Résumé d'entrevue : David Vigneault (Service canadien du renseignement de sécurité), Alia Tayyeb (Centre de la sécurité des télécommunications), Daniel Rogers (Bureau du Conseil privé)[1]

Contexte

De hauts fonctionnaires du Service canadien du renseignement de sécurité, du Centre de la sécurité des télécommunications et du Bureau du Conseil privé ont été interviewés en groupe par les avocats de la Commission le 16 janvier 2024.

L'entrevue s'est déroulée dans un environnement sécurisé et a fait référence à de l'information classifiée. Le présent résumé a été rédigé de manière à supprimer ou à synthétiser l'information classifiée, le but étant de pouvoir le divulguer publiquement.

Ce préambule et les passages entre crochets sont des notes explicatives fournies par les avocats de la Commission pour éclairer le lecteur.

* * *

Le **Service canadien du renseignement de sécurité** (« SCRS ») est un service civil de renseignement de sécurité. La mission principale du SCRS est d'enquêter sur les activités qui pourraient être raisonnablement perçues comme une menace pour la sécurité du Canada, ainsi que de fournir des rapports et des conseils au gouvernement du Canada concernant ces menaces. La *Loi sur le Service canadien du renseignement*

[1] Traduction.

de sécurité (« *Loi sur le SCRS* ») définit précisément les activités sur lesquelles le Service peut enquêter ainsi que le seuil à atteindre pour que le SCRS puisse entreprendre des activités d'enquête et prendre des mesures afin de réduire les menaces à la sécurité du Canada.

David Vigneault a été nommé directeur du SCRS en juin 2017 et son mandat a été renouvelé en juin 2022. Le directeur supervise la gestion globale du Service et assume certaines responsabilités officielles en vertu de la *Loi sur le SCRS*, notamment celle d'obtenir l'approbation du ministre avant de déposer une demande d'autorisation judiciaire concernant des activités d'enquête et des mesures de réduction de la menace. Le directeur rend compte au ministre de la Sécurité publique et est assisté de trois sous-directeurs représentant les opérations, les politiques et l'administration. M. Vigneault a précédemment occupé le poste de secrétaire adjoint du Cabinet, Sécurité et renseignement, au Bureau du Conseil privé de 2013 à 2017.

Le **Centre de la sécurité des télécommunications** (« CST ») est l'agence cryptologique nationale du Canada. Il est chargé de recueillir, pour le gouvernement du Canada, du renseignement électromagnétique étranger, et il héberge également le Centre canadien pour la cybersécurité. Sa mission principale est définie par les dispositions de la *Loi sur le Centre de la sécurité des télécommunications* (« *Loi sur le CST* »). Le CST recueille du renseignement étranger à partir de l'infrastructure mondiale de l'information, principalement par l'entremise des communications et d'autres signaux électroniques, collectivement appelés « renseignement électromagnétique » (« SIGINT »). Le CST utilise le SIGINT pour produire des rapports sur le renseignement étranger.

Alia Tayyeb a été nommée chef adjointe, SIGINT, au CST en 2022. À ce titre, elle est également responsable de l'aspect « cyberopérations à l'étranger » du mandat du CST. Avant cette nomination, elle a occupé d'autres postes au sein du CST, du BCP et du SCRS.

Le **Bureau du Conseil privé** (« BCP ») est le bureau central du gouvernement qui soutient l'élaboration et la mise en œuvre du programme politique et législatif du gouvernement. Il coordonne également les réponses de tous les ministères et organismes du gouvernement canadien. En matière de sécurité nationale, la Direction du conseiller à la sécurité nationale et au renseignement auprès du premier ministre (« CSNR »), qui comprend le Secrétariat de la politique étrangère et de la défense, le Secrétariat de la sécurité et du renseignement et le Secrétariat de l'évaluation du renseignement, fait notamment partie intégrante du BCP.

Dan Rogers a été nommé conseiller adjoint à la sécurité nationale et au renseignement auprès du premier ministre en mai 2023. À ce titre, il participe à la coordination en matière de sécurité nationale au sein du gouvernement. La CSNR et lui agissent en tant que conseillers auprès du premier ministre et de son cabinet sur les questions de sécurité nationale, ainsi qu'en tant qu'agent de liaison auprès d'autres gouvernements étrangers et de la communauté du renseignement. M. Rogers a précédemment occupé les fonctions de chef adjoint du CST; de sous-chef, Renseignement électromagnétique étranger au CST; de directeur des opérations pour le Secrétariat de la sécurité et du renseignement au BCP et de Directeur, Exigences de programmes de SIGINT au CST.

Autorisation légale pour divulguer de l'information classifiée

SCRS et CSE

M. Vigneault a expliqué que le SCRS est limité par la loi dans sa capacité à divulguer des informations classifiées. Par exemple, les articles 18 et 19 de la *Loi sur le SCRS* interdisent la communication d'information classifiée, sauf dans certaines circonstances bien définies. L'article 19 limite la communication de toute information classifiée à l'extérieur du gouvernement du Canada, sauf dans les cas où communiquer une telle information est nécessaire dans le cadre de mesures de réduction de la menace prises par le SCRS ou est exigé par la loi. Les articles 18 et 18.1 interdisent la communication de toute information pouvant menée à l'identification, respectivement, d'un employé du SCRS ou d'une source humaine. Au sein du gouvernement du Canada, la divulgation de toute information classifiée peut généralement avoir lieu lorsque le destinataire possède l'habilitation de sécurité appropriée et a besoin de connaître les informations contenues dans les documents classifiés.

M^{me} Tayyeb a fait remarquer qu'il n'existe aucune disposition précise dans la *Loi sur le CST* qui confère l'autorisation légale de divulguer de l'information classifiée. Elle a également expliqué que la structure de la *Loi sur le CST* permet de mener des activités afin de maintenir le secret des opérations. De plus, l'article 55 de la *Loi sur le CST* interdit la divulgation de toute information pouvant révéler l'identité de personnes ou d'entités qui, à titre confidentiel, viennent en aide au CST dans l'accomplissement de sa mission. Le CST s'appuie sur l'aide volontaire de ses partenaires pour remplir sa mission, qui est secrète par nature.

M. Vigneault et M^me^ Tayyeb ont tous deux noté que la *Loi sur la protection de l'information* (« LPI ») fait en sorte que la plupart des employés du SCRS et du CST sont tenus au secret à perpétuité. Ils ont tous deux souligné que la nécessité de protéger l'information classifiée est implicite dans la structure de la LPI.

M. Rogers a expliqué que la Politique sur la sécurité du gouvernement du Conseil du Trésor détermine la manière dont l'information doit être classifiée et traitée, ce qui régit à son tour la manière dont un organisme doit traiter l'information classifiée.

Échange de renseignement avec des partenaires nationaux et étrangers

SCRS

M. Vigneault a expliqué que le SCRS échange des données de renseignement avec des partenaires nationaux et étrangers. Au sein du pays, il communique du renseignement à ses partenaires du gouvernement fédéral. Cette communication est régie par des politiques internes. M. Vigneault a souligné que l'article 19 de la *Loi sur le SCRS* interdit la divulgation de l'information que le SCRS recueille, comme cela est expliqué ci-dessus. Le SCRS échange également du renseignement avec des partenaires étrangers conformément à l'article 17 de la *Loi sur le SCRS*. Le SCRS entretient plus de 300 relations avec des entités étrangères en vertu de cette autorisation.

CST

M^me^ Tayyeb a fait remarquer que l'échange d'information et de renseignement avec les partenaires nationaux est essentiel pour que le CST puisse accomplir son mandat. La *Loi sur le CST* permet à l'organisation de distribuer ses produits pour qu'ils soient consommés par d'autres organismes du gouvernement fédéral. La *Loi sur le CST* donne

également au CST le pouvoir de conclure des accords avec des partenaires étrangers. En pratique, le CST échange de l'information principalement avec ses partenaires de l'alliance du Groupe des cinq. [Le Groupe des cinq est un partenariat qui remonte à la Seconde Guerre mondiale. Il a été créé pour faciliter l'échange de renseignement entre le Canada, les États-Unis, le Royaume-Uni, la Nouvelle-Zélande et l'Australie].

Pour sa part, le Centre canadien pour la cybersécurité (« Centre pour la cybersécurité ») [qui relève du CST] a la possibilité de conclure des accords avec différents partenaires étrangers et nationaux. Cela dit, étant donné la nature de son mandat, qui comprend la publication d'avis publics sur des questions de cybersécurité susceptibles de toucher le public, le Centre pour la cybersécurité fournit de nombreux produits non classifiés au public canadien et au secteur privé.

Produits du renseignement

CST

M[me] Tayyeb a expliqué que le principal produit du CST est un type de rapport qui présente le renseignement sous une forme narrative à l'intention des responsables gouvernementaux ou d'autres partenaires. Ces rapports sont des résumés qui ne contiennent pas nécessairement une analyse ou une évaluation détaillée. Le CST produit également des rapports analytiques. Les rapports du CST peuvent être distribués directement parmi les organismes gouvernementaux, le SCRS étant le principal consommateur de ces rapports, et ils peuvent être diffusés au sein de l'alliance du Groupe des cinq, s'il y a lieu. Les rapports du CST peuvent être « expurgés » pour limiter la divulgation de données confidentielles, en fonction du destinataire. [Expurger consiste à supprimer l'information confidentielle d'un document afin d'en permettre une plus large

diffusion.] Enfin, le CST rédige un rapport annuel qui donne au public un aperçu de ses activités et de son fonctionnement.

BCP

M. Rogers a expliqué que le BCP fournit des produits de renseignement évalués à partir de toutes les sources par l'intermédiaire du Secrétariat de l'évaluation du renseignement (SER). En d'autres termes, le BCP analyse tant de l'information classifiée que de l'information provenant de sources ouvertes en élaborant ses produits de renseignement. Le volume de rapports créés par le BCP est moins élevé que celui des produits créés par le SCRS ou le CST, parce que le BCP ne collecte pas ses propres données de renseignement et que ses rapports sont généralement créés dans un but précis. Par exemple, le BCP peut créer un document pour conseiller le premier ministre avant un événement à l'étranger. Par ailleurs, le SER crée des produits quotidiens destinés à une large diffusion au sein du BCP et des notes d'information hebdomadaires à l'intention du premier ministre et d'autres ministres concernés par la sécurité nationale.

M. Rogers a également souligné, à titre d'exemple, que le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections élabore des produits de renseignement. Toutefois, ce groupe de travail est composé de plusieurs organismes parce que ses rapports reposent sur la collaboration de représentants d'Affaires mondiales Canada (« AMC »), du BCP, du SCRS et du CST.

SCRS

Étant donné que son mandat est de recueillir du renseignement et de communiquer de l'information au gouvernement, le SCRS crée du renseignement brut. Dans ce contexte, l'expression « renseignement brut » s'entend de l'information recueillie par le SCRS qui

n'a pas été évaluée de manière globale, c'est-à-dire en relation avec d'autres données pertinentes. Le SCRS peut distribuer ce renseignement brut à des partenaires s'il est utile à leur mandat ou à leurs besoins en matière de renseignement.

M. Vigneault a expliqué que, comme le mandat du SCRS est de signaler les menaces au gouvernement et de le conseiller, la plupart de ses produits sont des produits de renseignement classifiés qui vont de la distribution des rapports susmentionnés accompagnés d'une information contextuelle à des produits d'évaluation approfondie du renseignement. Ces produits sont rédigés à l'intention de personnes précises qui ont l'habilitation de sécurité appropriée et qui ont besoin de connaître l'information qu'ils contiennent. Souvent, il est fait mention d'une liste restreinte de personnes à qui ils peuvent être distribués. Les produits du SCRS fournissent généralement des explications sur la source de l'information, en indiquant notamment si l'information est corroborée ou non.

En raison de leur contenu, ces produits ne peuvent être divulgués publiquement sans être considérablement caviardés. S'il est nécessaire de divulguer un tel produit, toute l'information classifiée doit être caviardée. Dans certains cas, l'information non classifiée peut elle aussi être caviardée si elle est susceptible de révéler quelque chose à propos de l'information classifiée qui s'y trouve. En général, l'information est caviardée parce qu'elle est susceptible de dévoiler une information à propos d'une source du SCRS ou d'une enquête en cours, ou d'autres données sensibles que le SCRS ne peut divulguer sans compromettre ses opérations et la sécurité nationale du Canada. La spécificité de l'information contenue dans les produits du SCRS entraîne généralement la nécessité de

caviarder ou de protéger une plus grande quantité de renseignements avant toute publication.

Le SCRS crée également des documents appelés « brochures » [*placemats*]. Ce sont généralement des documents d'une page qui résument l'information sous forme de courts récits présentés graphiquement afin d'aider le destinataire à comprendre les données de renseignement qui y sont décrites. Ces documents sont habituellement rédigés à l'intention de personnes disposant d'une habilitation de sécurité précise et sont classifiés en fonction de la nature confidentielle de l'information du renseignement qu'ils contiennent.

Le SCRS crée également des produits d'évaluation du renseignement. Les évaluations de renseignement colligent de l'information provenant d'autres produits de renseignement et l'utilisent pour décrire une situation ou pour formuler une réponse à une question de renseignement. Cela se produit généralement lorsqu'une personne ou un organisme particulier a manifesté son intérêt pour comprendre une situation et a demandé au SCRS de répondre. Encore une fois, si de tels documents devaient être divulgués, il faudrait les caviarder afin d'empêcher la divulgation de toute information sensible.

Enfin, dans le cadre des breffages ministériels, le SCRS peut produire des notes d'information en s'appuyant sur une combinaison de rapports et de produits, selon les besoins.

Attribution du niveau de classification

CST

M^me^ Tayyeb a expliqué que le CST a mis en place diverses normes qui dictent le niveau de classification à appliquer à ses différents produits de renseignement. Ces normes bien établies ont été élaborées en collaboration avec les partenaires de l'alliance du Groupe des cinq du CST. En général, l'auteur du produit de renseignement détermine le niveau de classification en fonction des normes applicables.

M^me^ Tayyeb a fait remarquer que, lorsque le CST reçoit de l'information de partenaires étrangers, ceux-ci indiquent le niveau de classification du produit de renseignement communiqué. Il est impératif de respecter les niveaux de classification établis par les partenaires étrangers afin de maintenir les relations avec ces derniers et de favoriser l'échange d'information.

En ce qui concerne le SIGINT, la plupart des produits du CST sont classés Très secret/Renseignement spécial. M^me^ Tayyeb a expliqué qu'un document contenant de l'information particulièrement sensible peut être classé dans une catégorie qui donne lieu à un accès encore plus restreint que la classification « Très secret ».

De manière générale, un niveau de classification limite la diffusion de données sensibles. Il vise à réduire les risques et à assurer la reddition de compte de l'organisme qui reçoit le produit auquel la classification est appliquée. Le CST peut expurger un document ou diminuer son niveau de classification, mais cela supprimera nécessairement des détails et de l'information de son contenu.

SCRS

M. Vigneault a expliqué que le SCRS détermine également des niveaux de classification en utilisant des normes bien établies qui sont fixées par des politiques. Le plus souvent, le niveau de classification attribué à un produit de renseignement est lié à la gravité du préjudice qui résulterait de sa divulgation. Ce préjudice pourrait être causé à une personne, c'est-à-dire à une source humaine, ou à d'autres aspects d'une enquête en cours. Dans chaque situation, le niveau de classification est déterminé par des professionnels au sein du SCRS, tels que des experts en la matière qui comprennent le contexte propre à l'information et le niveau de protection requis.

Par ailleurs, M. Vigneault a souligné la nécessité d'appliquer une protection rigoureuse à l'information qui révèle des sources humaines. Il est absolument nécessaire que le SCRS protège cette information, afin de protéger la sécurité des sources, d'assurer un accès continu à celles-ci et de préserver la capacité du SCRS à recruter d'autres sources.

BCP

M. Rogers a expliqué que, comme le BCP ne recueille pas lui-même du renseignement, il n'attribue pas ses propres niveaux de classification aux produits de renseignement. Il tient plutôt compte des niveaux de classification attribués par l'agence d'origine (p. ex. le CST, le SCRS) à ces produits. M. Rogers a également fait remarquer que le Canada hérite de la classification de l'information fournie par ses partenaires étrangers.

Divulgation d'information ou de renseignement

Demandes de divulgation et risques pour la sécurité nationale

M[me] Tayyeb a expliqué que le CST dispose d'une équipe qui traite les demandes de divulgation d'information. L'équipe s'occupe de la déclassification, des demandes en justice, des demandes d'accès à l'information, des politiques et de la conformité. Lorsqu'elle répond aux demandes de divulgation, l'équipe doit tenir compte de la nécessité de préserver l'accès du CST à l'information. Le CST ne peut pas divulguer de l'information qui révélerait son intérêt pour une cible, ni le fait qu'il a accès à de l'information sur une cible, ni la manière dont il y a accédé. La divulgation de cette information permettrait à une cible d'utiliser des contre-mesures ou de compromettre d'une autre manière la capacité du CST à recueillir de l'information et du renseignement. La divulgation n'est généralement possible que lorsque la source du renseignement ne peut être déduite à partir de l'information divulguée.

M[me] Tayyeb a également souligné la nécessité de protéger l'information des partenaires étrangers du CST. Le CST ne peut pas divulguer de l'information susceptible de révéler les méthodes, les techniques ou les objectifs de partenaires étrangers. [Le CST ne peut pas divulguer de l'information provenant d'un partenaire étranger sans le consentement de ce dernier.] À défaut, le CST risque de compromettre ses relations avec ce partenaire. Enfin, M[me] Tayyeb a également souligné la nécessité de protéger la sécurité des Canadiens. Certaines informations, si elles étaient divulguées, pourraient également révéler l'identité d'employés du CST ou d'autres personnes. M. Vigneault a exprimé son accord avec les commentaires de M[me] Tayyeb.

M. Vigneault a souligné qu'à l'ère des données de masse, il est possible pour les adversaires de rassembler des éléments d'information parcellaires sans liens apparents, de les rassembler et d'apprendre des choses sur les sources ou les techniques du SCRS qui resteraient autrement cachées.

Les trois témoins ont expliqué que, plus une information est précise, plus il est facile pour un adversaire de l'utiliser pour identifier une source ou une technique. Ainsi, le risque pour la sécurité nationale est généralement plus élevé lorsque l'information concerne du renseignement précis que lorsqu'elle est de nature plus générale.

Demandes impliquant une forte intensité de ressources

Les trois témoins ont expliqué que les demandes de divulgation requièrent beaucoup de ressources et de main-d'œuvre. Lorsqu'une demande de divulgation est formulée, des experts en procédures juridiques doivent la traiter et analyser les paramètres juridiques qui l'entourent. Les experts en la matière doivent examiner chaque élément d'information pour s'assurer que sa divulgation ne causera pas de préjudice, directement ou en conjonction avec d'autres informations qui sont ou pourraient éventuellement être connues du public. Ces experts sont des personnes qui disposent des connaissances nécessaires pour déterminer si la divulgation d'une information est préjudiciable compte tenu du contexte.

M. Vigneault a déclaré qu'il était important que nos institutions restent le plus transparentes possible afin de maintenir le contact avec le public et la confiance de ce dernier. Le SCRS dispose d'unités spécialisées qui répondent aux exigences de divulgation découlant d'enquêtes policières, des procédures devant la Cour fédérale, des

demandes des organismes d'examen (OSSNR et CPSNR) et des demandes d'AIPRP. Ces unités consultent également des experts en la matière afin d'évaluer le préjudice potentiel que causerait une divulgation à la sécurité nationale. Par conséquent, les demandes de divulgation nécessitent un travail et des ressources considérables. À titre d'exemple, il a fallu 200 heures-personnes pour caviarder les treize (13) échantillons de documents demandés par la Commission. Un grand nombre de ces demandes peut mobiliser des ressources précieuses et affecter la capacité d'un organisme à s'acquitter de son mandat. Or, il n'est pas dans l'intérêt public de compromettre la capacité d'un organisme à faire son travail et à protéger les Canadiens.

Il n'existe pas d'accords préexistants avec des partenaires étrangers qui permettraient à une agence canadienne de divulguer du renseignement étranger sans le consentement de son auteur. Les demandes de divulgation de renseignement d'origine étrangère sont faites au cas par cas. M. Vigneault a mis en garde contre le fait que, si un service de renseignement canadien demande trop souvent la divulgation d'informations qui lui ont été communiquées par des partenaires étrangers, ces derniers risquent de réévaluer les accords d'échange d'information. Il a également souligné que lorsque les demandes de divulgation concernent du renseignement obtenu auprès de partenaires étrangers, les organismes canadiens ne contrôlent pas l'échéancier de caviardage et de divulgation.

« Rédaction pour publication »

Les trois témoins ont expliqué que, dans certaines circonstances, l'information ou le renseignement recueilli par les agences peut être « rédigé pour être publié ». Cela signifie que l'agence (par ex., CST, SCRS) rédigera un compte rendu du renseignement sous-jacent destiné à être rendu public. Cette méthode est souvent plus efficace que le

caviardage individuel des documents. À titre d'exemple, les participants au Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections ont utilisé l'approche de la « rédaction pour publication » pour les rapports qu'ils ont publiés lors d'une élection partielle. Comme ils savaient qu'un rapport public devrait être diffusé, ils ont présenté le renseignement de manière à ce qu'il puisse être divulgué publiquement.

De manière générale, M^{me} Tayyeb a expliqué que le CST peut parfois « rédiger pour publier » au lieu de caviarder un document qui a été rédigé selon le niveau de classification le plus élevé. Cela s'explique par le fait que très peu de personnes sont habilitées à prendre connaissance des rapports au niveau de classification le plus élevé. La rédaction pour publication permet de diffuser l'information à ceux qui ont besoin de la connaître sans compromettre des techniques de collecte confidentielles ou d'autres informations qu'un destinataire n'a pas besoin de connaître. Le CST rédige aussi pour publier lorsque les informations en question doivent être partagées de manière urgente et lorsque les informations concernent des menaces pour la sécurité publique.

M. Vigneault a expliqué que le SCRS recourt à des « lettres d'utilisation » qui sont rédigées à l'intention des autorités policières pour leur permettre d'entamer des enquêtes en matière criminelle qui ont été portées à l'attention du SCRS. Il a noté qu'il n'existe pas de politique gouvernementale pour convertir l'information classifiée en information pouvant être divulguée publiquement. Le SCRS détermine plutôt s'il y a lieu de rédiger pour publier en fonction des destinataires et de la nature de l'information à divulguer.

Le processus de déclassification

Contestation d'un caviardage

M^me^ Tayyeb a indiqué que les décisions relatives à la modification ou à la révision d'un caviardage sont prises par les fonctionnaires sur recommandation d'experts en la matière. Le rang du décideur dépend des circonstances, mais dans le contexte de la présente Enquête, il est élevé aux sous-ministres adjoints ou aux sous-ministres (ou un rang équivalent), selon les circonstances. Règle générale, toute procédure liée à la modification ou à la révision d'un caviardage exige de concilier l'intérêt public pour la divulgation et le risque de préjudice qui peut en résulter. M^me^ Tayyeb a déclaré que la divulgation d'information confidentielle sur les sources et les méthodes peut avoir une incidence sur la capacité d'un service de renseignement à obtenir de l'information sur les menaces éventuelles. Elle a de plus souligné que l'intérêt public s'oppose fortement à la divulgation dans ce type de situation, car la perte d'information sur les menaces éventuelles nuit à la capacité du CST de protéger les Canadiens.

M. Vigneault a expliqué qu'il était très peu probable que l'on renonce au caviardage visant de l'information susceptible d'identifier une source humaine, même si la question lui était soumise pour décision. Il est important que le SCRS soit en mesure de protéger ses sources et d'éviter l'effet dissuasif qui résulterait de l'incapacité du SCRS de les protéger efficacement. Cela compromettrait la capacité du SCRS à s'acquitter de son mandat. M. Vigneault a soulevé la possibilité que l'on croie peut-être, à tort, que la transparence maximale est toujours dans l'intérêt public. Il a noté qu'il n'y a pas de dichotomie entre la restriction de la divulgation et l'intérêt public, car le mandat du SCRS est de protéger la sécurité nationale du Canada. Il est donc parfois dans l'intérêt public de restreindre la

divulgation dans la mesure où cela est nécessaire pour permettre au SCRS de s'acquitter de son mandat.

M. Rogers a expliqué que les fonctionnaires à qui l'on confie des informations classifiées ont le devoir de les protéger. Ils cherchent ainsi à agir dans l'intérêt public. Bien que la transparence serve l'intérêt public, il est également dans l'intérêt public de protéger cette information, car une diffusion sans limites pourrait avoir des répercussions importantes sur la capacité du gouvernement à protéger les Canadiens à l'avenir.

Impacts des divulgations non autorisées

La confiance du public dans les institutions est entachée

M. Vigneault a expliqué que la divulgation non autorisée d'information peut nuire à la confiance du public envers la communauté du renseignement et les institutions démocratiques. Cela peut également avoir une incidence sur les relations des services de renseignement canadiens avec leurs partenaires internationaux et amener ces derniers à limiter les informations qu'ils partagent avec eux. Les divulgations non autorisées entravent également les capacités de collecte du renseignement et compromettent les enquêtes en cours. En outre, les divulgations non autorisées ont une incidence sur la confiance des Canadiens envers la capacité des institutions fédérales à protéger leurs informations.

M. Vigneault et M^{me} Tayyeb ont expliqué que ce sont les divulgations non autorisées d'informations qui empêchent la communauté du renseignement d'échanger avec le public sur le fonctionnement des institutions de renseignement, ce qui peut donner au

public une image partielle de leurs activités. Cela peut mener le public à tirer des conclusions erronées ou trompeuses sur une institution et ses activités.

Manque de contexte crucial pour comprendre l'information

M. Rogers a expliqué que l'information ou le renseignement qui fait l'objet d'une divulgation non autorisée a généralement été élaboré pour un public particulier disposant d'un bagage d'information et d'une expertise particulière. Ce public dispose du contexte et de l'expérience nécessaires pour comprendre et évaluer la fiabilité et l'exhaustivité de l'information ou du renseignement fourni. Il peut également consulter l'agence d'origine pour clarifier les ambiguïtés ou les malentendus. Or, dans la plupart des cas, le public ne dispose pas de ce contexte crucial ni de la capacité à clarifier les ambiguïtés ou les malentendus. Considérée hors contexte, l'information qui fait l'objet d'une divulgation non autorisée peut être mal comprise ou mal interprétée par le public, ce qui peut entraîner d'autres conséquences négatives.

M[me] Tayyeb a reconnu que l'absence de contexte quant à l'information ou le renseignement faisant l'objet d'une diffusion non autorisée peut donner une impression erronée à une personne qui ne connaît pas l'ensemble des circonstances.

M. Vigneault a expliqué que le public n'est souvent pas en mesure d'évaluer de manière informée le contenu d'un rapport classifié et risque d'accorder trop d'importance à son contenu. Il a souligné que les renseignements ne constituent pas des preuves en soi et que seul un professionnel du renseignement formé peut interpréter un produit de renseignement du SCRS. En outre, M. Vigneault a expliqué qu'une divulgation non autorisée ne donne pas la possibilité à l'agence de commenter le contenu de cette

divulgation dans un forum public. Ainsi, la capacité du SCRS à clarifier les malentendus dans le contexte des divulgations non autorisées est limitée.

Le contexte de l'ingérence étrangère

M. Vigneault a distingué l'ingérence étrangère de l'espionnage en se référant à l'élément humain. L'ingérence étrangère implique souvent que des acteurs étrangers exercent des pressions sur des êtres humains ou les menacent. L'ingérence étrangère est un concept qui va au-delà des élections et des institutions démocratiques. Elle est susceptible de porter préjudice à des individus et a effectivement porté préjudice à des individus.

Collecte d'information

M. Vigneault a expliqué que la collecte de renseignement dans le contexte de l'ingérence étrangère emploie un vaste spectre de moyens. Le SCRS recueille de l'information lors de ses contacts avec le public, mais aussi en provenance de sources très sensibles. Certaines informations sont non classifiées, alors que d'autres sont hautement classifiées.

Parties sophistiquées

M^{me} Tayyeb et M. Rogers ont fait remarquer que la collecte de renseignement dans le contexte de l'ingérence étrangère se distingue également des autres collectes en raison de la sophistication des parties impliquées. L'ingérence étrangère implique des acteurs étatiques. Ces acteurs disposent de ressources importantes et de vastes capacités. Ils peuvent être en mesure de détecter des techniques d'enquête plus facilement grâce à la divulgation d'information que n'y parviendraient des acteurs moins sophistiqués.

M. Vigneault a souligné que certains acteurs étrangers n'opèrent pas selon les mêmes contraintes démocratiques que les institutions canadiennes et disposent de ressources beaucoup plus importantes. Cela signifie que ces acteurs ont des capacités différentes.

Structures et fonctions du BCP dans le contexte de l'interférence étrangère

Structures internes

M. Rogers a décrit les structures internes du BCP relatives à l'ingérence étrangère. Il a expliqué que le CSNR rassemble et coordonne la communauté canadienne du renseignement, en plus de conseiller le premier ministre et le Cabinet sur les questions de sécurité nationale.

La CSNR soutient le premier ministre et les ministres, y compris le ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales, notamment en réunissant la communauté de la sécurité et du renseignement sur les questions de sécurité nationale. Le Secrétariat des institutions démocratiques s'emploie quant à lui à renforcer le système électoral canadien, notamment au moyen d'initiatives comme le Protocole public en cas d'incident électoral majeur et le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections.

Produits pertinents

M. Rogers a expliqué que le BCP ne produit pas un seul type de renseignement en matière d'ingérence étrangère. Comme indiqué ci-dessus, le BCP produit des analyses fondées sur plusieurs sources et peut préparer des breffages écrits ou oraux pour le premier ministre ou le Cabinet, ou des mémoires destinés au Cabinet. Si le BCP reçoit

un résumé ou une analyse du SCRS, il peut le fournir au premier ministre ou au Cabinet. M. Rogers a souligné que le BCP est généralement un consommateur, plutôt qu'un producteur, de renseignements.

Fourniture d'information par le BCP

M. Rogers indique que le BCP est soumis au même système de traitement de l'information que celui imposé aux autres agences composant la communauté du renseignement. Il ne fournit pas de matériel classifié aux personnes qui n'ont pas d'habilitation de sécurité et/ou d'endoctrinement appropriés. [Les endoctrinements sont des breffages de sécurité nécessaires pour accéder à certains types d'information. Les personnes endoctrinées relativement à un type ou un sujet particulier d'information classifiée s'engagent à protéger ladite information conformément à la loi et à la politique applicables.]

Lorsqu'une personne ne dispose pas de l'habilitation et/ou de l'endoctrinement approprié, mais que le BCP doit tout de même lui communiquer certains documents classifiés, le BCP entame une procédure pour que cette personne obtienne l'habilitation et/ou l'endoctrinement approprié. À défaut, le BCP consulte l'organisme à l'origine des documents classifiés pour déterminer si l'information peut être ramenée à un niveau de classification inférieur en supprimant les parties préjudiciables ou si elle peut être communiquée d'une manière différente qui respecte les niveaux de classification.

Dans le cas hypothétique où le premier ministre souhaiterait partager le contenu de documents classifiés à un public plus large, le BCP pourrait travailler avec les agences à l'origine de ces documents pour adapter l'information de manière à ce qu'elle reste exacte sans être préjudiciable.

Politiques en matière de divulgation autorisée

M. Rogers a expliqué que le CSNR, en tant que coordonnateur au sein de la communauté du renseignement, peut conseiller le premier ministre sur les questions de politique relatives à la divulgation autorisée d'information classifiée, mais qu'il n'a aucun pouvoir de décision en ce qui a trait aux politiques de divulgation d'information classifiée. Le pouvoir d'élaborer des politiques dans ce domaine appartient aux agences elles-mêmes et au Conseil du Trésor.