels et d'appels téléphoniques. Ces équipes partagent le même espace et ont une relation de travail solide et collaborative, ce qui permet de s'assurer que l'information est échangée de façon dynamique et que tous les membres d'équipe ont de bons rapports.

M. Rogers a souligné que, dans certains cas, grâce à ces relations de travail collaboratives, il n'est pas toujours nécessaire d'avoir une procédure officielle pour assurer la coordination au sein de l'agence. Dans certaines circonstances, toutefois, des mécanismes de contrôle doivent être en place afin d'assurer la conformité aux lois et aux

politiques, y compris lorsque le renseignement peut être utilisé à titre consultatif ou dans le cadre d'opérations. Cette pratique assure une gestion appropriée de l'information.

M^me^ Tayyeb a ajouté qu'il existe un cadre solide pour les approbations opérationnelles relatives aux cyberopérations. Il existe un système de gouvernance à multiples paliers, ainsi que des plans pour encadrer toute cyberopération étrangère qui pourrait survenir. M^me^ Tayyeb a ajouté que la contribution et la collaboration d'**Affaires mondiales Canada** (**« AMC »**) sont requises pour ce type d'opérations.

Mandat d'assistance du CST

Explication du mandat d'assistance

M. Rogers a expliqué que le mandat d'assistance du CST permet à ce dernier d'agir au nom des agences chargées de l'application de la loi, des agences de sécurité nationale, ainsi qu'au nom du MDN et des FAC. Lorsque le CST prête assistance, il mène ses activités conformément aux pouvoirs conférés à l'agence auquel il prête assistance, et il exerce les pouvoirs, et leurs limites, de cette agence. À titre d'exemple, si le CST prêtait assistance au SCRS, il serait assujetti aux mêmes conditions que celles auxquelles est assujetti le SCRS.

M. Rogers a expliqué que, habituellement, une agence de sécurité nationale ou chargée de l'application de la loi ou de sécurité nationale demande l'assistance technique du CST. Lorsqu'il reçoit la demande d'assistance, le CST entreprend un processus officiel pour évaluer la demande. Ce processus comprend une évaluation juridique et un plan des opérations pour comprendre la demande. Le plan des opérations peut établir des paramètres pour la rétention des données, ou évaluer comment le CST créera les capacités techniques demandées, ou toute exigence applicable liées aux rapports.

M. Rogers a affirmé que les demandes portent souvent sur l'assistance technique pour recueillir ou analyser des renseignements. À titre d'exemple, le SCRS pourrait demander l'assistance du CST pour intercepter des communications en vertu d'un mandat.

Selon M[me] Tayyeb, il est important de souligner que, pour chaque demande, le CST s'assure lui-même que l'organisation qui présente la demande a la capacité légale de faire ce qui fait l'objet de sa demande d'assistance présentée au CST. M. Rogers a ajouté que ces demandes sont typiquement très précises et pourraient concerner des Canadiens. Si c'est le cas, le CST prend des mesures spéciales pour s'assurer que toute information recueillie dans le cadre de ces demandes est traitée selon les conditions appropriées de l'agence qui fait la demande (p. ex., les périodes de rétention) et fait l'objet d'une diffusion limitée au sein du CST. C'est en partie parce que le mandat du CST ne lui permet pas de mener des activités visant des Canadiens ou quiconque au Canada.

M. Rogers a poursuivi en soulignant que l'information recueillie au titre d'une demande d'assistance appartient à l'organisation qui fait la demande. Par exemple, l'information recueillie par le CST au titre d'une demande présentée par le SCRS appartient à ce dernier. Il revient au SCRS de décider ce qu'il fera avec l'information et qui pourra la recevoir. Si l'information recueillie est également pertinente au mandat du CST, le SCRS peut donc décider de communiquer à nouveau l'information au CST pour que celui-ci puisse en faire usage.

Mandat lié à l'assistance pendant les élections de 2019 et de 2021

M. Rogers a expliqué que le CST a prêté assistance au SCRS relativement au mandat de ce dernier lié au renseignement étranger. Ce travail a aidé à éclairer la stratégie et les intérêts du Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (**« Groupe de travail »**) pendant les élections de 2019 et de 2021. Cependant, il n'était pas au courant d'autres demandes d'assistance particulières liées à l'IE qui auraient été présentées au CST pendant l'une ou l'autre période électorale.

Échange d'information

Base de données centrale

M[me] Bruce a expliqué que les renseignements produits par le CST sont téléchargés dans une base de données centrale. Les clients peuvent ensuite consulter la base de données

et rechercher de l'information qui est pertinente à leurs priorités en matière de renseignement. Le CST décide qui peut accéder à quelle information. La base de données permet de veiller à ce que les clients du CST puissent accéder à de l'information et à du renseignement qui sont liés à leurs priorités. Le CST a de nombreux clients, et il arrive parfois que de l'information et des renseignements soient pertinents pour plus d'un client.

M[me] Tayyeb a décrit deux produits qui vont dans cette base de données : des rapports finaux et des résumés. Un rapport final est un rapport de renseignement particulier et détaillé. Les résumés sont moins détaillés, peuvent faire la synthèse de plusieurs rapports et sont adaptés à des publics particuliers.

M. Rogers a souligné que le CST met en évidence des rapports de renseignement pour des clients particuliers. Il a également fait remarquer que des échanges analytiques, des discussions et d'autres échanges ont lieu entre le CST et ses homologues au SCRS. à titre d'exemple, l'équipe du CST spécialisée en matière de renseignements relatifs à un État idoine échange souvent de l'information avec le bureau du SCRS lié à cet État. Si le CST découvre de l'information qui serait importante pour le SCRS, les employés du CST peuvent appeler ou aviser les employés pertinents du SCRS pour leur indiquer que de l'information serait disponible avant qu'elle soit publiée dans un rapport, et ils fourniront tout le contexte approprié. Sauf dans un contexte lié à une demande d'assistance, le CST ne proposera pas de mesure concernant des enquêtes au Canada, puisque celles-ci dépassent le mandat du CST.

M. Rogers a aussi mentionné que le CST expurge l'identité de Canadiens qui figurent de façon accessoire dans les rapports du CST en matière de renseignement étranger. Si la destinataire du rapport a besoin de connaître l'identité de ces Canadiens, et qu'elle a l'autorisation légitime de recevoir cette information, des processus officiels permettent de diffuser cette l'information à un nombre limité de personnes dans des cas appropriés.

M^me^ Tayyeb a expliqué que l'accès à de l'information cloisonnée est principalement contrôlé par des moyens technologiques, notamment les contrôles d'accès à la base de données. Ces contrôles sont basés sur le principe du « besoin de savoir » et des politiques de diffusion. M. Rogers a ajouté qu'en plus de ces contrôles officiels, une culture et des systèmes (p. ex., les exigences en vigueur du gouvernement en matière de renseignement) au sein du CST et de la communauté du renseignement veillent à ce que les employés du CST qui sont affectés à un domaine particulier soient conscients (i) du lieu où se trouve le renseignement auquel ils doivent avoir accès et les diverses équipes avec lesquelles ils devraient régulièrement interagir afin d'en discuter, et (ii) des renseignements qui doivent être échangés avec des partenaires externes. Tous les témoins ont souligné que ces pratiques font partie intégrante de la culture du CST depuis longtemps.

À l'extérieur du CST, M. Rogers a expliqué que des **agents de relations avec la clientèle** (« **ARC** ») [des employés du CST qui travaillent au sein d'autres ministères ou organismes comme le SCRS, le MDN ou le Bureau du Conseil privé] coopèrent avec de hauts fonctionnaires pour veiller à ce que ces derniers aient accès aux renseignements pertinents dans la base de données. Les ARC sont aussi généralement responsables de fournir de l'information aux hauts fonctionnaires et aux bureaux ministériels.

M. Rogers a expliqué que, puisque la plupart des ministres ne travaillent pas dans un local isolé pour l'information sensible cloisonnée, un ARC apporte généralement un classeur en format papier afin qu'ils puissent lire son contenu. L'ARC ramène normalement le classeur avec lui une fois que le ministre a terminé sa lecture et consigne le fait que le rapport a été fourni. M^me^ Tayyeb a précisé qu'il s'agissait de la méthode la plus fiable dont le CST disposait pour assurer le suivi de la consultation par un ministre d'un produit de renseignement du CST. Elle a ajouté que la base de données comporte aussi un système de suivi qui permet au CST d'identifier les personnes qui ont directement ouvert un rapport donné, ou si des personnes ont pu avoir accès à une copie grâce à un ARC. M Rogers a poursuivi en mentionnant que, pour évaluer l'utilité de ses

produits de renseignement, le CST surveille ce système de suivi pour obtenir de la rétroaction (qui peut être fournie électroniquement ou par l'entremise d'ARC) et mène des enquêtes d'opinion auprès de ses clients en matière de renseignement.

M[me] Tayyeb a aussi ajouté qu'en plus des ARC, le CST forme des agents de diffusion du SIGINT, qui sont des employés du ministère ou de l'organisme pertinent, mais qui exercent les mêmes fonctions que les ARC.

Activité du CST pendant les périodes électorales de 2019 et de 2021

M[me] Bruce a mentionné que le CST a détecté diverses tentatives de balayer, de sonder ou d'exploiter l'infrastructure électorale canadienne pendant les élections de 2019. Toutefois, aucune de ces tentatives n'a compromis cette infrastructure.

M. Rogers a souligné que le CST a surveillé les cyberattaques et les intrusions pendant les élections, et que cela était pertinent, étant donné que les cyberattaques pourraient être utilisées comme une composante d'activités d'IE. M[me] Bruce a ajouté que le CST s'est concentré sur la cybersécurité pendant les élections depuis 2017, lorsque la lettre de mandat de la ministre Gould, qui était à l'époque ministre des Institutions démocratiques, a été délivrée et a donné au CST la directive de se concentrer sur ce domaine. M[me] Bruce a expliqué que la lettre faisait suite à des incidents documentés d'IE en ligne liés aux élections qui ont eu lieu en 2016 aux États-Unis d'Amérique.

M[me] Bruce a expliqué que, en raison du système de vote sur papier du Canada, les systèmes que le CST aide à surveiller sont principalement de nature administrative (p. ex., les réseaux d'Élections Canada, le registre des électeurs, la diffusion des débats), et le CST aide aussi à protéger les communications des mandataires élus. Elle a aussi souligné le besoin de protéger l'infrastructure en ligne pour s'assurer que le public ait confiance en leurs systèmes électoraux, et s'est rappelé que le CST a communiqué avec Postes Canada concernant les pratiques exemplaires en matière de cybersécurité pour les systèmes permettant de traiter les bulletins de vote soumis par la poste.