Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Rapport institutionnel sur la protection de l'information dans l'intérêt national ou public

À: **Me SHANTONA CHAUDHURY**
Procureure en chef

Tél: 343-630-3755
Courriel: Shantona.Chaudhury@pifi-epic.gc.ca

De: **Procureur Général du Canada**
Ministère de la justice du Canada
Section du contentieux des affaires civiles
50 rue O'Connor, Suite 500
Ottawa, Ontario, K1A 0H8
Fax: (613) 954-1920

Gregory Tzemenakis
Avocat général principal

Barney Brucker
Avocat général principal p.i.

Tél: 613-297-2670 / 416-520-4301
Courriel: JusticeCanada.Inquiry-Enquete@justice.gc.ca

Procureurs du gouvernement du Canada

Table des matières

1) Structure de la sécurité nationale au Canada

(1) Un bref aperçu de la structure de la sécurité nationale au Canada, qui devrait décrire les organismes ou entités concernés et leurs rôles (par exemple, le mandat général de chaque organisme ou entité, s'il s'agit d'un collecteur de renseignements, d'un consommateur de renseignements ou d'un organisme de surveillance ou d'examen, et sa structure organisationnelle, dans la mesure où cela est pertinent pour les questions soulevées à l'alinéa (a)(i)(D) du mandat;

La communauté de la sécurité nationale et du renseignement du Canada est composée de plusieurs ministères et organismes, relève de ministres et fait l'objet d'un examen par plusieurs organismes et comités parlementaires. Chacun des ministères et organismes a un mandat précis et est régi par ses propres attributions, politiques et procédures.

Les principaux ministères et organismes de la communauté de la sécurité et du renseignement qui participent à la détection, à la dissuasion et à la lutte contre l'ingérence étrangère qui cible directement ou indirectement les processus démocratiques du Canada sont les suivants:

- Bureau du Conseil privé (BCP)
- Sécurité publique Canada (SP)
- Service canadien du renseignement de sécurité (SCRS)
- Centre de la sécurité des télécommunications (CST)
- Affaires mondiales Canada (AMC)
- Gendarmerie royale du Canada (GRC)

Bien que les rôles de producteur et de consommateur de renseignements ne s'excluent pas entièrement mutuellement, en général, le SCRS et le CST sont des producteurs de renseignements, tandis que AMC, la GRC, SP et le BCP sont des consommateurs de renseignements. Les membres de la communauté de la sécurité et du renseignement échangent des renseignements au besoin, dans les limites de leurs mandats, de sorte que chaque producteur de renseignements peut également consommer les renseignements d'autres organismes. Le Groupe de travail sur les menaces à la sécurité et au renseignement pour les élections (MSRE) en est un excellent exemple: le SCRS, le CST, AMC et la GRC ont échangé de l'information et des renseignements pertinents à la fois en tant que producteurs et consommateurs.

Le Parlement a mis en place de solides mécanismes de surveillance et de reddition de comptes pour examiner les activités de la communauté de la sécurité et du renseignement, par l'entremise de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), du commissaire au renseignement et du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR). De plus, plusieurs comités parlementaires, comme le Comité permanent de la sécurité publique et nationale (SECU) et le Comité permanent de la procédure et des affaires de la Chambre des communes (PROC), entendent régulièrement des questions relatives à la communauté de la sécurité et du renseignement.

Les rôles, les mandats et les structures organisationnels des départements et agences clés identifiés ci-dessus sont:

a. Le Bureau du Conseil privé (BCP)

i. Les responsabilités du BCP

Le BCP relève directement du premier ministre. Le BCP:

- Appuie l'élaboration et la mise en œuvre des programmes politiques et législatifs du gouvernement du Canada;
- Soutient le Ministre des Institutions démocratiques;
- Coordonne les réponses aux problèmes auxquels le Gouvernement et le pays sont confrontés;
- Fournit des conseils relies à la sécurité et le renseignement au Premier Ministre; et
- Favorise le bon fonctionnement du Cabinet.

Le BCP est dirigé par le greffier du Conseil privé, qui est également secrétaire du Cabinet, chef de la fonction publique et sous-ministre au premier ministre. En tant qu'organisme central, le BCP coordonne principalement le travail des ministères et organismes gouvernementaux, surveille et développe une connaissance à jour des questions liées aux cas potentiels d'ingérence étrangère.

ii. Participation du BCP à la communauté de la sécurité et du renseignement

a. Conseillère à la sécurité nationale et au renseignement auprès du premier ministre

La conseillère à la sécurité nationale et au renseignement auprès du premier ministre (CSNR) fournit des conseils stratégiques et opérationnels, ainsi que des renseignements, au premier ministre et au Cabinet sur des questions liées à la sécurité nationale, y compris l'ingérence étrangère. La CSNR, le CSNR adjoint et les secrétariats d'appui convoquent la communauté de la sécurité et du renseignement pour assurer la coordination des interventions gouvernementales face à tous les types de menaces d'ingérence étrangère.

En ce qui concerne l'ingérence étrangère, la CSNR est principalement appuyée par deux secrétariats : le Secrétariat Sécurité et renseignement (S&R) et le Secrétariat Évaluation du renseignement (ÉR). En plus de l'information provenant des secrétariats de soutien, la CSNR s'appuie sur l'information fournie par la communauté de la sécurité nationale et du renseignement, y compris des mises à jour sur l'état d'avancement des incidents de sécurité en cours et des renseignements sur les menaces à la sécurité nationale.

Le Secrétariat S&R fournit des conseils stratégiques et un soutien à CSNR sur les questions de sécurité nationale et du renseignement, y compris la coordination des initiatives opérationnelles et d'élaboration de politiques pour les comités interministériels de haut niveau. Le Secrétariat S&R aide la CSNR à informer le premier ministre et le Cabinet sur les principales questions de sécurité nationale et joue un rôle de coordination chaque fois que le Cabinet est saisi de questions de sécurité nationale ou de renseignement. Le Secrétariat S&R travaille en étroite collaboration avec Sécurité publique Canada et d'autres ministères afin de convoquer et d'appuyer des réunions régulières de la haute gouvernance sur les menaces d'ingérence étrangère et les mesures à prendre.

Le Secrétariat ÉR est une unité d'analyse et d'évaluation du renseignement étranger stratégique. Il fournit des analyses et des évaluations du renseignement au premier ministre, au Cabinet, au greffier du Conseil privé et aux hauts fonctionnaires du gouvernement du Canada, et joue un rôle clé de leadership et de coordination interministériels pour les évaluations de la communauté canadienne du renseignement. Le Secrétariat ÉR favorise également les relations avec les organismes alliés d'évaluation du renseignement et renforce la communauté alliée du renseignement grâce à des initiatives horizontales à l'échelle de la collectivité, à des solutions d'entreprise et à de la formation sur l'analyse du renseignement à la fois collaborative et rentable. Le Secrétariat ÉR surveille et évalue l'ingérence étrangère, en examinant les tendances, les menaces et les questions émergentes liées à l'ingérence étrangère en ce qui concerne l'environnement géostratégique qu'il couvre. Le Secrétariat ÉR rend compte de ces questions par l'entremise de sa gamme de produits de renseignement à ses principaux clients, ainsi qu'à l'ensemble de la communauté canadienne de la sécurité et du renseignement.

b. Rôle de coordination du BCP

Le BCP joue un rôle de premier plan dans la coordination des hauts fonctionnaires, y compris les sous-ministres, les sous-ministres adjoints et les directeurs généraux, de divers ministères et organismes de la communauté de la sécurité et du renseignement, au sein de comités thématiques.

b. Sécurité publique (SP)

i. Les responsabilités de SP

Le ministère de la Sécurité publique et de la Protection civile (SP) est responsable des questions de sécurité publique, de sécurité nationale et de gestion des urgences.

Le Ministère élabore et fournit des conseils sur les questions de sécurité nationale au ministre de la Sécurité publique à l'appui des nombreuses activités opérationnelles entreprises par la communauté canadienne de la sécurité et du renseignement. Il agit notamment comme plaque tournante centralisée pour coordonner le travail sur un certain nombre de questions de sécurité nationale, y compris la lutte contre l'ingérence étrangère.

SP fonctionne comme une plaque tournante centralisée pour le travail dans les domaines de la lutte au terrorisme, des infrastructures essentielles, de la cybersécurité et de la sécurité des transports. SP coordonne et fournit un soutien en ce qui a trait à la détection, au rejet, à la prévention, à l'intervention et au rétablissement sur les questions relatives à la sécurité nationale et à la cybersécurité. Il travaille notamment avec des partenaires opérationnels pour fournir des conseils stratégiques au gouvernement sur des questions de sécurité délicates et en constante évolution. SP identifie et s'efforce de combler les lacunes dans la capacité du Canada à aborder et à faire face aux menaces nationales et aux menaces à la cybersécurité. Ces menaces comprennent notamment les rançongiciels, l'influence étrangère, le blanchiment d'argent, le financement du terrorisme, les menaces contre les infrastructures essentielles, les armes de destruction massive, les activités hostiles des États et le terrorisme.

ii. Le rôle de SP dans la communauté de la sécurité et du renseignement

SP supervise cinq organismes : la GRC, le SCRS, l'Agence des services frontaliers du Canada (ASFC), le Service correctionnel du Canada (SCC) et la Commission des libérations

conditionnelles du Canada. De ce nombre, la GRC et le SCRS s'efforcent de lutter contre l'ingérence étrangère.

Le ministre de la Sécurité publique a le pouvoir de donner des directives aux chefs d'organismes, qui sont responsables du contrôle et de la gestion de leur organisme respectif. L'orientation est parfois fournie par le biais d'instruments officiels connus sous le nom de directives ministérielles. La plupart des directives fournissent des lignes directrices de haut niveau et exigent que le sous-ministre ou le chef d'organisme détermine les moyens d'atteindre les objectifs. Dans certains cas, cela est exigé par la loi ; Dans d'autres cas, il peut être souhaitable de le faire par mesure de bonne gouvernance.

c. Service canadien du renseignement de sécurité (SCRS)

i. Responsabilités du SCRS

Créé en 1984, le Service canadien du renseignement de sécurité (SCRS ou le Service) est un service civil de renseignement de sécurité. Le mandat principal du SCRS est d'enquêter sur les menaces à la sécurité du Canada et de conseiller le gouvernement du Canada à ce sujet. La *Loi sur le Service canadien du renseignement de sécurité* (*Loi sur le SCRS*) précise les activités sur lesquelles le Service peut enquêter ainsi que le seuil qui doit être atteint pour que le SCRS puisse enquêter sur des activités. Entre autres, l'article 2 de la *Loi sur le SCRS* définit comme une menace à la sécurité du Canada « l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage » et « les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque ». Le pouvoir du SCRS de recueillir des renseignements sur les menaces à la sécurité du Canada repose principalement sur l'article 12 de la *Loi sur le SCRS*.

Le paragraphe 12(2) précise que le SCRS peut enquêter à l'intérieur ou à l'extérieur du Canada. En plus de son mandat d'enquêter sur les menaces à la sécurité du Canada, le SCRS a également le pouvoir, en vertu de l'article 12.1 de la *Loi sur le SCRS*, de prendre des mesures pour réduire ces menaces dans certaines circonstances.

En plus d'enquêter sur les menaces à la sécurité du Canada, le SCRS recueille des renseignements étrangers au Canada en vertu de l'article 16 de la *Loi sur le SCRS*, c'est-à-dire des renseignements sur les intentions, les moyens et les activités d'un État étranger, d'un groupe d'États étrangers ou de toute personne étrangère. Le SCRS ne peut recueillir de tels renseignements qu'à la demande personnelle du ministre des Affaires étrangères ou du ministre de la Défense nationale et avec le consentement personnel du ministre de la Sécurité publique.

Le dirigeant du SCRS est le directeur. Il sert de sous-ministre pour l'organisation et relève directement du ministre de la Sécurité publique. Le directeur est appuyé par plusieurs directeurs adjoints. La sous-directrice des opérations (SDO) est la plus directement impliquée dans les enquêtes sur la menace que l'ingérence étrangère représente pour le Canada, y compris l'ingérence dans les élections fédérales et les processus démocratiques. La SDO dirige la direction qui est responsable des activités opérationnelles du Service, y compris la collecte de renseignements, les évaluations et les mesures de réduction de la menace. La sous-directrice Politiques et partenariats stratégiques (SDP) est responsable de l'ensemble du cadre de politique stratégique du Service,

incluant la proposition de modifications à la *Loi sur le SCRS* afin que le SCRS puisse mieux faire face aux menaces d'ingérence étrangère.

ii. Participation du SCRS à la communauté de la sécurité et du renseignement

En tant que service civil du renseignement de sécurité du Canada, le SCRS recueille et évalue des renseignements, puis fournit des conseils au gouvernement du Canada, notamment sous forme d'évaluations et de rapports de renseignement qui sont communiqués à d'autres ministères concernés du gouvernement du Canada à des fins d'information et pour leur usage dans leurs propres analyses des menaces. En 2022, le SCRS a produit plus de 2 500 évaluations et rapports sur toutes les menaces sur lesquelles il enquêtait, y compris l'ingérence étrangère.

Les activités de collecte de renseignements du SCRS peuvent servir à faire avancer des enquêtes, à aider le ministre de la Défense nationale ou le ministre des Affaires étrangères, à fournir des évaluations de sécurité aux ministères du gouvernement du Canada, ainsi qu'à fournir des conseils sur l'admissibilité de personnes au Canada ou à diffuser des renseignements, des évaluations et des conseils au gouvernement. Dans le cadre de ses enquêtes, le SCRS peut recourir à un large éventail de techniques opérationnelles plus ou moins intrusives (ex., entrevues avec des cibles, surveillance physique et le pouvoir sous mandat d'intercepter des communications ou d'entrer dans des locaux). Lorsque les enquêtes mettent en cause des institutions fondamentales canadiennes, les politiques et procédures du SCRS fournissent des instructions précises supplémentaires, y compris des directives ministérielles, lesquelles impliquent des considérations spéciales et des approbations accrues.

d. Centre de la sécurité des télécommunications (CST)

i. Responsabilités du CST

Le Centre de la sécurité des télécommunications (CST) est l'organisme national de cryptologie du Canada qui fournit au gouvernement du Canada des renseignements d'origine électromagnétique étrangère (SIGINT), de la cybersécurité et d'assurance de l'information. Le CST intercepte et analyse les communications électroniques étrangères afin de fournir au gouvernement du Canada des renseignements uniques sur les menaces étrangères à la sécurité et à la prospérité du Canada, ainsi que des renseignements importants à l'appui de la politique étrangère et de la prise de décisions. Le CST mène également des cyber opérations actives et défensives pour le Canada en ce qui a trait aux affaires internationales, à la défense et à la sécurité, y compris la cybersécurité. Le Centre canadien pour la cybersécurité du CST aide à protéger les infrastructures fédérales canadiennes et les infrastructures jugées importantes pour le gouvernement contre les cyber activités malveillantes. Le CST fournit de l'aide aux organismes fédéraux d'application de la loi et de sécurité, comme le SCRS et la GRC, ainsi qu'aux Forces armées canadiennes (FAC) et au ministère de la Défense nationale (MDN) dans l'exercice de leurs fonctions légales.

Le dirigeant de l'organisation est le chef du CST. Le chef du CST agit à titre de sous-ministre de l'organisation et relève du ministre de la Défense nationale (MDN). Le chef, sous la direction du ministre de la Défense nationale, est responsable de la gestion et du contrôle du CST et de toutes les questions qui s'y rapportent.

L'article 15 de la *Loi sur le Centre de la sécurité des télécommunications* énonce le mandat du CST en tant qu'organisme national de renseignement électromagnétique pour le renseignement

étranger et autorité technique en matière de cybersécurité et d'assurance de l'information. Ce mandat comporte cinq volets énoncés aux articles 16 à 20 : le renseignement étranger (art. 16) ; la cybersécurité et l'assurance de l'information (art. 17) ; les cyber opérations défensives (art. 18) ; les cyber opérations actives (art. 19) ; et l'assistance technique et opérationnelle (art. 20).

ii. L'implication du CST dans la communauté de la sécurité et du renseignement

Le CST produit plus de 3 200 rapports de renseignement électromagnétiques par année pour aider le gouvernement à prendre des décisions dans les domaines des affaires internationales, de la défense et de la sécurité, y compris l'ingérence étrangère, et pour mieux comprendre les événements mondiaux et les crises et contribuer à promouvoir les intérêts et la sécurité du Canada dans le monde. Les rapports du CST sont communiqués à d'autres organismes pertinents du gouvernement du Canada (le MDN/FAC, le SCRS, la GRC, AMC et le BCP, entre autres) à des fins d'information et pour utilisation conformément à leur propre mandat. Ces rapports sont communiqués aux fonctionnaires qui détiennent l'autorisation appropriée et qui ont besoin de savoir.

Le CST travaille avec ses partenaires cryptologiques du Groupe des cinq (États-Unis, Royaume-Uni, Australie et Nouvelle-Zélande). Ce partenariat dure depuis plus de 77 ans. Grâce à ces partenariats et à d'autres, le CST fournit des renseignements pertinents et opportuns pour répondre aux besoins du Canada en matière de renseignement étranger.

En plus de fournir des services de cybersécurité et d'assurance de l'information pour protéger l'infrastructure fédérale, notamment en bloquant près de six milliards d'activités malveillantes sur le réseau du gouvernement par jour et en protégeant les secrets les plus précieux du Canada, le CST fournit une assistance technique et opérationnelle à des organismes comme le SCRS, la GRC et les FAC. Dans le cadre de la prestation d'assistance, le CST opère sous l'autorité de l'agence requérant pour effectuer l'activité, incluant les exigences relatives à tout mandat applicable.

Le CST tire parti de tous les aspects de son mandat (renseignement étranger, cybersécurité, cyberopérations étrangères et assistance technique et opérationnelle) pour contrer les activités hostiles des États, y compris l'ingérence étrangère. Le CST collabore également avec des partenaires mondiaux et fédéraux pour atténuer les risques posés par les activités de répression transnationales en recueillant des messages SIGINT et en appuyant la communauté canadienne de la sécurité et du renseignement. Le CST est également un acteur important dans la lutte contre la désinformation. Les États étrangers utilisent la désinformation pour déstabiliser la démocratie canadienne. Le CST contribue à des campagnes de sensibilisation à la désinformation à l'échelle du gouvernement afin de contrer les efforts d'ingérence étrangère par la désinformation en ligne.

e. Affaires Mondiales Canada (AMC)

i. Responsabilités d'AMC

Affaires Mondiales Canada (AMC), sous la direction du ministre des Affaires étrangères, du ministre du Commerce international, de la Promotion des exportations, de la Petite Entreprise et du Développement économique et du ministre du Développement international, est chargé de faire progresser les relations internationales du Canada.

ii. L'implication d'AMC dans la communauté de la sécurité du renseignement

Bon nombre des menaces les plus importantes pour la sécurité nationale du Canada, y compris l'ingérence étrangère, sont liées à la politique étrangère. Dans le cadre de son travail de promotion des intérêts mondiaux et régionaux en matière de sécurité et de gestion des relations bilatérales et multilatérales, AMC contribue donc à prévenir les menaces qui pèsent sur les Canadiens et les intérêts internationaux du Canada et à y réagir.

Les renseignements sur les capacités, les intentions et les activités des États étrangers recueillis par les partenaires nationaux et alliés en matière de renseignement éclairent un large éventail d'activités d'AMC, de l'élaboration de politiques à la sécurité des missions du Canada à l'étranger. Par exemple, en vertu de l'article 16 de la *Loi sur le SCRS*, le SCRS peut aider le ministre des Affaires étrangères, au Canada, à recueillir des renseignements étrangers. AMC produit également des rapports diplomatiques spécialisés et fondés sur des sources publiques sur les questions liées à l'ingérence étrangère, ainsi que des évaluations stratégiques du renseignement. La Loi sur le CST prévoit également la nécessité d'obtenir le consentement préalable du ministre des Affaires étrangères pour les cyber opérations actives du CST.

f. Gendarmerie royale du Canada (GRC)

i. Responsabilités de la GRC

La GRC est le service de police national du Canada, dont le mandat est de prévenir le crime, de maintenir la paix, d'appliquer les lois, de contribuer à la sécurité nationale, d'assurer la sécurité des représentants de l'État et de fournir un soutien opérationnel aux organismes d'application de la loi. La GRC tire ses pouvoirs de plusieurs lois, dont la *Loi sur la Gendarmerie royale du Canada*, la *Loi sur les infractions en matière de sécurité*, le Code criminel et la common law. Les manuels administratifs et opérationnels, qui font office de manuels nationaux à l'intention des policiers, font partie des manuels de service qui contiennent les politiques, les procédures et les protocoles qui régissent la GRC.

La prise de décision et l'autorité incombent au commissaire de la GRC, qui est appuyé par l'État-major supérieur (ÉMS), qui comprend le commissaire, le dirigeant principal des ressources humaines, les sous-commissaires, les commandants divisionnaires de la Colombie-Britannique et de l'Alberta, le dirigeant principal des finances, la dirigeante principale des politiques stratégiques et le sous-ministre adjoint principale, Réforme, reddition de comptes et culture.

ii. Participation de la GRC à la communauté de la sécurité et du renseignement

La GRC est l'organisme chargé de l'application de la loi au sein de la communauté canadienne de la sécurité et du renseignement et travaille étroitement avec d'autres organismes et ministères gouvernementaux pour coordonner les efforts et résoudre les problèmes complexes qui nécessitent une intervention multi-institutionnelle.

La GRC collabore également avec les principaux intervenants nationaux et internationaux qui cherchent à mieux faire connaître les domaines prioritaires du gouvernement fédéral en matière d'exécution de la loi, y compris l'ingérence étrangère, au moyen d'initiatives de prévention du crime et de signalement. L'objectif de ces efforts est de réduire la victimisation et d'accroître le signalement à la police et aux partenaires d'activités illicites, y compris l'ingérence étrangère, qui,

autrement, pourraient ne pas faire l'objet d'enquêtes. Les personnes visées par l'ingérence d'acteurs étrangers ignorent peut-être qu'elles peuvent signaler ces activités aux autorités canadiennes. La GRC travaille avec les collectivités canadiennes, les services de police locaux, ainsi qu'avec les entités des secteurs public et privé sur ces questions.

2) L'Alliance du Groupe des cinq

(2) Une description de l'Alliance du Groupe des cinq;

L'alliance du Groupe des cinq (en anglais « Five Eyes ») (FVEY) est un réseau collaboratif d'échange de renseignements composé de cinq pays : le Canada, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande. Créée au lendemain de la Seconde Guerre mondiale, elle est largement considérée comme l'alliance de partage de renseignements la plus importante au monde. Les pays FVEY collaborent pour partager un large éventail d'informations et de renseignements, et coordonner les efforts de sécurité, dans le cadre de l'un des accords multilatéraux les plus unifiés au monde. Les cinq pays membres ont une longue histoire de confiance et de coopération, et ils partagent un engagement envers des valeurs communes. Le partenariat a joué un rôle important dans la sécurité mondiale au cours des sept dernières décennies, renforçant l'échange de renseignements et la coopération entre ses pays membres afin de protéger leur sécurité nationale et leurs intérêts communs.

L'alliance du Groupe des cinq a été créée en temps de guerre pour le partage de renseignements d'origine électromagnétique entre les États-Unis et le Royaume-Uni. En 1948, le traité a été étendu pour inclure le Canada et, en 1955, le statut officiel des autres pays du Groupe des cinq a été officiellement reconnu dans une nouvelle version de l'accord UKUSA.

L'alliance FVEY demeure l'une des relations internationales les plus complètes et les plus importantes pour le Canada et repose sur le respect mutuel des lois, la protection de l'information et la protection des citoyens et des nations respectives des pays membres. Les renseignements échangés au sein du FVEY comprennent le renseignement d'origine électromagnétique (SIGINT), le renseignement humain (HUMINT), le renseignement de défense et géospatial, ainsi que le renseignement de sécurité. L'étendue et la portée de l'information partagée diffèrent entre chacun des organismes canadiens et leurs partenaires équivalents, et vont de l'interopérabilité totale dans certains cas à l'échange transactionnel dans d'autres. Le Canada est un membre actif de l'alliance et en tire un grand bénéfice. L'un des principaux engagements du FVEY est de protéger les renseignements de chacun conformément à la « règle des tiers », qui est une entente selon laquelle les fournisseurs d'information conservent le contrôle de la divulgation et de l'utilisation ultérieure de celle-ci. Le non-respect du Canada risquerait d'entraîner la perte de l'accès à l'énorme quantité de renseignements d'une valeur cruciale que les partenaires du FVEY partagent avec le Canada.

3) Protection de l'information: classifications et diffusion

(3) Une explication des diverses classifications des renseignements protégés et classifiés utilisées par le gouvernement du Canada;

Renseignements classifiés - Intérêt national

Tous les gouvernements, y compris celui du Canada, doivent maintenir un certain degré de sécurité et de confidentialité pour fonctionner. L'intérêt national à ce que les renseignements confidentiels soient traités de façon appropriée peut être plus aigu dans les affaires mettant en cause des renseignements relatifs aux relations internationales, à la défense nationale ou à la sécurité nationale. L'importance de protéger les renseignements dont la divulgation pourrait nuire aux relations internationales, à la défense nationale ou à la sécurité nationale est reconnue depuis longtemps par le Parlement et par les tribunaux canadiens.

En vertu de la *Politique sur la sécurité du gouvernement du* Secrétariat du Conseil du Trésor du Canada, les documents contenant de l'information de nature délicate sont contrôlés au moyen d'un marquage de sécurité approprié pour protéger les renseignements qu'ils contiennent. L'auteur de l'information est responsable de déterminer le marquage approprié, qui offre une protection au moyen de contrôles d'accès basés sur des cotes de sécurité et des endoctrinements. La *Norme sur la catégorisation de sécurité* détaille les catégories de classification utilisées pour protéger les renseignements en fonction des dommages potentiels aux intérêts nationaux du Canada auxquels on pourrait raisonnablement s'attendre à la suite d'une divulgation non autorisée de ces renseignements. Les catégories d'informations protégées et classifiées sont détaillées ci-dessous.

De plus, les informations classifiées doivent être traitées dans des zones de sécurité dûment accréditées. Une zone de sécurité est une zone dont l'accès est limité au personnel autorisé et aux visiteurs dûment escortés. De plus, les renseignements classifiés ne peuvent être transmis que conformément aux politiques de sécurité et ne peuvent être transportés que par des personnes dûment autorisées à l'aide de contenants sécurisés approuvés pour le niveau d'information à transporter. Enfin, d'autres restrictions sont en place en ce qui concerne l'impression, la copie et la destruction de copies de documents classifiés.

Informations protégées

S'applique aux renseignements ou aux biens qui, s'ils étaient compromis, pourraient vraisemblablement causer un préjudice à un intérêt non national, c'est-à-dire à un intérêt individuel comme celui d'une personne ou d'une organisation. Les niveaux sont les suivants:

- PROTÉGÉ A: S'applique aux renseignements ou aux biens qui pourraient porter préjudice à une personne, à une organisation ou à un gouvernement s'ils étaient compromis. Par exemple, le salaire exact d'une personne.
- PROTÉGÉ B: S'applique aux renseignements ou aux biens qui pourraient porter un préjudice grave à une personne, à une organisation ou à un gouvernement s'ils étaient compromis. Par exemple, la perte de réputation ou d'avantage concurrentiel, et les enquêtes criminelles.
- PROTÉGÉ C: S'applique aux renseignements ou aux biens qui pourraient porter un préjudice extrêmement grave à une personne, à une organisation ou à un gouvernement s'ils étaient compromis. Par exemple, des pertes financières catastrophiques ou des pertes de vie.

Informations classifiées

S'applique aux renseignements ou aux biens qui, s'ils étaient compromis, pourraient vraisemblablement causer un préjudice à l'intérêt national, à la défense et au maintien de la stabilité sociale, politique et économique du Canada. Les niveaux sont les suivants:

- CONFIDENTIEL : S'applique aux renseignements ou aux biens qui pourraient porter préjudice à l'intérêt national s'ils étaient compromis. Par exemple, l'atteinte aux relations diplomatiques du Canada ou à ses intérêts économiques à court terme.

- SECRET: S'applique aux renseignements ou aux biens qui pourraient porter des préjudices graves à l'intérêt national s'ils étaient compromis. Par exemple, des blessures graves à des infrastructures essentielles ou à des opérations de renseignement.
- TRÈS SECRET: S'applique aux renseignements ou aux biens qui pourraient porter un préjudice extrêmement grave à l'intérêt national s'ils étaient compromis. Par exemple, une atteinte grave à la sécurité des Forces armées canadiennes, des relations avec des gouvernements aux vues similaires ou des pertes de vie.

Systèmes de contrôle

Un système de contrôle est un cadre administratif qui protège les sources de renseignements de nature délicate (renseignements classifiés) en établissant des normes pour l'accès, le marquage, le traitement et le contrôle des renseignements provenant de la source de renseignement ou liés à celle-ci. Les informations protégées par les systèmes de contrôle sont également connues sous le nom d'informations cloisonnées.

Par exemple, le renseignement spécial (SI) est le système de contrôle qui limite l'accès au renseignement d'origine électromagnétique (SIGINT) et vise à limiter l'accès à ces informations à ceux qui sont autorisés à recevoir des renseignements sur les transmissions d'origine électromagnétique. L'information SI nécessite des protocoles de manipulation spéciaux. Le système de contrôle SI comporte deux autres sous-systèmes de contrôle : GAMMA et Information Exceptionnellement Contrôlée (ECI), afin d'imposer des limites supplémentaires à l'accès aux informations particulièrement sensibles.

- GAMMA: ce système et ses sous-compartiments correspondants protègent les rapports SIGINT particulièrement sensibles et les informations connexes.
- ECI: ce système est composé de plusieurs programmes: chaque programme ECI et ses sous-compartiments correspondants protègent les informations relatives à une capacité, une méthode ou une technique particulièrement sensible.
- L'accès à l'information GAMMA ou ECI nécessite des endoctrinements supplémentaires spécifiques à ce système de contrôle et à ce compartiment.

Ces systèmes de contrôle nécessitent des protocoles de manipulation spéciaux, et même ceux qui ont une cote de sécurité Très secret peuvent ne pas avoir les endoctrinements requis pour accéder à tous les niveaux cloisonnés. Des mesures doivent donc être prises pour s'assurer que les personnes disposent de la cote, de l'endoctrinement et du besoin de savoir appropriés avant que l'information ne soit partagée, même au sein de la communauté de la sécurité et du renseignement.

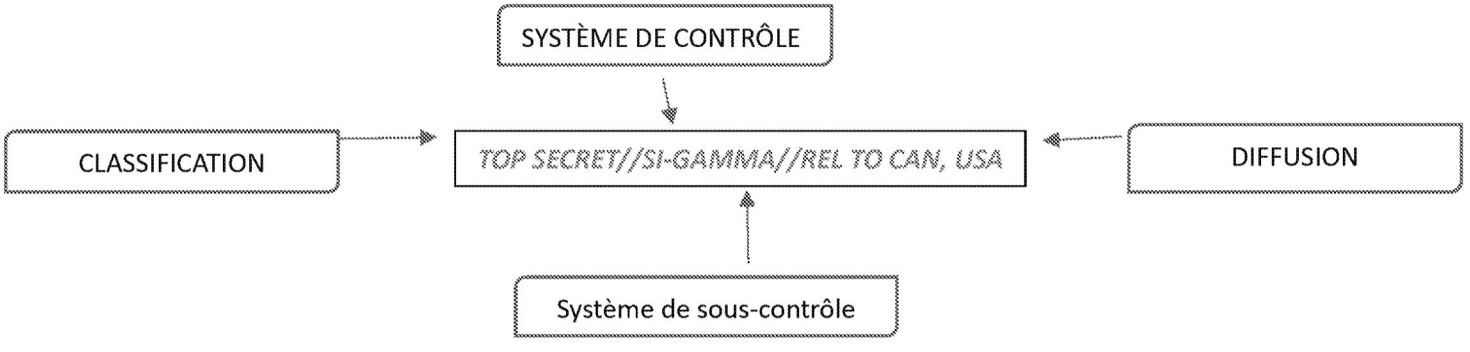
Endoctrinements

Tel que mentionné précédemment, ce ne sont pas toutes les personnes qui ont une cote de sécurité Très secret qui auront accès à une partie ou à la totalité de l'information cloisonnée. Les individus sont endoctrinés dans un système de contrôle ou un système de sous-contrôle en fonction de leur

besoin de connaître l'information. La plupart des systèmes de contrôle s'appuient sur le cadre de la *Loi sur la protection de l'information* pour les renseignements opérationnels spéciaux, et l'accès nécessite une autorisation TS et un statut de « secret à perpétuité » (décrit plus en détail ci-dessous).

Contrôle de la diffusion

Des marques de contrôle de la diffusion sont utilisées pour limiter la distribution de renseignements classifiés à des personnes, des groupes ou des nationalités spécifiques, par exemple en limitant la diffusion de renseignements *à CANADIAN EYES ONLY (CEO),* conformément à leur « besoin de savoir » et à leur niveau de cote de sécurité.



Loi sur la protection de l'information

La *Loi sur la protection de l'information* (« LPI ») est une loi du Parlement du Canada qui criminalise la communication des renseignements gouvernementaux les plus sensibles sur le plan opérationnel.

Certains ministères, certaines catégories de personnes (employés anciens et actuels) et certaines personnes désignées qui, en raison de leur poste, auraient accès à des « renseignements opérationnels spéciaux » sont astreints au secret à perpétuité en vertu de la LPI. Il s'agit de personnes qui sont assujetties à un niveau de responsabilité plus élevé à l'égard des communications non autorisées de renseignements obtenus dans le cadre de leur travail, par exemple, le renseignement militaire, les employés du SCRS et du CST, et certains membres de la GRC. L'Enquête publique sur l'ingérence étrangère dans les processus électoraux fédéraux et les institutions démocratiques est également restreinte au secret à perpétuité.

Déclassification et déclassement

- Le déclassement ou nettoyage est le processus visant à abaisser la classification du renseignement. Par exemple, un document dont la classification initiale était TRÈS SECRET//SI//CEO peut être nettoyé en SECRET//PDG, si l'information contribuant à la classification TRÈS SECRET et au système de contrôle SI est supprimée.
- La déclassification est le processus qui consiste à rendre les informations classifiées non classifiées. En règle générale, il s'agit de supprimer ou de modifier tous les renseignements qui, s'ils étaient divulgués publiquement, pourraient porter atteinte à l'intérêt national, par exemple en fournissant à un adversaire les sources et les méthodes d'obtention de l'information.

L'organisme d'où origine le renseignement est l'autorité chargée de déclasser ou de déclassifier le renseignement. Si les renseignements produits comprennent des renseignements obtenus par un organisme partenaire national ou un partenaire international, l'organisme d'origine doit consulter ce partenaire au sujet du déclassement ou de la déclassification de ses renseignements, et doit obtenir l'approbation de ce partenaire pour le faire. Pour déterminer s'il y a lieu de déclasser ou de déclassifier l'information, l'organisme d'origine doit soupeser l'intérêt public à rendre l'information disponible par rapport au risque et aux coûts associés à la divulgation de l'information.

4) Protection de l'information : privilèges et immunités

(4) Une explication des divers privilèges et immunités qui pourraient s'appliquer aux documents produits par le gouvernement du Canada à la Commission dans le cadre de ses travaux;

L'atteinte à la sécurité nationale et le besoin de protection

Le secret est essentiel pour le renseignement. Pour que les services de renseignement fonctionnent efficacement, les connaissances, les sources et les méthodes utilisées pour obtenir l'information, ainsi que l'étendue de l'information qu'ils recueillent, doivent demeurer confidentielles. Cela protège l'intégrité des enquêtes, des méthodologies et des capacités passées, présentes et futures de nos agences de renseignement. Bien que les organismes puissent obtenir des renseignements de diverses sources, dans de nombreuses circonstances, cette collecte est effectuée secrètement et, par conséquent, les méthodes et les sources de cette collecte ne peuvent être divulguées.

Alors que les pays s'appuient de plus en plus sur des systèmes numériques et des réseaux d'information interconnectés, la vulnérabilité des données et des informations sensibles a augmenté de manière exponentielle. Le préjudice causé au Canada par la divulgation illégale de renseignements est important. Lorsque ces informations sont divulguées en dehors des réseaux autorisés, elles peuvent entraîner des conséquences désastreuses : compromettre les opérations de sécurité nationale ou exposer des sources et des méthodes humaines ou techniques, ce qui peut potentiellement mettre en danger la vie des personnes impliquées (y compris les consommateurs de ces renseignements). Il y a aussi le risque de perdre l'accès à des sources d'information techniques, qu'il est très coûteux pour le Canada d'obtenir et de conserver. De plus, il y a un risque d'atteinte à la confiance et la coopération dont jouit le Canada avec ses plus proches partenaires et alliés, comme le Groupe des cinq. Cela nuirait à la sécurité nationale, à la position du Canada sur le plan mondial et poserait des risques pour la stabilité géopolitique et économique du Canada.

La divulgation non autorisée des connaissances opérationnelles à un moment donné, l'évaluation opérationnelle précise faite par l'organisme ou le fait que l'organisme est en mesure de tirer certaines conclusions concernant un sujet ou une cible pourraient indiquer le niveau d'intérêt, ou l'absence d'intérêt envers une personne ou un groupe à divers moments dans le temps et le fait que l'organisme dispose de suffisamment d'information pour faire une évaluation ou tirer une conclusion. La divulgation non autorisée de renseignements protégés pourrait également:

- permettre à un sujet d'intérêt d'introduire délibérément des informations fausses ou trompeuses dans une enquête s'il apprend qu'il fait l'objet d'une enquête;
- avoir une incidence sur la portée et la fiabilité de l'information disponible, car on ne sait pas s'il s'agit d'une information fausse ou trompeuse;

- permettre l' utilisation de contre-mesures par les personnes faisant l'objet d'une enquête ou des cibles opérationnelles contre des activités d'enquête futures, ce qui entraînerait une lacune dans les renseignements liés à la menace.

Le 15 décembre 2023, le Canada a remis à la Commission une lettre qui explique plus en détail les préjudices causés aux relations internationales, à la défense nationale et à la sécurité nationale. Cette lettre se retrouve à **l'onglet B.**

Privilèges et immunités

Les Règles de pratique et de procédure prévoient que les documents produits à la Commission par les participants peuvent faire l'objet des privilèges et immunités applicables. Bien que d'autres privilèges et immunités puissent également s'appliquer[1], les deux suivants sont particulièrement mentionnés:

- Article 37 de la *Loi sur la preuve au Canada:* Immunité d'intérêt public déterminé (« IIPD »)
- Article 38 de la *Loi sur la preuve au Canada:* Relations internationales, défense nationale ou privilège relatif à la sécurité nationale (« Confidentialité relative à la sécurité nationale » ou « CRSN »)

La Loi sur la preuve au Canada (« LPC »)

L'article 37 de la LPC offre une protection contre la divulgation des renseignements assujettis à une IIPD. La LPC ne définit pas ce qu'est un « intérêt public déterminé »; ceci doit être évaluée au cas par cas. Les types de renseignements souvent protégés par l'IIPD comprennent les renseignements qui permettraient d'identifier un informateur confidentiel; les informations relatives aux enquêtes criminelles en cours; les renseignements qui doivent être protégés afin d'assurer la sécurité des policiers, des témoins, des victimes et des employés; les techniques d'enquête policière et les renseignements de nature délicate; les communications et les renseignements internes de la police ; et les ressources et la structure organisationnelles dans certains contextes opérationnels.

L'article 38 offre une protection contre la divulgation de renseignements qui seraient préjudiciables aux relations internationales, à la défense nationale ou à la sécurité nationale s'ils étaient divulgués. Voir ci-dessous pour plus de détails sur la CRSN.

L'article 39 offre une protection contre la divulgation des renseignements confidentiels du Cabinet. L'article 39 de la LPC stipule que l'attestation par écrit qu'un renseignement constitue un renseignement confidentiel du Cabinet empêchera la divulgation de celui-ci sans qu'il soit nécessaire de l'examiner ou de tenir d'audition à son sujet.

Article 38 de la LPC (CRSN)

L'article 38 de la LPC crée un processus visant à protéger les renseignements dont la divulgation, dans le cadre d'une procédure, porterait atteinte aux relations internationales, à la défense nationale

[1] Tels que le privilège lié au secret professionnel de l'avocat, aux renseignements confidentiels du cabinet et au privilège relatif au litige.

ou à la sécurité nationale. Les personnes impliquées dans des procédures où il est possible que des renseignements de ce type soient divulgués doivent en aviser le procureur général du Canada (PGC). Cet avis permet au PGC de décider s'il y a lieu ou non d'autoriser la divulgation des renseignements. Si le PGC n'autorise pas la divulgation des renseignements, ou n'autorise la divulgation que d'une partie de l'information, un recours judiciaire auprès de la Cour fédérale du Canada peut être exercé.

Concrètement, les renseignements qui peuvent être protégés en vertu de la CRSN comprennent les renseignements qui révèlent ou tendent à révéler:

- l' identité d'une source d'information confidentielle, autre que les sources humaines du SCRS;
- les cibles d'une enquête;
- les sources techniques d'information;
- les méthodes d'opération et les techniques d'enquête;
- l'identité des employés sous couverture;
- les télécommunications et les systèmes de chiffrement (cryptologie);
- la relation confidentielle avec un gouvernement ou un organisme étranger et les renseignements qu'il a partagés en toute confidentialité;
- les échanges diplomatiques confidentiels;
- les critiques à l'égard d'un gouvernement étranger qui nuiraient aux relations internationales;
- l'information divulguant les stratégies et les objectifs du gouvernement canadien en matière d'affaires étrangères;
- des renseignements consulaires se rapportant à une cible précise d'une enquête de sécurité nationale;
- les caractéristiques, les capacités, le rendement, le déploiement potentiel et les fonctions ou rôles des Forces canadiennes;
- les opérations militaires et les politiques relatives à la conduite des opérations militaires;
- les opérations, les organisations et les sources de renseignement;
- l'équipement militaire et les systèmes de télécommunications.

Bien que la cote de sécurité d'un document puisse indiquer que sa divulgation pourrait nuire aux relations internationales, à la défense nationale ou à la sécurité nationale, la classification elle-même n'est pas déterminante pour ces questions.

Restrictions législatives en matière de divulgation

Les restrictions législatives en matière de divulgation qui peuvent s'appliquer aux renseignements fournis à la Commission pourraient comprendre:

- Ordonnances de non-publication d'un tribunal;
    - *Code criminel :* article 164, articles 278.1 et 278.9, article 320, article 486.4, article 486.5, article 487.2, article 517, paragraphe 520(9), article 539, paragraphe 542(2), paragraphe 631(6), article 672.501
    - Lois provinciales (p. ex., paragraphe 137(2) de *la Loi sur les tribunaux judiciaires de l'Ontario)*
- Mandats scellés;
    - Article 487.3 du *Code criminel;*
- Autorisations d'écoute électronique;
    - Articles 187 et 193 du *Code criminel;*
- *Loi sur l'accès à l'information;*
    - Paragraphes 13(1), 15(1) et articles 16, 17 et 19;
- *Loi sur le casier judiciaire;*
    - Paragraphe 6(2), article 6.1;
- *Loi sur la protection des renseignements personnels;*
    - Articles 7, 8(1) et 22;
- *Loi sur la protection de l'information,* Articles 4 et 14;
- *Loi sur la statistique,* Article. 17;
- *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*
    - Paragraphes 55(1) et 59(1)
- *Loi sur le Service canadien du renseignement de sécurité* (*Loi sur le SCRS*)
    - Paragraphes 18(1) et 18.1
- *Loi sur le Centre de la sécurité des télécommunications* (*Loi sur le CST*)
    - Article 55

Paragraphes 18(1) et 18.1 de la Loi sur le SCRS

La *Loi sur le SCRS* interdit la divulgation de renseignements permettant de découvrir l'identité d'un employé du SCRS qui a participé ou pourrait participer à des activités opérationnelles cachées. La *Loi sur le SCRS* interdit également la divulgation, dans le cadre d'une instance, de l'identité d'une source humaine ou de toute information qui permettrait de découvrir l'identité d'une source humaine.

Article 55 de la Loi sur le CST

La *Loi sur le CST* interdit la divulgation, dans le cadre d'une instance, de l'identité d'une personne ou d'une entité qui assiste ou a assisté le CST de manière confidentielle, ou de toute information qui permettrait de découvrir l'identité d'une telle personne ou entité.

5) Protection de l'information : caviardage et contestation

(5) Une explication du processus interne entrepris par le gouvernement du Canada lorsqu'il répond à une demande de la Commission pour qu'un document soit rendu public, y compris :

a. le processus interne permettant de déterminer si des renseignements devraient être caviardés en vertu d'un privilège ou d'une immunité applicable, y compris une description des postes/rôles des personnes responsables de l'analyse et des décisions finales ; et

b. Le processus interne entrepris lorsque la Commission remet en question ou conteste un caviardage, y compris une description des positions/rôles des personnes responsables des positions prises par le gouvernement et des interactions avec la Commission.

Processus de l'équipe interne de litige pour déterminer si l'information doit être caviardée, y compris les positions des personnes responsables

Avant que les documents soient produits à la Commission, ils sont examinés et caviardés afin de protéger le secret professionnel de l'avocat, les renseignements secrets du Cabinet et le privilège relatif au litige, étant entendu que le Canada ne renonce à aucune autre restriction applicable en matière de privilège, d'immunité ou de divulgation. Cela permet de faciliter la production en temps opportun des documents à la Commission.

Lorsque la Commission demande que des documents soient rendus publics ou qu'elle indique qu'ils seront utilisés dans le cadre d'une partie du processus de la Commission, les documents identifiés par la Procureure de la Commission sont examinés par l'équipe de litige afin de déterminer à qui appartient chaque document (c.-à-d. le ministère ou l'organisme canadien qui l'a produit ou reçu en premier). Les ministères et organismes seront invités à informer l'équipe de litige de tous les caviardages que leur ministère ou organisme pourrait devoir appliquer sur ces documents avant qu'ils ne soient divulgués au public. L'équipe de litige demandera également aux ministères et organismes de les informer si, au cours de leur examen, ils prennent connaissance d'autres ministères ou organismes dont les renseignements peuvent être contenus dans les documents en question. Chaque ministère ou organisme présentera ses propositions de caviardage à l'équipe de litige, en précisant le fondement de chacune d'entre elles.

Après avoir appliqué électroniquement le caviardage proposé, l'équipe de litige enverra au ministère ou organisme tous les documents caviardés par ce dernier, tous leurs caviardages étant identifiés par des surbrillances transparentes. On demandera au ministère ou à l'organisme de confirmer l'application appropriée des caviardages à ses renseignements (l'approbation de couleur).

Le début du processus est légèrement différent pour les documents du SCRS. Compte tenu des sensibilités particulières liées à l'information du SCRS en question, ainsi que de l'efficacité obtenue en réduisant le dédoublement de l'examen, l'équipe de litige enverra d'abord tous les documents appartenant au SCRS à ce dernier pour qu'il les examine. Une fois le caviardage du SCRS finalisé et l'approbation de couleur terminée, les renseignements dont le SCRS demande la protection seront caviardés (remplacés par un caviardage noir), et ces documents seront ensuite envoyés à d'autres ministères et organismes pour examen. Tous les autres ministères et organismes indiqueront à l'équipe de litige le caviardage qu'ils proposent

sur les documents du SCRS. Le caviardage de chaque ministère ou organisme fera ensuite l'objet d'une approbation de couleur par ce ministère ou organisme.

Une fois toutes les approbations de couleur propres au ministère ou à l'organisme effectuées, une version caviardée des documents sera préparée. Cette version vise à représenter les documents tels qu'ils apparaîtraient s'ils étaient rendus publics. Chaque ministère et organisme participant au processus sera invité à examiner la version caviardée pour s'assurer qu'aucun renseignement préjudiciable ne demeure non protégé. Une fois les approbations reçues de tous les ministères et organismes, les documents seront préparés pour être produits à la Commission. Ce processus prend une quantité considérable de temps et de ressources.

Au fur et à mesure que le processus de caviardage progresse, toutes les modifications apportées aux caviardages feront l'objet d'un suivi électronique par le système de gestion des documents du PGC.

Le temps nécessaire aux ministères et organismes et à l'équipe de litige pour s'acquitter de leur rôle d'examen et de production de documents dépendra de facteurs tels que la nature, la complexité, le nombre total et la longueur des documents à examiner. L'examen des caviardages requis par la CRSN et l'IIPD implique l'examen systématique de chaque mot de chaque document, souvent plusieurs fois, afin d'en assurer l'exactitude et la cohérence. Par exemple, le SCRS effectue une analyse pour déterminer la source de l'information contenue dans le document, la nature délicate de la source, s'il s'agit ou non de renseignements provenant des partenaires, analyse les déclarations publiques du SCRS et effectue une remise en question interne. Cet examen ne peut être effectué que par un nombre limité de personnes qui possèdent la cote de sécurité nécessaire et qui sont familiers avec le préjudice qui résulterait de la divulgation. Le temps requis est également affecté par l'obligation pour les personnes concernées de suivre des règles et les procédures applicables à ces documents.

Processus interne du ministère ou de l'organisme pour déterminer si l'information doit être caviardée, y compris les postes des personnes responsables.

Habituellement, un groupe restreint de personnes est responsable du processus d'examen du caviardage. Ces personnes sont normalement des experts en la matière. Les experts en la matière sont des personnes qui possèdent des connaissances factuelles spécialisées et des connaissances contextuelles en lien avec les questions soulevées dans une instance particulière. Les personnes responsables de l'examen au sein d'un ministère ou d'un organisme identifient le caviardage proposés propres aux intérêts de ce ministère ou organisme particulier et expliquent les motifs au soutien de la protection de l'information. Au sein d'un ministère ou d'un organisme, un ensemble de documents proposés pour la production est généralement examiné plusieurs fois par différents représentants des clients (à la fois pour s'assurer que l'examen est effectué par des personnes ayant différentes expertises ainsi que pour assurer le contrôle de la qualité) et peut également être examiné par un avocat de l'Unité des services juridiques ministériels (USJM). Par exemple, au sein de la GRC, le caviardage est d'abord proposé par des analystes. Le caviardage proposé est ensuite examiné par un groupe d'experts en la matière, puis une fois de plus par un autre expert en la matière avant que les documents ne soient examinés par l'avocat de l'USJM. Une fois le processus d'examen interne terminé, le caviardage proposé est envoyé à l'avocat de litige. En plus des discussions avec les avocats de litige, les ministères et organismes de la communauté de la sécurité et du renseignement peuvent se consulter mutuellement en ce qui concerne le caviardage potentiel liés à la CRSN et de l'IIPD.

Processus interne lorsque la Commission remet en question un caviardage, y compris les positions des responsables

Lorsque la Commission remet en question ou conteste un caviardage, la procédure est la suivante:

- L'avocat de l'équipe de litige acheminera la contestation au ministère ou à l'organisme concerné.
- Le ministère ou l'organisme déterminera, au niveau opérationnel (c.-à-d. expert en la matière), quel avis sera fourni au sous-ministre adjoint ou à l'équivalent responsable (SMA) au sujet du préjudice et de l'exigence de caviardage. Le ministère ou l'organisme peut proposer une autre méthode pour rendre ces renseignements publics, comme un résumé. D'autres ministères et organismes seront consultés à cette étape, au besoin. Il se peut que le ministère ou l'organisme doive effectuer d'autres recherches ou consultations afin de répondre adéquatement à la contestation.
- L'avis sera ensuite transmis au SMA pour approbation. Le SMA déterminera si un caviardage peut être levé à ce stade (peut-être qu'un caviardage a été effectué par erreur ou que l'analyse du préjudice a surévalué le risque). Le SMA peut également décider de soulever la question au niveau du sous-ministre ou son équivalent (SM). Si une décision est prise au niveau du SMA, l'équipe de litige en sera informée à cette étape.
- Si la question est portée au SM, celui-ci prendra une décision en fonction de la recommandation du SMA, de tout avis juridique et de toute information reçue d'autres organismes. La décision du SM sera communiquée à l'équipe de litige à ce stade.
- L'équipe de litige s'acquittera d'une fonction de remise en question tout au long du processus décisionnel du ministère ou de l'organisme, en faisant appel au groupe de la sécurité nationale du ministère de la Justice, au besoin.
- La décision finale sur toutes les contestations de la Commission demeurera entre les mains du SM du ministère ou de l'organisme en question et sera communiquée à la Commission par l'intermédiaire de l'avocat du litige.
- Si le Commissaire conteste la décision prise, il peut y avoir un recours devant la Cour compétente conformément aux lois applicables. En ce qui concerne les renseignements à l'égard desquels la commissaire conclut qu'ils ne porteraient pas atteinte aux intérêts essentiels du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale, et en avise le PGC, conformément au mandat, ceci constituera un avis en vertu de l'article 38 de la LPC. Le PGC prendra ensuite une décision quant à la divulgation des renseignements. À la suite de cette décision, d'autres recours sont disponibles auprès de la Cour fédérale, au besoin, conformément à l'article 38.04.

ONGLET A – Lettre datée du 15 décembre 2023 de la part du Canada à la procureure de la Commission

Department of Justice Canada
Civil Litigation Section
National Litigation Sector
50 O'Connor Street, Suite 500
Ottawa, ON K1A 0H8

Ministère de la Justice Canada
Section du contentieux des affaires civiles
Secteur national du contentieux
50, rue O'Connor, bureau 500
Ottawa (ON) K1A 0H8

PAR COURRIEL

Lettre non classifiée
avec pièces jointes « Très secret »

15 décembre 2023

Shantona Chaudhury
Procureure en chef
Enquête publique sur l'ingérence étrangère
dans les processus électoraux et les institutions démocratiques

Me Chaudhry:

Re: ***Examen de la confidentialité des 13 documents sélectionnés pour sécurité nationale***

L'Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux (l'« Enquête ») a été mise sur pied en septembre 2023 à la suite de l'accord du gouvernement du Canada, des chefs de tous les partis reconnus à la Chambre des communes et de l'honorable juge Marie-Josée Hogue sur le mandat proposé.

Suite à sa nomination, la Commissaire a eu l'occasion d'examiner certains renseignements liés aux travaux de l'Enquête. La Commission d'enquête a demandé au gouvernement du Canada d'examiner une partie de ces documents (les documents sélectionnés) auxquels elle a accès afin d'évaluer à quoi ressembleraient ces documents s'ils étaient utilisés publiquement.

Le gouvernement a terminé cet exercice, et la présente correspondance contient une réponse en six éléments : (i) la présente lettre ; (ii) les documents sélectionnés qui ont été caviardés pour permettre leur divulgation publique ; (iii) les documents sélectionnés avec surlignage transparent identifiant la justification de chaque caviardage ; (iv) une annexe classifiée fournissant des informations supplémentaires sur le préjudice qui résulterait de la divulgation ; (v) un guide de codage qui identifie le préjudice associé à chaque caviardage ; et (vi) des résumés de trois rapports de renseignement du Service canadien du renseignement de sécurité (SCRS) tirés des documents sélectionnés et préparés à des fins de discussion (voir ci-dessous les autres options pour aller de l'avant). Les points (i) et (ii) ne sont pas classifiés, et le gouvernement consent à leur divulgation publique. Les points (iii), (iv), (v) et (vi) sont classifiés et ne peuvent être divulgués publiquement.

Les documents en cause démontrent concrètement l'une des contraintes les plus difficiles auxquelles la Commission d'enquête sera confrontée dans l'exécution de son mandat. Bien que les audiences publiques sur les défis, les limites et les effets préjudiciables potentiels associés à la divulgation au public d'information et de renseignement classifiés sur la sécurité nationale soient envisagées à l'alinéa a)(i)(D) du mandat de l'enquête, l'exercice actuel met en lumière plusieurs des considérations applicables. Le gouvernement a proposé certains outils à la Commission et demeure disponible pour en discuter à sa convenance.

Quelques définitions sur l'information dite classifiée, sensible et préjudiciable

En particulier, il est utile de préciser, en termes généraux, certaines définitions qui s'appliquent aux travaux de la Commission d'enquête.

Premièrement, l'expression « renseignements classifiés » s'applique aux renseignements dont la divulgation non autorisée pourrait vraisemblablement causer un préjudice à l'intérêt national. Les informations classifiées peuvent être classées au niveau « Confidentiel », « Secret » et « Très secret ». À titre d'exemple, la classification « Très secret » s'applique aux renseignements dont on peut raisonnablement s'attendre à ce que la divulgation non autorisée cause un préjudice extrêmement grave à l'intérêt national s'ils étaient compromis.

De même, l'expression « information cloisonnée » fait référence à l'information provenant de sources et de méthodes de nature délicate. L'accès à une information cloisonnée est limité aux citoyens canadiens ayant obtenu une cote de sécurité de niveau « Très secret » qui sont autorisés à accéder à des informations après avoir suivi une séance d'endoctrinement officiel. Le cloisonnement est mis en œuvre par le contrôle de l'accès à des informations au moyen de cadresappelés systèmes de contrôle. Les systèmes de contrôle déterminent qui peut avoir accès à des informations et à quelles conditions. Une grande partie de ces renseignements sont également des « renseignements opérationnels spéciaux » en vertu de la *Loi sur la protection de l'information*.

En plus de ces classifications, les « renseignements sensibles » sont des renseignements qui concernent les relations internationales ou la défense ou la sécurité nationales à l'égard desquels le gouvernement du Canada prend des mesures de protection. À leur tour, les « renseignements préjudiciables » sont des renseignements qui, s'ils sont divulgués porteraient préjudice aux relations internationales ou à la défense ou à la sécurité nationales du Canada.

Bien qu'il existe diverses politiques gouvernementales en matière de protection des renseignements classifiés, le Parlement a établi un régime exhaustif de protection des renseignements sensibles et préjudiciables, qui figure à l'article 38 de la *Loi sur la preuve au Canada* et sur lequel la Cour fédérale du Canada a compétence et peut se prononcer. Conformément aux alinéas a)(iii)(E) et a)(iv) du mandat, la Commission d'enquête est assujettie à ces restrictions et à d'autres qui comprennent notamment l'obligation de protéger les sources humaines en vertu de l'article 18.1 de la *Loi sur le Service canadien du renseignement de sécurité*.

L'explication du préjudice

Les documents sélectionnés ont été rédigés à l'intention d'un public qui se limite aux personnes détenant l'attestation de sécurité requise. Par conséquent, les documents comprennent une

quantité importante d'information hautement classifiée, sensible et préjudiciable qui ne peut pas être divulguée et qui doit être soigneusement protégée. En effet, une proportion importante de cette information ne pourrait être rendue publique, quelles que soient les circonstances, sans nuire à la sécurité nationale, à la défense nationale ou aux relations internationales du Canada.

À titre d'exemple, lorsque le gouvernement affirme que la divulgation serait préjudiciable à la sécurité nationale, à la défense nationale ou aux relations internationales, cela peut signifier notamment que:

- En ce qui concerne la *sécurité nationale*, la divulgation nuirait aux opérations ou aux enquêtes en cours ou futures, mettrait en danger les personnes qui travaillent ou collaborent avec les ministères et organismes du gouvernement et permettrait aux acteurs de menace de prendre des contre-mesures. Par exemple, la divulgation peut révéler, directement ou indirectement :
    - L'intérêt envers des personnes, des groupes ou des enjeux, y compris l'existence ou l'inexistence de dossiers ou d'enquêtes passés ou présents, l'intensité des enquêtes, ou le niveau de succès ou l'échec des enquêtes ;
    - Des modes d'opération et des techniques d'enquête ;
    - Les relations avec d'autres services de police, de sécurité et de renseignement, ainsi que les renseignements échangés à titre confidentiel avec ces organismes ;
    - Les employés, les procédures internes, les méthodologies administratives et les systèmes de télécommunications ; et
    - Les personnes qui collaborent avec les organismes de renseignement canadiens ou qui leur fournissent des renseignements confidentiels.

- En ce qui concerne les *relations internationales*, la divulgation nuirait aux relations du Canada avec d'importants alliés. Cela comprend l'échange d'informations entre pays étrangers et la capacité de mener de tels échanges dans un climat de confiance afin de s'assurer que l'information est aussi complète et exacte que possible. La divulgation de telles informations compromettrait ou porterait atteinte à la confiance non seulement de la nation à laquelle elles se rapportent, mais aussi d'autres nations étrangères. Le Canada profite énormément de ces échanges et il doit conserver la confiance de tous les pays étrangers pour continuer d'en profiter. De même, la « règle des tiers » est une entente entre les partenaires d'échange d'information selon laquelle les fournisseurs d'information conservent le contrôle de la divulgation et de l'utilisation ultérieure de celle-ci. Une violation de la règle des tiers pourrait avoir une incidence négative sur les relations entre les partenaires, dont la plus prévisible est l'arrêt ou la réduction de l'échange de renseignements à l'avenir.

Lors de l'examen des documents sélectionnés, le gouvernement a analysé les renseignements en cause et a consacré des ressources importantes à la détermination de l'étendue du préjudice qui pourrait découler de la divulgation publique de ces renseignements. Si la Commission d'enquête insistait à divulguer au public l'information contenue dans les documents sélectionnés, le gouvernement s'opposerait, au besoin, à toute divulgation de l'information contenue, en vertu de l'article 38 de la *Loi sur la preuve au Canada*.

La majorité des documents sélectionnés proviennent du SCRS. Le caviardage de ces documents a été effectué par le SCRS, le Centre de la sécurité des télécommunications, Affaires mondiales Canada, la Gendarmerie royale du Canada et le Centre d'analyse des opérations et déclarations financières du Canada. Le résultat de cet exercice d'examen documentaire démontre que les documents du SCRS sont caviardés presque dans leur intégralité. Étant donné que la majorité des caviardages effectués dans les documents sélectionnés sont liés à l'information du SCRS, la présente lettre porte davantage sur les renseignements du SCRS.

Les renseignements provenant du SCRS

Les documents du SCRS en question sont des produits du SCRS destinés à diffuser des renseignements à un lectorat du gouvernement afin qu'il puisse les utiliser dans sa propre analyse et éclairer la prise de décisions, propres à son ministère. Les documents varient de renseignements uniques à des produits analytiques complets basés sur de multiples flux de rapports, tant nationaux qu'étrangers. Un point commun important entre les documents est qu'ils sont rédigés uniquement pour un lectorat qui possède l'attestation de sécurité appropriée pour accéder et utiliser les renseignements en question.

Les renseignements du SCRS ne sont pas classifiés et réservés à un lectorat restreint parce qu'ils sont des renseignements en soi ou parce qu'ils proviennent de sources classifiées. Plutôt, une cote de sécurité et une distribution restreinte sont mises en place puisque que la divulgation des renseignements exposera une source humaine ou technique, une méthodologie, une enquête ou une lacune dans l'enquête à des adversaires ou qu'elle nuira aux relations internationales. Ceci est particulièrement le cas des renseignements concernant les activités constituant des menaces de la part des gouvernements étrangers qui disposent de ressources considérables pour mener des opérations de contre-espionnage.

Les renseignements concernant de multiples aspects des activités d'ingérence étrangère et d'influence malveillante de la République populaire de Chine (RPC) sont de la plus haute importance pour le gouvernement du Canada en raison de l'ampleur et de l'impact de cette menace. Ces activités comportent des menaces immédiates ou des préjudices graves aux intérêts stratégiques du Canada. Il s'agit d'activités sur lesquelles le gouvernement doit être pleinement informé afin de prendre des décisions politiques ou opérationnelles immédiates et efficaces. Ces activités portent sur les questions qui revêtent la plus grande importance pour les intérêts canadiens, qui sont les plus susceptibles d'avoir une incidence négative ou positive sur les intérêts canadiens et qui nécessitent le plus une compréhension basée sur des renseignements canadiens distincts.

L'ingérence étrangère

La menace d'ingérence étrangère dans nos processus démocratiques émane de la RPC et d'autres pays. La divulgation publique des renseignements du Canada, en particulier au moment où ces produits sont rédigés, risque d'exposer les sources du SCRS et la compréhension que le Canada a ou non des activités de menace. À cela s'ajoute l'effet de mosaïque, en vertu duquel un adversaire suit et rassemble un grand nombre de renseignements individuels, possiblement disparates, souvent sur de longues périodes, à partir de sources multiples, et acquiert ainsi la capacité de reconstituer un portrait de nos connaissances. Il n'est pas toujours possible d'identifier un élément

précis dans un seul document et d'expliquer pourquoi sa divulgation serait préjudiciable en soi, mais lorsqu'il est combiné avec d'autres renseignements rendus publics, ou ceux qui ont été obtenus par l'espionnage et le vol de données, les adversaires peuvent être en mesure de tirer des inférences et des conclusions concernant les enquêtes du SCRS. L'information qui est dévoilée par l'effet de mosaïque et qui présente un grand intérêt pour les services de renseignement étrangers qui sont actifs au Canada comprend les intérêts en matière d'enquête, les lacunes en matière de renseignement, les méthodes d'opération, les procédures administratives, les employés, les partenariats étrangers, l'emplacement des sources techniques et l'identité des contacts occasionnels du SCRS et des sources humaines.

Les acteurs étatiques étrangers qui se livrent à des activités d'ingérence étrangère ont d'importantes capacités d'agréger des « mégadonnées » et d'utiliser l'information de géolocalisation et l'intelligence artificielle pour rassembler des informations provenant d'une variété de produits ou de flux de rapports différents qui ont été diffusés au fil des ans. Par exemple, les médias ont indiqué que la RPC avait déjà utilisé avec succès de telles capacités pour démanteler le réseau de sources humaines de l'Agence centrale de renseignement des États-Unis (« CIA »), ce qui a entraîné de graves conséquences, notamment l'emprisonnement et des dizaines de pertes de vie.[1]

L'annexe classifiée jointe à la présente lettre utilise un exemple précis tiré des documents sélectionnés pour expliquer les raisons pour lesquelles il serait préjudiciable à la sécurité nationale du Canada de divulguer ces renseignements information.

Il est également essentiel de noter que les enquêtes sur l'ingérence étrangère, comme l'ingérence étrangère elle-même, se poursuivent souvent sur des années ou des décennies. De nombreux points d'accès du renseignement canadien sur cette question prennent beaucoup de temps à développer et restent en place pendant de longues périodes. Bon nombre des enquêtes sur l'ingérence étrangère qui étaient en cours en 2019 et en 2021 demeurent des enquêtes actives aujourd'hui, ce qui signifie que leur exposition aura une incidence négative sur les enquêtes en cours. Particulièrement, les divulgations qui identifient les sources humaines ou permettent de déduire leur identité mettent en danger la sécurité des sources et celle de leurs proches.

La divulgation entraînerait également des conséquences négatives à long terme. Il est raisonnable de présumer que des représentants étrangers suivent le processus de cette Enquête de telle sorte qu'ils seront informés des divulgations de renseignements sensibles. Cela entraînera probablement une perte immédiate de l'accès aux renseignements que le Canada a jugé de la plus haute priorité. Il faudrait des années pour remplacer cet accès (s'il peut être remplacé). Enfin, une telle incapacité à protéger les sources humaines et les renseignements classifiés en général entraînerait probablement une diminution de la confiance dans le SCRS de la part d'autres personnes qui envisagent de fournir des renseignements au SCRS et à des organismes étrangers partenaires, ce qui pourrait entraîner une diminution des renseignements reçus.

Les ressources

Cet examen de la confidentialité relative à la sécurité nationale des documents sélectionnés a été effectué de façon accélérée. Pour respecter l'échéancier prévu, le gouvernement a détourné les

[1] *China Used Stolen Data to Expose CIA operatives in Africa and Europe*, foreignpolicy.com

experts sur le sujet des renseignements précis contenus dans les documents de leur rôle de collecte et d'analyse de renseignement afin qu'ils participent à cet examen. Il s'agit d'un écart par rapport à leur processus standard. Au total, le personnel a consacré plus de 200 heures-personnes à l'examen de ces 13 documents. Comme vous le savez, le gouvernement prend le processus d'examen au sérieux, car il peut entraîner des conséquences indirectes sur d'autres enquêtes et procédures, y compris des procédures judiciaires. En règle générale, le gouvernement relie toutes les déclarations faites dans les produits de renseignements aux renseignements bruts afin de valider, entre autres, l'exactitude du rapport et la méthode de collecte. Ce niveau d'examen n'est pas viable s'il est reproduit à long terme. Il est clair que le caviardage de documents à grande échelle ne sera pas une solution efficace compte tenu des délais impartis.

Autres options pour aller de l'avant

Le gouvernement du Canada reconnaît l'importance d'éduquer le public sur la menace de l'ingérence étrangère. Ce faisant, il est essentiel de protéger les renseignements qui seraient préjudiciables à la sécurité nationale s'ils étaient divulgués. Nous sommes déterminés à aider la Commission d'enquête à s'acquitter de son mandat. À cet égard, nous aimerions ouvrir un dialogue sur les options viables pour aider la commissaire à remplir son mandat. Une partie de ce dialogue nécessite une meilleure idée du type d'information que la Commission d'enquête souhaite rendre public, étant entendu qu'il existe des limites très pratiques quant aux renseignements classifiés qui peuvent être rendus publics. Dans cette optique, nous pensons que les options suivantes et/ou une combinaison de ces options contribueront à faire avancer ce processus. Ces options comprennent le caviardage d'un nombre limité de documents qui soit viable et proportionné, des résumés d'un nombre limité de documents ou de sujets (voir des exemples dans les pièces jointes classifiées) et/ou des audiences à huis clos menant à un résumé public.

Nous sommes à votre disposition pour vous rencontrer à votre convenance et nous souhaitons ouvrir ce dialogue dès que possible.

Cordialement,

Gregory Tzemenakis
Avocat-conseil

Barney Brucker
Avocat-conseil

p.j. 13 documents sélectionnés, caviardés (Non-classifiés)
13 documents sélectionnés, surlignés (Classifiés)
Annexe (Classifiée)
Guide de codage (Classifié)
3 résumés (Classifié)

NOTE : La Commission d'enquête a demandé la traduction de cette présente lettre seulement.