



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

L'honorable Marie-Josée Hogue,  
commissaire

**VOLUME 4** CHAPITRES 14-18

# La capacité du gouvernement à détecter, prévenir et contrer l'ingérence étrangère (faits et analyse 2/2)



Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux. Rapport final.  
Volume 4 : La capacité du gouvernement à détecter, prévenir et contrer l'ingérence étrangère (faits et analyse 2/2).  
© Sa Majesté le Roi du chef du Canada (2025).  
Tous droits réservés.

Toutes les demandes d'autorisation de reproduire ce document, en totalité ou en partie, doivent être adressées au Bureau du Conseil privé.

This publication is also available in English:  
*Volume 4: The Government's Capacity to Detect, Deter and Counter Foreign Interference (Facts and Analysis 2/2).*

CP32-169/2-2025F-4-PDF  
ISBN 978-0-660-75089-7

(Ensemble) CP32-169/2-2025F-PDF

### **Note concernant la traduction**

Plusieurs notes de bas de page du rapport contiennent des références aux transcriptions des audiences de la Commission. Ces notes de bas de page réfèrent à la pagination de la version bilingue des transcriptions (version « plancher » telle que prononcée) et non à la pagination de la version traduite en français.

Par ailleurs, aux fins du rapport, les citations originales anglaises tirées des transcriptions bilingues ont été traduites en français par la Commission. Les citations traduites dans le rapport peuvent être différentes des citations qu'on retrouve dans la version française des transcriptions.

Pour alléger le texte, nous avons évité d'identifier les citations traduites avec la mention « [traduction] ». Nous avons seulement utilisé des guillemets.

Finalement, il est possible que des notes de bas de page réfèrent uniquement à des documents rédigés en anglais. Cette situation s'explique habituellement par le fait qu'aucune version française de ces documents n'est accessible ou que la Commission n'a pas été en mesure de l'obtenir à temps pour le dépôt du rapport

## Table des matières

<b>CHAPITRE 14</b>	<b>Circulation du renseignement au sein du gouvernement</b>	<b>8</b>
14.1	Introduction	9
14.2	Un système centralisé de diffusion du renseignement	10
14.3	Le Centre de la sécurité des télécommunications (CST)	11
	La diffusion des produits de renseignement	12
	La circulation du renseignement vers le niveau ministériel	13
14.4	Le Service canadien du renseignement de sécurité (SCRS)	14
	La diffusion de produits de renseignement	15
	La circulation du renseignement au niveau ministériel	16
	La rétroaction sur les produits de renseignement	17
14.5	Affaires mondiales Canada (AMC)	17
	Diffusion des produits de renseignement	18
	Circulation du renseignement au niveau ministériel	18
14.6	La Gendarmerie royale du Canada (GRC)	20
	La diffusion des produits de renseignement	20
	L'initiative Une Vision	21
	La circulation du renseignement vers le niveau ministériel	22
14.7	Sécurité publique Canada	22
	La diffusion des produits de renseignement	23
	La transmission du renseignement au niveau ministériel	24
	Les modifications récentes apportées aux procédés utilisés pour transmettre du renseignement à Sécurité publique Canada	27
14.8	Le Bureau du Conseil privé (BCP)	28
	Secrétariat de l'évaluation du renseignement du BCP (SER du BCP)	28
	Le Secrétariat de la sécurité et du renseignement du BCP (S&R du BCP)	29
	Le poste de conseiller à la sécurité nationale et au renseignement auprès du premier ministre (CSNR)	30
	Le Secrétariat des institutions démocratiques du BCP (SID)	32
	Le greffier du Conseil privé (le greffier)	33
14.9	Le cabinet du premier ministre (CPM)	34
14.10	Le premier ministre	35
14.11	La responsabilité ministérielle	36
14.12	Les cas particuliers où des inquiétudes ont été soulevées	37
	Le Rapport spécial du BCP et le document sur le ciblage	37
	Le document sur le ciblage	41
	La motion sur les Ouïghours	46
	Le mandat du SCRS	55
14.13	Conclusion	64

<b>CHAPITRE 15 Communication d'informations aux parlementaires et aux partis politiques</b>	<b>65</b>
15.1 Introduction	66
15.2 Breffages non classifiés à l'intention des parlementaires	66
Breffages défensifs (breffages préventifs de sécurité)	67
Campagne de breffages préventifs de sécurité (BPS) en 2021	68
Breffages non classifiés à l'intention de tous les parlementaires	69
15.3 Prestation de breffages aux parlementaires dans le cadre de l'autorité du SCRS en matière de mesures de réduction de la menace	74
La directive ministérielle	75
Le breffage sur les mesures de réduction de la menace donné à Erin O'Toole et le discours à la Chambre des communes	76
Le Protocole de gouvernance	78
Considérations particulières pour fournir de l'information classifiée aux parlementaires	80
15.4 Une préoccupation concernant la communication d'information aux parlementaires : la cybercampagne du <i>Advanced Persistent Threat 31</i> qui ciblait les membres de l'Alliance interparlementaire sur la Chine	81
Courriels aux membres de l'Alliance interparlementaire sur la Chine en 2021	81
Détection de la campagne de courriels de l'APT 31 et mesures prises à l'encontre de celle-ci	82
Manière dont les parlementaires ont eu connaissance de la campagne de l'APT 31	84
Nature de la menace	85
Les parlementaires auraient-ils dû être avisés?	85
Qui a la responsabilité d'aviser les parlementaires d'une cybermenace?	86
15.5 Communication d'informations par le Bureau du Conseil privé	87
15.6 Communication d'informations par Affaires mondiales Canada	88
Désinformation ciblant M. Chong	88
Campagne de camouflage de pourriels	89
15.7 Informer les représentants des partis politiques durant une élection	90
Breffages classifiés aux représentants de parti détenant une cote de sécurité	90
Breffages non classifiés aux partis politiques	91
15.8 Breffages classifiés aux chefs de parti politique	91
Le rôle spécial des chefs de parti	91
Défis liés aux breffages aux chefs de parti	92
Offrir des autorisations de sécurité de niveau « Très secret » aux chefs de l'opposition	93
Breffages sur du renseignement précis au printemps de 2024	94
La difficulté des chefs d'opposition qui ne sont pas breffés	95

15.9	Communication d'informations par le Centre canadien pour la cybersécurité	96
15.10	L'effet du projet de loi C-70	96
15.11	Conclusion	97

---

## **CHAPITRE 16 La communication d'informations à l'extérieur du gouvernement fédéral**

		<b>98</b>
16.1	Introduction	99
16.2	Rapports avec d'autres gouvernements au Canada	99
	L'importance de la communication intergouvernementale	99
	Les défis du dialogue avec les autres gouvernements	100
	Les travaux réalisés à ce jour	102
16.3	Rapports avec le public	103
16.4	Conclusion	105

---

## **CHAPITRE 17 La répression transnationale**

		<b>106</b>
17.1	Introduction	107
17.2	La répression transnationale et le mandat de la Commission	108
17.3	Les acteurs de la répression transnationale et leurs tactiques	108
	L'Iran	109
	La République populaire de Chine	110
	L'Inde	111
17.4	La réponse du Canada à la répression transnationale	112
17.5	Des exemples d'activités de répression transnationale au Canada	114
	Les postes de police étrangers de la RPC	114
	L'assassinat de Hardeep Singh Nijjar	116
17.6	Conclusion	120

---

## **CHAPITRE 18 La motion de la Chambre des communes sur le rapport du CPSNR**

		<b>121</b>
18.1	Introduction	122
18.2	La motion de la Chambre des communes	124
18.3	L'enquête de la Commission	126
	Le mandat de la Commission	126
	Le processus de la Commission	127
18.4	Observations sur le renseignement	129
	La nature du renseignement	129
	La perte d'exactitude et de nuance lorsque le renseignement est résumé	129
	Les difficultés à évaluer le « caractère volontaire » des actes des parlementaires	130

18.5	Discussion sur les affirmations identifiées dans le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)	132
	Le « caractère volontaire » des actes des parlementaires	132
	Les erreurs relatives au renseignement lui-même	133
	Le renseignement est une mosaïque et une cible mouvante	134
	Des erreurs dans la description du renseignement	136
18.6	Le renseignement et le défi de l'équité procédurale	138
18.7	La réponse du gouvernement	141
18.8	Conclusions sur le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)	143
	L'ampleur du problème	143
	L'incidence du rapport du CPSNR	144
<hr/>		
	<b>Conclusions quant à la capacité du gouvernement à détecter, prévenir et contrer l'ingérence étrangère</b>	<b>145</b>
<hr/>		
	<b>ANNEXE A Glossaire</b>	<b>150</b>

## CHAPITRE 14

# Circulation du renseignement au sein du gouvernement

14.1	Introduction	9
14.2	Un système centralisé de diffusion du renseignement	10
14.3	Le Centre de la sécurité des télécommunications (CST)	11
14.4	Le Service canadien du renseignement de sécurité (SCRS)	14
14.5	Affaires mondiales Canada (AMC)	17
14.6	La Gendarmerie royale du Canada (GRC)	20
14.7	Sécurité publique Canada	22
14.8	Le Bureau du Conseil privé (BCP)	28
14.9	Le cabinet du premier ministre (CPM)	34
14.10	Le premier ministre	35
14.11	La responsabilité ministérielle	36
14.12	Les cas particuliers où des inquiétudes ont été soulevées	37
14.13	Conclusion	64

*Les informations peuvent être incomplètes : des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.*

## 14.1 Introduction

Conformément à la division C de mon mandat, j’ai examiné la manière dont le renseignement sur l’ingérence étrangère est créé, échangé, évalué et diffusé au sein du gouvernement fédéral. Dans ce chapitre, je résume ce que j’ai appris.

Pour être utile à la prise de décision gouvernementale, le renseignement doit être communiqué de façon appropriée. Les agences de renseignement ont différentes façons de procéder, mais l’objectif est le même : veiller à ce que le gouvernement ait accès au renseignement dont il a besoin pour planifier ses actions et ses décisions.

Pour plusieurs raisons, la communication du renseignement exige de faire preuve de jugement.

Tout d’abord, les producteurs de renseignement doivent protéger leurs sources et leurs méthodes. Cette protection s’accomplit par la mise en place de procédures qui veillent à ce que le renseignement soit distribué de manière réfléchie et sécurisée, et seulement aux personnes qui ont besoin de le connaître.

Ensuite, les producteurs canadiens de renseignement doivent faire preuve de discernement lorsqu’ils communiquent leurs produits aux échelons supérieurs du gouvernement parce qu’ils diffusent un volume colossal de renseignement. Des témoins m’ont affirmé que la communauté de la sécurité nationale et du renseignement génère environ 70 000 produits de renseignement par an. D’autres témoins ont décrit le flux d’informations qu’ils recevaient comme un « fleuve », aussi bien du point de vue du volume que de la portée. Michael MacDonald, ancien conseiller à la sécurité nationale et au renseignement auprès du premier ministre (le « **CSNR** ») par intérim et secrétaire adjoint du Cabinet (sécurité et renseignement) au Bureau du Conseil privé (le « **BCP** »), estime avoir reçu environ 25 000 à 28 000 produits de renseignement au cours des trois années qu’il a passées au BCP. Leur importance, leur crédibilité et leur intérêt variaient. Il est essentiel de trouver un juste équilibre entre la nécessité de partager du renseignement pertinent et celle d’éviter de submerger les destinataires avec trop d’information. Tel que je l’explique plus loin, il n’est pas nécessaire que tous les produits de renseignement soient transmis au premier ministre, aux ministres, aux sous-ministres ni même à d’autres hauts fonctionnaires au sein du gouvernement. J’y reviendrai dans mes recommandations.

Le volume considérable des informations, le rythme auquel elles sont collectées et traitées, les complications liées à la classification et le caractère sensible des opérations de renseignement signifient que communiquer efficacement des informations dans le domaine de la sécurité nationale constitue un défi de taille. Cependant, c'est un défi qui doit être relevé. Il faut que les bonnes personnes obtiennent les bonnes informations, au bon moment, et de la bonne manière, pour être en mesure de répondre efficacement aux enjeux de sécurité nationale.

J'ai entendu des témoignages portant sur un certain nombre de questions et de problèmes liés à la manière dont l'information a circulé, ou n'a pas circulé, vers les décideurs de haut rang au sein du gouvernement. Certains de ces problèmes ont également été examinés par d'autres organes de surveillance, tels que l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (l'« **OSSNR** ») et le Comité des parlementaires sur la sécurité nationale et le renseignement (le « **CPSNR** »). Certaines de ces questions ont également suscité une grande attention de la part du public.

Depuis, le gouvernement a pris un certain nombre de mesures pour améliorer ses procédures en matière de communication du renseignement.

Dans ce chapitre, je décris d'abord les processus généraux au moyen desquels les différents acteurs de l'appareil gouvernemental de sécurité nationale reçoivent et transmettent des informations.

J'aborde ensuite les problèmes précis de circulation de l'information qui ont retenu mon attention au cours des travaux de la Commission.

## 14.2 Un système centralisé de diffusion du renseignement

Vers la fin du printemps ou à l'été 2023, la communauté de la sécurité nationale et du renseignement, sous la direction du BCP, a entrepris de moderniser les méthodes de diffusion et de suivi du renseignement. L'objectif était de résoudre les problèmes auxquels le gouvernement faisait face lorsqu'il tentait d'assurer le suivi de certains éléments de renseignement, notamment pour retracer si, quand et comment un élément de renseignement avait été transmis à un haut fonctionnaire ou à un ministre.

Auparavant, certains organismes utilisaient SLINGSHOT, l'ancien système de base de données de diffusion et de suivi du renseignement du Centre de la sécurité des télécommunications (le « **CST** »), mais d'autres ne le faisaient pas. Le Service canadien du renseignement de sécurité (le « **SCRS** »), par exemple, communiquait ses produits en envoyant des courriels au moyen du Réseau canadien Très secret (le « **RCTS** »). Cela entraînait des difficultés à savoir qui avait vu quoi, à quel moment, et comment.

L'initiative de modernisation a débouché sur un nouveau système, utilisé depuis l'automne 2023, qui permet de diffuser du renseignement envoyé aux hauts fonctionnaires et d'en faire le suivi.

Le nouveau processus garantit que tous les rapports de renseignement formels produits par le SCRS, le CST, Affaires mondiales Canada (« **AMC** »), le Centre intégré d'évaluation du terrorisme et le Secrétariat de l'Évaluation du renseignement du BCP (le « **SER du BCP** ») sont diffusés et suivis par l'intermédiaire d'un système de base de données centralisé et mis à jour par le CST.

Ce système comporte des mécanismes intégrés qui permettent à l'agence ou au ministère qui téléverse un produit de renseignement de le signaler à un destinataire. La base de données permet également de savoir qui accède aux documents et de recueillir des commentaires relatifs à un produit. De plus, si quelqu'un imprime un document, la base de données du CST lui demande d'indiquer pour qui il l'imprime. L'impression par des individus est enregistrée et le système ajoute d'autres mesures de sécurité et de suivi.

Le renseignement à l'attention de décideurs très haut placés, tels que les ministres du Cabinet ou le premier ministre, leur est souvent transmis au moyen de breffages oraux, plutôt que de produits de renseignement écrits. Marie-Hélène Chayer, ancienne secrétaire adjointe par intérim au Secrétariat de la sécurité et du renseignement du BCP, a expliqué que son équipe a également essayé de mettre en œuvre des méthodes plus systématiques pour assurer le suivi des breffages oraux dans l'ensemble de la communauté du renseignement. Dorénavant, les agences consignent la date, les personnes présentes et les sujets abordés lors de chaque breffage. Selon elle, ce système de suivi fonctionne mieux, même s'il demeure toujours possible de l'améliorer.

### 14.3 Le Centre de la sécurité des télécommunications (CST)

Les rapports du CST sur le renseignement étranger, contrairement à ceux d'autres organismes gouvernementaux responsables de la sécurité et de l'application de la loi, sont uniquement des représentations factuelles de données de communications électroniques. Les principaux destinataires des rapports du CST au sein du gouvernement sont le SCRS, AMC, le BCP et, dans une moindre mesure, la Gendarmerie royale du Canada (la « **GRC** »). Étant donné que le CST ne peut cibler des Canadiennes et des Canadiens ou des personnes au Canada, ses rapports de renseignement étranger sont moins pertinents aux fins du mandat de la GRC. Pour cette raison, le CST fournit beaucoup moins d'informations à la GRC que le SCRS.

La diffusion des produits du CST est régie par l'*Ensemble des politiques relatives à la mission*<sup>1</sup>, qui impose des exigences strictes quant à la manière dont les produits du CST peuvent être communiqués. Le CST distribue du renseignement à la communauté de la sécurité nationale et du renseignement au moyen de « rapports de produit final » dans sa base de données centralisée. Lorsqu'ils détiennent un compte, les clients gouvernementaux peuvent accéder directement aux rapports que leur autorisation de sécurité et leurs endoctrinements leur permettent de consulter.

Comme cela sera expliqué plus loin, le CST transmet également du renseignement en format papier en le remettant en main propre à des personnes désignées, et le reprend généralement après qu'il a été lu.

Le mandat du CST est relatif à la collecte de renseignement étranger. Bien qu'il se concentre sur les communications d'étrangers hors du Canada, lorsqu'il recueille du renseignement étranger, il peut également, de manière fortuite, recueillir du renseignement concernant des Canadiennes ou des Canadiens. Lorsque cela se produit, le CST utilise l'expurgation afin de protéger la vie privée des Canadiennes et des Canadiens dans ses rapports de renseignement étranger. Les destinataires désignés de rapports de renseignement étranger qui ont le besoin de savoir doivent demander les identités dans le cadre d'une procédure particulière, justifier la raison pour laquelle ils les demandent et démontrer qu'ils sont légalement habilités à les obtenir. Le CST, conformément à la *Loi sur le Centre de la sécurité des télécommunications*, détermine ensuite s'il y a lieu de permettre l'accès et identifie dans sa base de données centrale les personnes qui les ont reçus.

## La diffusion des produits de renseignement

Le CST est responsable de deux éléments clés de la diffusion du renseignement au sein du gouvernement.

Comme je l'ai expliqué précédemment dans ce chapitre, le CST gère la base de données centrale actuellement utilisée par la communauté de la sécurité nationale et du renseignement pour communiquer des rapports. Le CST décide qui parmi le personnel du gouvernement peut avoir accès au renseignement contenu dans la base de données à la lumière des politiques d'échange de renseignement et du besoin de savoir de chaque individu.

Le CST est également responsable du système d'agents des relations avec la clientèle (les « **ARC** »). Ces derniers sont employés par le CST et sont en poste dans d'autres ministères. Ils sont généralement responsables de

---

<sup>1</sup> La *Loi sur le Centre de la sécurité des télécommunications* prévoit les actes que peut poser le CST en vertu de la loi. L'*Ensemble des politiques relatives à la mission* est le document qui énonce la manière dont le CST exercera ses pouvoirs.

communiquer du renseignement à leurs clients, à savoir les hauts fonctionnaires et les cabinets ministériels.

Les ARC sélectionnent les rapports qui correspondent aux besoins de leurs clients et les signalent en indiquant « à montrer » dans la base de données du renseignement. Au fil du temps, ils développent une connaissance des besoins de leurs clients. Ceux-ci peuvent aussi demander aux ARC des breffages ponctuels sur des sujets précis. Les ARC remettent généralement le renseignement à leurs clients sur papier ou par d'autres moyens sécurisés. Ils restent en leur présence pendant qu'ils le lisent. Les ARC consignent les produits que leurs clients ont lus et recueillent leurs commentaires.

J'ai entendu des témoignages indiquant que le réseau des ARC ne suffit pas toujours à la tâche. La demande pour les services des ARC est élevée, mais l'offre pour répondre aux besoins de la communauté de la sécurité nationale et du renseignement est limitée en raison de leur nombre défini. Alia Tayyeb, cheffe adjointe du Secteur du renseignement électromagnétique au CST, a indiqué que le CST cherche activement des solutions pour accroître la capacité des ARC à répondre aux besoins des clients gouvernementaux.

## La circulation du renseignement vers le niveau ministériel

Le CST relève du ministre de la Défense nationale. Le chef du CST ou son délégué décide du renseignement à communiquer au ministre de la Défense nationale. En temps normal, le CST a recours aux ARC pour transmettre ses rapports, de même que ceux qu'il reçoit de ses partenaires, au cabinet du ministre. Le chef du CST donne également des breffages oraux au ministre de la Défense nationale sur des rapports pertinents du CST au cours de réunions planifiées ou ponctuelles. Si un rapport nécessite l'attention urgente du ministre, le chef du CST peut prendre des mesures pour alerter le cabinet du ministre par téléphone ou par courriel.

Le ministre de la Défense nationale à l'heure actuelle, Bill Blair, a expliqué qu'il recevait deux à trois breffages par semaine du CST, en plus de breffages ponctuels au besoin. Il a ajouté que la tenue des dossiers au sein du CST était rigoureuse : tous les produits de renseignement sont datés et il appose sa signature pour indiquer les rapports de renseignement qu'il a reçus et lus.

## 14.4 Le Service canadien du renseignement de sécurité (SCRS)

Le SCRS produit une quantité importante de renseignement. En 2022, il a produit plus de 2 500 évaluations et rapports sur les menaces, notamment sur l'ingérence étrangère. Le renseignement du SCRS est transmis à d'autres ministères à des fins d'information, et pour être utilisé dans leurs analyses et leurs breffages à l'intention du personnel de direction. Le renseignement est également partagé avec les autres ministères afin de contribuer à leur prise de décision et leur élaboration de politiques.

Le SCRS communique un large éventail de produits à l'ensemble du gouvernement. Il peut s'agir de renseignement brut<sup>2</sup>, qui vient enrichir l'ensemble des informations sur un sujet, ou d'évaluations du renseignement, qui analysent plusieurs éléments de renseignement à un niveau plus stratégique. Le SCRS transmet également des rapports, des notes de breffage et des notes de service ministérielles. Le SCRS peut créer ces produits de son propre chef ou en réponse à une demande d'un ministère, ou encore à l'intention d'un comité interministériel précis (voir le chapitre 11, volume 3).

En plus de communiquer des produits de renseignement écrits, le SCRS donne des breffages oraux aux ministres, aux sous-ministres, aux fonctionnaires du BCP et au cabinet du premier ministre (le « **CPM** »). Il les rencontre, ainsi que le personnel de leurs bureaux, à leur demande. Régulièrement, le SCRS fournit aussi des conseils lors de la préparation de mémoires au Cabinet et des discussions qui auront lieu au sein du Cabinet.

Lorsque le SCRS communique du renseignement, les noms des citoyennes et citoyens canadiens sont souvent supprimés ou « masqués ». Cela se produit lorsque le SCRS transmet des informations recueillies dans le cadre de son mandat d'assistance en matière de renseignement étranger, prévu à l'article 16 de la *Loi sur le Service canadien du renseignement de sécurité*. Le SCRS peut également masquer des identités pour d'autres raisons, notamment la nature sensible des sources. Le SCRS m'a indiqué que cette pratique est conforme au fait qu'il se concentre sur les acteurs menaçants eux-mêmes, et non sur les individus qui font l'objet d'activité menaçante.

Le masquage des identités peut parfois empêcher un client de comprendre la pertinence et l'incidence d'un rapport. Si un destinataire estime que les noms sont nécessaires pour comprendre le contexte d'un rapport, il peut demander au SCRS de ne pas masquer les identités. Ce faisant, il doit indiquer qui fait la demande et en quoi le démasquage d'un nom en particulier soutiendrait ses activités. Le SCRS prend ensuite une décision.

---

<sup>2</sup> Le renseignement brut est l'information que recueille une agence de renseignement qui n'a pas encore fait l'objet d'évaluation ni d'analyse.

## La diffusion de produits de renseignement

Le directeur adjoint des exigences du SCRS décide s'il y a lieu de communiquer du renseignement et quel produit convient le mieux selon la situation, en fonction de plusieurs facteurs.

L'un de ces facteurs est la fiabilité de la source. Les témoins du SCRS ont déclaré que le SCRS communique autant d'informations que possible sur son évaluation de la source des informations. Cette évaluation peut évoluer au fil du temps. La fiabilité des sources est un élément très important à prendre en considération lors du partage et de l'interprétation du renseignement.

D'après ce que j'ai vu, le SCRS s'appuie fortement sur des mises en garde et des formules génériques pour communiquer la fiabilité des sources. Je ne considère pas que cette façon de faire est suffisante. Je reviendrai sur cette question lorsque je ferai mes recommandations.

Une unité spéciale relevant du directeur adjoint des exigences du SCRS est responsable de la diffusion des produits de renseignement du SCRS. Cette unité dispose d'une liste de personnes désignées auprès de chaque client gouvernemental, qui sont les principaux contacts du SCRS. Ces personnes sont chargées de recevoir les produits de renseignement du SCRS au nom de leur organisation, puis de les diffuser au sein de celle-ci conformément à son mandat, ses priorités et ses préoccupations.

Certains produits de renseignement contiennent des informations particulièrement sensibles. Dans ce cas, le SCRS utilise une liste de diffusion restreinte de destinataires désignés. Il est bien sûr nécessaire et approprié de restreindre la diffusion de renseignements hautement sensibles.

Toutefois, la diffusion limitée du renseignement en raison de son caractère sensible peut avoir pour effet d'empêcher l'information de se rendre à ceux qui ont besoin de la connaître et qui peuvent être en mesure d'agir en réponse à cette information. Pour donner un exemple concret, j'ai entendu un témoignage portant sur une situation où le SCRS a communiqué un produit de renseignement à AMC en 2021 concernant les activités de Zhao Wei, un diplomate de la République populaire de Chine (la « **RPC** »). Le SCRS a restreint la distribution de ce produit à un analyste junior et un ARC, qui eux-mêmes étaient limités dans leur droit de le partager au sein d'AMC. Par conséquent, les officiers supérieurs du renseignement d'AMC n'avaient pas connaissance de ce produit et ne l'ont pas pris en compte avant de produire une évaluation des activités de M. Zhao le 2 mai 2023. Je reviens sur ce point au chapitre 11 (volume 3).

Le SCRS peut signaler les rapports qui doivent être portés à l'attention des hauts fonctionnaires de chaque ministère, soit pour qu'ils prennent une mesure, soit pour donner lieu à une discussion stratégique, en les désignant précisément comme destinataires. Le SCRS décide des éléments de renseignement à signaler aux échelons supérieurs en fonction de son évaluation de l'importance et des répercussions du rapport de renseignement en question.

Jusqu'à l'automne 2023, le SCRS envoyait tous les produits de renseignement à ses clients gouvernementaux par courriel sur le Réseau canadien Très secret (RCTS), ce qui ne lui permettait pas de faire un suivi précis de la réception de ces produits. Comme je l'ai mentionné plus haut, le SCRS utilise désormais le système de base de données centralisé du CST pour transmettre des informations. Cela permet au SCRS de contrôler la diffusion du renseignement en toute sécurité et de savoir qui a accès aux rapports.

Le SCRS fait encore appel à des ARC pour communiquer du renseignement aux ministres personnellement. Il dispose maintenant également d'un agent de liaison en poste à Sécurité publique Canada, ce qui a amélioré sa capacité à communiquer et à assurer le suivi du renseignement.

## La circulation du renseignement au niveau ministériel

Le SCRS relève directement du ministre de la Sécurité publique. Il rencontre régulièrement le ministre et son cabinet afin de les informer des développements en matière de sécurité nationale et relativement à l'activité opérationnelle du SCRS, et aussi pour signaler les enjeux émergents. Le SCRS transmet également au ministre d'importants produits de renseignement par l'intermédiaire de Sécurité publique Canada.

Un type de document produit par le SCRS est appelé note de gestion d'enjeu (une « **NGE** »<sup>3</sup>). Les NGE sont utilisées pour alerter le ministre de la Sécurité publique et les hauts fonctionnaires lorsque le SCRS s'apprête à prendre des mesures particulières. Le SCRS envoie des NGE lorsqu'une action prévue est délicate sur le plan politique ou risque de devenir publique. Le SCRS m'a indiqué qu'il envoyait environ trois NGE par semaine. Le SCRS a eu recours à ces produits pour informer le ministre de la Sécurité publique de problèmes à venir afin qu'il ne soit pas pris de court.

Il semble que le SCRS et ses clients n'aient pas compris les NGE de la même manière. Les informations contenues dans les NGE ne sont pas toujours parvenues au ministre et les hauts fonctionnaires de Sécurité publique Canada auxquels elles étaient destinées n'ont pas toujours considéré les NGE comme étant des produits de renseignement particulièrement importants parmi ceux partagés par le SCRS.

Le SCRS m'a dit que les problèmes dans la manière dont les informations circulaient étaient particulièrement marqués pendant la pandémie de COVID-19. L'ancien directeur du SCRS, David Vigneault, m'a expliqué que, si le personnel du SCRS, de manière générale, devait continuer à travailler dans ses bureaux (bien que parfois avec un personnel réduit afin de respecter les directives de santé publique), de nombreux destinataires de ses produits étaient en télétravail (et ne pouvaient donc pas accéder à des moyens de

---

<sup>3</sup> Pour « note de l'unité de gestion d'enjeu ».

communication sécurisés). Par conséquent, il est arrivé à quelques reprises que des produits ne soient pas transmis aux bonnes personnes, ni lus par elles, puisqu'elles n'étaient pas sur les lieux de travail.

## La rétroaction sur les produits de renseignement

Les témoins du SCRS m'ont dit qu'il était parfois difficile pour le SCRS d'obtenir des retours de la part de ses clients gouvernementaux.

Toutefois, j'ai également obtenu de la preuve quant à l'existence d'échanges utiles entre le SCRS et ses clients à propos de renseignement. Par exemple, Katie Telford, cheffe de cabinet du premier ministre, a expliqué que le CPM fournit fréquemment des commentaires sur le renseignement ou demande aux agences de renseignement des informations complémentaires sur des éléments de renseignement particuliers, surtout lorsque le renseignement qu'il reçoit pourrait avoir une incidence sur la carrière d'une personne.

J'ai également entendu que les clients peuvent faire des commentaires sur les produits de renseignement par l'intermédiaire de la nouvelle base de données centralisée du CST, et qu'ils le font. Le SCRS m'a dit que cette rétroaction était importante, car elle lui permet d'orienter sa collecte et ses rapports futurs, et lui donne une idée des types d'informations que les destinataires veulent.

Je comprends également que, pour élaborer les priorités du Canada en matière de renseignement, le BCP a mis en place un processus de rétroaction entre les agences de renseignement et leurs clients habituels.

La rétroaction est essentielle et doit être encouragée à tous les niveaux, régulièrement et fréquemment. Les commentaires reçus doivent être communiqués aux personnes chargées de confectionner les rapports de renseignement. Cela leur permettra de s'assurer que les futurs produits répondent mieux aux besoins des destinataires du renseignement.

### 14.5 Affaires mondiales Canada (AMC)

La Direction générale du renseignement d'AMC prépare chaque semaine des cartables pour le ministre des Affaires étrangères et son personnel politique, ainsi que pour le sous-ministre des Affaires étrangères. Ces cartables contiennent du renseignement brut et évalué, qui est jugé comme le plus pertinent. AMC maintient un registre des produits diffusés dans ses cartables, mais n'est pas en mesure de confirmer si les destinataires ont lu leur contenu.

## Diffusion des produits de renseignement

Les évaluations de renseignement étranger produites par la Direction générale du renseignement d'AMC sont diffusées à l'échelle du gouvernement à l'aide de la base de données sécurisée du CST, et elles sont communiquées à des pays alliés par l'intermédiaire d'agents de liaison du renseignement.

La direction générale du renseignement diffuse ses évaluations et ses autres produits de renseignement aux hauts fonctionnaires d'AMC par l'intermédiaire d'agents de relations avec la clientèle (ARC).

Si la Direction générale du renseignement estime qu'un produit est particulièrement important, elle le signale auprès des hauts fonctionnaires de manière ponctuelle ou dans le cartable hebdomadaire, et l'envoie par l'entremise d'un ARC pour s'assurer qu'il soit lu.

Entre 2016 et 2020, en raison de l'évolution des priorités et du fait que l'ingérence étrangère prenait de plus en plus d'importance, une section consacrée à l'ingérence étrangère a été ajoutée aux cartables d'AMC.

La Direction générale du renseignement organise des breffages oraux pour les hauts fonctionnaires, au niveau des sous-ministres adjoints et au-delà, de sa propre initiative ou sur demande. Philippe Lafortune, directeur général de cette Direction, a expliqué que ces breffages ont lieu au moins une fois par semaine.

## Circulation du renseignement au niveau ministériel

La Direction générale du renseignement entretient des liens directs avec le cabinet du ministre des Affaires étrangères.

Dans sa lettre de mandat de décembre 2021, le premier ministre a demandé à la ministre des Affaires étrangères, Mélanie Joly, de répondre à l'ingérence étrangère par des mesures internationales collectives.

La preuve présentée à la Commission concernant le niveau d'exposition de la ministre Joly à des informations sur l'ingérence étrangère avant 2023 manquait de clarté.

La ministre Joly a déclaré qu'elle avait véritablement commencé à considérer l'ingérence étrangère comme un élément pertinent dans l'élaboration de politiques lorsqu'elle travaillait sur la Stratégie pour l'Indo-Pacifique. Elle a indiqué que la Stratégie a notamment été élaborée afin de traiter des répercussions importantes des activités d'ingérence étrangère de la République populaire de Chine (RPC). La Stratégie pour l'Indo-Pacifique a été rendue publique en novembre 2022.

Lors d'une entrevue avec les avocats de la Commission, de même qu'à l'occasion de son témoignage public, la ministre Joly a déclaré qu'elle avait

seulement commencé à recevoir du renseignement sur l'ingérence étrangère au Canada, y compris des breffages et les produits du SCRS, à compter du printemps 2023. Dans son résumé d'entrevue, elle a indiqué que cela avait commencé en mars 2023. Lors de son témoignage aux audiences publiques, elle a plutôt indiqué que cela avait commencé au début du mois de mai, à la suite de la publication d'articles dans les médias sur le ciblage dont aurait fait l'objet le député Michael Chong.

À ce moment, elle a conclu qu'elle n'avait pas reçu de renseignement sur l'ingérence étrangère auparavant, ce qu'elle estimait problématique. En réaction à ce constat, la ministre Joly a créé le poste de directeur de la sécurité nationale au sein de son cabinet afin de s'assurer qu'elle obtiendrait ce renseignement. Cette mesure a permis de résoudre le problème. La ministre Joly participe désormais à des breffages portant sur du renseignement à toutes les deux semaines, lesquels touchent à un large éventail de sujets. Elle reçoit également des breffages ponctuels en cas d'urgence ou en préparation à des événements à venir. Lors de l'été 2023, elle a reçu deux ou trois breffages faisant état du contexte de la menace.

Le dossier de la Commission ne contient aucune preuve indiquant que la ministre Joly a reçu des breffages précis sur des événements d'ingérence étrangère avant mai 2023. Cependant, certains éléments de la preuve documentaire obtenue au cours de l'enquête de la Commission tendent à démontrer que la ministre Joly a néanmoins été au fait d'informations portant sur l'ingérence étrangère avant mai 2023 dans le cadre de son travail ministériel. Cela inclut notamment de l'information utilisée au soutien de demandes d'assistance en matière de renseignement étranger prévues à l'article 16 de la *Loi sur le SCRS*, ainsi que de l'information en lien avec la Stratégie Indo-Pacifique et le mémoire au Cabinet sur les activités hostiles parrainées par des États, qui a été présenté au Cabinet en mai 2022. Le dossier de la Commission inclut également des notes préparatoires relatives à la comparution de la ministre Joly devant le Comité permanent de la procédure et des affaires de la Chambre des communes en décembre 2022, au cours de laquelle elle a discuté de l'ingérence étrangère.

Le portrait de ce que la ministre Joly savait (ou ne savait pas) sur l'ingérence étrangère avant mai 2023 me paraît toujours incertain. Toutefois, deux choses sont claires.

Premièrement, il est clair que la ministre Joly a eu connaissance du sujet de l'ingérence étrangère avant le printemps 2023. D'ailleurs, cela n'a rien de surprenant, étant donné le lien étroit qui existe entre l'ingérence étrangère et le travail que doit exécuter la ministre des Affaires étrangères du Canada. Au contraire, il aurait été surprenant qu'aucune information sur l'ingérence étrangère n'ait été portée à son attention dans le cadre de ses fonctions.

Deuxièmement, que les premiers breffages sur le renseignement relatif à l'ingérence étrangère aient eu lieu en mars 2023 ou en mai 2023, il demeure qu'ils auraient dû avoir lieu bien plus tôt au cours de son mandat à titre de ministre des Affaires étrangères. Être au fait de certaines informations au

sujet de l'ingérence étrangère est une chose, mais recevoir des breffages de renseignement à ce sujet en est une autre. Lorsqu'un État se livre à de l'ingérence étrangère dans les institutions et processus démocratiques du Canada, cela peut être pertinent afin d'élaborer la politique du Canada à son égard. En tant que responsable des relations du Canada avec les États étrangers, la ministre des Affaires étrangères aurait dû recevoir du renseignement sur ces activités afin de nourrir ses réflexions et ses actions.

Il semble que, depuis mai 2023, des mesures importantes ont été prises par AMC et par la ministre pour s'assurer que davantage de renseignement lié à l'ingérence étrangère lui soit transmis en temps opportun. Les efforts en ce sens doivent se poursuivre afin de garantir que cette ministre et les futurs ministres des Affaires étrangères continuent à protéger correctement les intérêts canadiens sur la scène internationale.

## 14.6 La Gendarmerie royale du Canada (GRC)

Les unités au sein du programme de police fédérale et de sécurité nationale de la GRC consultent et utilisent tous les rapports disponibles pour générer des évaluations et des produits de renseignement en matière criminelle. Ces produits de renseignement issus de diverses sources visent à informer les hauts dirigeants et leur permettre de prendre des décisions éclairées. Les hauts fonctionnaires au sein du programme de police fédérale sont les principaux clients des produits de la GRC qui incluent des informations provenant des agences de renseignement. Toutefois, lorsqu'il est approprié de les diffuser plus largement, des versions de ces produits peuvent être préparées pour d'autres unités au sein de la GRC, pour le gouvernement ou pour des partenaires du Groupe des cinq (les États-Unis, le Royaume-Uni, l'Australie, la Nouvelle-Zélande).

### La diffusion des produits de renseignement

La GRC communique ses rapports et mises à jour à divers ministères, organismes, hauts fonctionnaires et ministres, et leur donne des breffages sur un large éventail de sujets, y compris sur les menaces pesant sur la sécurité nationale.

La GRC a recours à des listes de diffusion et choisit un système de diffusion adapté en fonction du niveau de classification du produit. Cela s'applique tant à la transmission interne au sein de la GRC qu'au partage externe avec d'autres ministères ou organismes gouvernementaux. Les produits classifiés au niveau « Secret » ou « Très secret » sont transmis à l'interne par l'entremise

soit du RCTS, soit de l'environnement classifié de la GRC. À l'externe, ces produits sont partagés au moyen du RCTS.

En ce qui a trait à l'échange d'information interne, la GRC a tenté de concilier le besoin des enquêteurs d'accéder aux informations classifiées avec le principe du « besoin de savoir », bien que cela soit difficile à réaliser. Afin de limiter l'accès à certains dossiers contenant des informations sensibles, la GRC utilise une « liste de contrôle d'accès ». Très peu d'unités de la GRC ont un accès illimité aux dossiers à accès restreint. Si un enquêteur ou un analyste a besoin de consulter un dossier à accès restreint auquel il n'a pas accès, il peut en faire la demande. Les témoins de la GRC ont reconnu que ces limites au partage d'informations au sein de la GRC pourraient être perçues comme une entrave à certaines enquêtes liées à l'ingérence étrangère, qui se fondent souvent sur du renseignement sensible qui peut être pertinent pour plusieurs enquêtes différentes. Cependant, les témoins ont également affirmé que certains systèmes sont mis en place pour atténuer ce risque, tout en veillant à ce que les éléments classifiés restent protégés.

La GRC a également des équipes intégrées et entretient des relations avec les services de police locaux pour assurer un échange d'informations. Ces équipes intégrées se trouvent dans d'importants centres urbains et comprennent des représentants des autorités policières locales. Dans les communautés plus reculées, l'ingérence étrangère peut ne pas immédiatement être reconnue, et l'information circule moins rapidement. Cet échange d'informations est crucial dans les enquêtes sur l'ingérence étrangère, puisque les services de police locaux sont souvent les premiers à y faire face.

La GRC travaille en étroite collaboration avec d'autres ministères et organismes gouvernementaux dans le cadre de la coordination d'interventions multiservices, notamment en cas d'ingérence étrangère. Cette collaboration implique notamment la participation hebdomadaire à de nombreux comités aux niveaux des sous-ministres, des sous-ministres adjoints et des directeurs, tant au niveau tactique que stratégique, afin de coordonner et prioriser les réponses entre les différents départements du gouvernement et éviter qu'elles entrent en conflit.

## L'initiative Une Vision

L'initiative Une Vision régit l'échange de renseignement entre le SCRS et la GRC. Elle a été lancée en 2012 pour assurer une coordination efficace entre les deux organisations et éviter les conflits dans leurs réponses respectives aux menaces à la sécurité publique, compte tenu du chevauchement de leurs mandats qui visent à protéger le Canada. L'initiative a été modifiée à plusieurs reprises. Au moment de rédiger ce rapport, Une Vision 3.0 est la version opérationnelle.

Dans le cadre de l'initiative Une Vision, le renseignement est échangé au moyen de réunions ou de « lettres d'utilisation ». Ces lettres représentent la méthode officielle par laquelle le SCRS transmet du renseignement à la GRC. Les informations peuvent être assorties d'une mise en garde et préciser si elles peuvent être utilisées, ainsi que la manière dont elles peuvent l'être. Dans certains cas, le renseignement est communiqué à la GRC uniquement pour l'informer d'une situation.

Une lettre d'utilisation n'est pas nécessairement transmise pour chaque réunion officielle, mais c'est fréquemment le cas. En moyenne, les deux organisations se rencontrent au moins une fois par semaine à l'occasion de réunions de gestion stratégique des dossiers.

De manière informelle, le directeur du SCRS échange également des informations avec le commissaire de la GRC lors des réunions hebdomadaires de comités des sous-ministres. Ces rencontres de comités ont pour but de discuter de la nature des menaces et de déterminer les réponses adéquates en fonction des mandats respectifs des organisations.

## La circulation du renseignement vers le niveau ministériel

La GRC relève du ministre de la Sécurité publique et peut lui fournir, au besoin, des rapports ou des breffages sur des informations classifiées ou sensibles. Cependant, la relation entre la GRC et le ministre est encadrée par le principe d'indépendance de la police. Selon ce principe, la police doit être libre de toute orientation ou influence de l'exécutif lorsqu'elle exerce ses pouvoirs de police ou prend des décisions liées à l'application de la loi et à l'enquête de cas individuels.

### 14.7 Sécurité publique Canada

Comme je l'ai expliqué au chapitre 11 (volume 3), le portefeuille de la Sécurité publique comprend cinq organismes : le SCRS, la GRC, l'Agence des services frontaliers du Canada, le Service correctionnel du Canada et la Commission des libérations conditionnelles du Canada. Chacun de ces organismes a un dirigeant (par exemple, le directeur du SCRS ou le commissaire de la GRC), dont le rang est équivalent à celui du sous-ministre de la Sécurité publique. Ces organismes relèvent du ministre de la Sécurité publique, et non du sous-ministre.

Le rôle principal de Sécurité publique Canada est de fournir à son ministre des conseils et des orientations en matière de stratégies et de politiques qui tiennent compte des mandats et des missions des organismes du portefeuille du ministère. Le ministère est séparé des organismes de son portefeuille et

est segmenté en fonction des politiques, incluant la sécurité nationale, la gestion des urgences et l'application de la loi.

Sécurité publique Canada est un consommateur de renseignement et non un producteur. Étant donné l'ampleur de son mandat ainsi que celui du ministre de la Sécurité publique, la quantité de renseignement que le ministère reçoit est considérable. C'est pourquoi je mentionne à nouveau qu'il ne semble ni nécessaire ni souhaitable de porter tous les éléments de renseignement à l'attention du ministre. Un tri devrait être effectué de façon à ce qu'il ne reçoive que le renseignement qu'il doit connaître, et qu'il ne connaît pas déjà.

## La diffusion des produits de renseignement

La façon dont le renseignement est fourni à Sécurité publique Canada, diffusé à l'interne et transmis au ministre a changé durant les travaux de la Commission. Je décris ces changements ci-dessous.

### **La Direction générale des opérations de sécurité nationale (DGOSN)**

La Direction générale des opérations de sécurité nationale (la « **DGOSN** ») est l'unité de Sécurité publique Canada principalement chargée de recevoir le renseignement et de le diffuser aux hauts fonctionnaires du ministère.

La DGOSN n'analyse pas le renseignement qu'elle reçoit et diffuse, mais assume plutôt une fonction de triage. Elle transmet aux hauts fonctionnaires le renseignement qui est particulièrement sensible ou orienté vers l'action, en fonction de leurs besoins et de l'évolution des priorités face aux événements internationaux ou nationaux qui se produisent.

Chaque jour, la DGOSN examine ses dossiers pour repérer le renseignement urgent qui doit être communiqué en temps utile aux destinataires désignés. Chaque semaine, elle compile le renseignement courant et pertinent qu'elle reçoit dans des trousseaux qu'elle transmet aux destinataires. De plus, ponctuellement et sur demande, la DGOSN fournit des rapports de renseignement particuliers aux hauts fonctionnaires pour appuyer les breffages classifiés destinés au ministre de la Sécurité publique.

Le renseignement reçu par Sécurité publique Canada porte non seulement sur l'ingérence étrangère, mais également sur plusieurs autres sujets tels les autres activités hostiles d'acteurs étatiques, les menaces à la sécurité économique, les événements mondiaux, les évaluations de situations géopolitiques et économiques, l'extrémisme violent, etc.

## La transmission du renseignement aux hauts fonctionnaires de Sécurité publique Canada : 2019-2022

J'ai entendu le témoignage de Rob Stewart, ancien sous-ministre de Sécurité publique Canada, et de Dominic Rochon, ancien sous-ministre adjoint principal du Secteur de la sécurité nationale et de la cybersécurité de Sécurité publique Canada (dont relève la DGOSN), au sujet de la circulation du renseignement pendant leurs mandats, c'est-à-dire de la toute fin de 2019 à octobre 2022<sup>4</sup>.

M. Rochon a déclaré que M. Stewart et lui-même recevaient les produits de renseignement principalement par deux moyens.

D'abord, la DGOSN préparait, à tous les quelques jours, un cartable à l'intention des hauts fonctionnaires. Un cartable moyen contenait entre 12 et 30 rapports, selon l'estimation de M. Rochon. La DGOSN ne disposait pas d'un système de suivi formel permettant d'identifier les produits transmis aux hauts fonctionnaires ou ceux qu'ils avaient lus.

L'autre moyen était le recours à des agents des relations avec la clientèle (ARC) toutes les deux semaines.

## La transmission du renseignement au niveau ministériel

Le ministre de la Sécurité publique reçoit du renseignement directement du SCRS et des autres agences de son portefeuille, ainsi que de Sécurité publique Canada.

### Avant la pandémie

J'ai entendu des témoignages sur la façon dont Sécurité publique Canada fournissait du renseignement au ministre avant la pandémie.

Les fonctionnaires du ministère étaient responsables de transmettre le renseignement marqué à l'attention du ministre. Le cabinet du ministre ne possédant pas de terminal pour accéder au RCTS, la DGOSN lui envoyait une copie papier du renseignement qu'elle recevait au bureau du ministre à Ottawa. La DGOSN ne filtrait pas les produits marqués à l'attention du ministre, c'est-à-dire qu'elle ne faisait pas de tri dans ce qu'elle envoyait. L'ensemble du renseignement destiné au ministre était censé lui être communiqué. M. Stewart a décrit la fonction de la DGOSN dans ces circonstances comme étant « la salle du courrier ».

---

<sup>4</sup> M. Rob Stewart a été nommé sous-ministre à Sécurité publique Canada le 17 décembre 2019. Il a occupé cette fonction jusqu'au 21 octobre 2022, date à laquelle il a été nommé sous-ministre du Commerce international. M. Dominic Rochon a occupé le poste de sous-ministre adjoint principal, Secteur de la sécurité nationale et de la cybersécurité, du 19 octobre 2019 au 31 octobre 2022. Au moment de la rédaction de ce rapport, il était dirigeant principal de l'information du gouvernement du Canada.

Sécurité publique Canada était également chargée de fournir au ministre un sous-ensemble de produits choisis, sélectionnés à partir du « fleuve » de renseignement reçu par le ministère. La sélection était généralement effectuée par le personnel du bureau de M. Rochon.

La DGOSN préparait aussi hebdomadairement un cartable à l'attention du ministre. Le personnel de Sécurité publique Canada ne signalait aucun élément de renseignement particulier dans ce cartable. Ce cartable était remis au cabinet du ministre par un agent de liaison ministériel, un employé du ministère affecté au cabinet et responsable de veiller à ce que Sécurité publique Canada soutienne le cabinet du ministre, notamment en s'assurant que les documents classifiés lui soient transmis.

Sécurité publique Canada n'effectuait pas le suivi après que ces informations avaient été communiquées au cabinet du ministre. Le personnel du ministère comptait sur le SCRS pour porter les questions importantes à l'attention du ministre, car ce dernier avait une relation indépendante avec le SCRS.

### **Pendant la pandémie**

Les témoins ont des souvenirs différents sur la manière dont le renseignement était communiqué au ministre Blair pendant la pandémie.

M. Stewart et M. Rochon ont déclaré que Sécurité publique Canada avait continué à produire des cartables de renseignement, qui étaient remis au ministre au bureau régional du SCRS à Toronto ou apportés à son domicile à Toronto. Cette pratique a été interrompue pendant les élections de 2021, alors que la transmission d'informations au ministre a été limitée aux questions urgentes.

Selon M. Stewart, la pandémie n'a pas eu de répercussions très importantes sur la façon dont le renseignement a circulé. Le personnel du SCRS a continué de travailler en personne tout au long de la période, et M. Stewart estime qu'il recevait un flux continu de renseignement.

Toutefois, M. Stewart se rappelle qu'au plus fort de la pandémie, notamment au printemps 2021, la quasi-totalité du personnel de Sécurité publique Canada travaillait à distance. Deux personnes étaient en poste au bureau de la DGOSN chaque jour. M. Stewart ne se souvenait pas du nombre de personnes que la DGOSN aurait normalement comptées au bureau, mais il a estimé ce nombre à « quelques centaines ». Au lieu de cela, il n'y avait parfois que M. Rochon et son chef de cabinet. Pourtant, M. Stewart m'a indiqué que les ressources étaient suffisantes pour décider ce qu'il fallait imprimer, l'imprimer et le verser dans un cartable.

Zita Astravas, cheffe de cabinet du ministre Blair à l'époque, a de son côté affirmé que les cartables hebdomadaires n'étaient plus produits pendant la pandémie. Elle a déclaré qu'elle ne recevait qu'un sous-ensemble plus restreint d'éléments de renseignement, moins fréquemment qu'une fois par semaine et pas sous forme de cartable. On lui avait dit qu'il n'était plus

possible de produire des cartables et que le personnel responsable de les constituer avait été réaffecté. M<sup>me</sup> Astravas se souvient avoir dit à Marco Mendicino, lorsqu'il est entré en fonction à titre de ministre de la Sécurité publique après les élections de 2021, que le cabinet du ministre avait l'habitude de recevoir un cartable de renseignement et qu'il devrait demander que cette pratique soit reprise.

M. Blair et M<sup>me</sup> Astravas ont déclaré que le renseignement sur papier a pratiquement cessé de circuler pendant la pandémie, sauf à l'occasion, lorsque le SCRS demandait que des lectures ponctuelles aient lieu. Celles-ci s'effectuaient dans une installation sécurisée. Lorsque les fonctionnaires du SCRS voulaient que M. Blair lise un produit particulier, ils demandaient à M<sup>me</sup> Astravas et à M. Blair de se rendre dans une installation sécurisée, où ils leur donnaient un breffage. Selon M. Blair, aucun renseignement ne lui a été remis à son domicile pendant la pandémie, car le programme des ARC ne lui remettait plus de renseignement.

Comme mentionné plus haut, M. Mendicino est entré en fonction à titre de ministre de la Sécurité publique peu après les élections de 2021. Il a témoigné se souvenir que M<sup>me</sup> Astravas l'avait encouragé à rétablir la pratique consistant à recevoir régulièrement des cartables de renseignement.

M. Mendicino a ajouté que pendant son mandat de ministre de la Sécurité publique (d'octobre 2021 à juillet 2023), son personnel et lui-même ont travaillé en étroite collaboration avec le sous-ministre (M. Stewart jusqu'en octobre 2022, puis Shawn Tupper), et qu'il avait un accès soutenu et fréquent au renseignement. Il recevait également des breffages, environ une fois par semaine et parfois plus fréquemment, de la part des organismes faisant partie de son portefeuille.

Il est clair que les souvenirs des uns et des autres diffèrent quant à savoir si les renseignements de routine ont été fournis au cabinet du ministre pendant la pandémie, et, si oui, de quelle façon. À mon avis, étant donné que très peu d'employés travaillaient en personne et que le ministre lui-même était à Toronto, il est possible que Sécurité publique Canada ait continué à imprimer et à fournir du renseignement au cabinet du ministre sans que cela ne soit fait de manière systématique comme c'était le cas avant la pandémie. C'est d'ailleurs ce qu'a déclaré M<sup>me</sup> Astravas : elle a continué à recevoir du renseignement, mais en moins grande quantité et moins souvent.

M. Mendicino a indirectement corroboré son témoignage à cet égard lorsqu'il s'est souvenu qu'elle lui avait suggéré qu'il devrait rétablir la pratique consistant à recevoir régulièrement des cartables de renseignement. Cependant, il est aussi possible que Sécurité publique Canada ait continué à envoyer des cartables de renseignement au cabinet du ministre, sans que ceux-ci ne parviennent, pour une raison quelconque, à M<sup>me</sup> Astravas. Quoi qu'il en soit, cette différence dans le souvenir qu'ont les uns et les autres démontre qu'il y a eu une importante rupture de communication durant cette période.

J'ai appris au cours des travaux de la Commission que transmettre des informations aux ministres par le biais de produits de renseignement écrits n'était pas un moyen particulièrement fiable. Cela étant, la preuve dont je dispose démontre que, souvent, lorsque quelque chose d'urgent devait être porté à l'attention du ministre, cela se faisait généralement à l'aide d'un breffage oral et non par l'envoi d'un produit de renseignement écrit.

Ainsi, la véritable question n'est pas tant de savoir si un rapport de renseignement s'est rendu au ministre, mais plutôt de savoir si les informations elles-mêmes lui ont été communiquées. La preuve à cet égard est convaincante et préoccupante : certaines informations ne lui ont pas été communiquées en temps opportun. Comprendre les raisons expliquant ces retards est toutefois difficile puisque personne n'a été en mesure de me l'expliquer clairement. Je souligne cependant que je n'ai pas de preuve démontrant que ce serait volontairement, dans un but illégitime, que l'information n'aurait pas été communiquée. Je n'ai pas non plus vu de preuve démontrant qu'en fait, les informations se seraient rendues au ministre, et qu'il aurait décidé de ne pas agir.

Je reviendrai sur la question de la transmission du renseignement aux décideurs de haut rang dans mes recommandations.

## Les modifications récentes apportées aux procédés utilisés pour transmettre du renseignement à Sécurité publique Canada

Comme je l'ai décrit précédemment dans ce chapitre, le Bureau du Conseil privé (BCP) a lancé une initiative pour uniformiser l'échange de renseignement au sein du gouvernement au printemps ou à l'été 2023. En conséquence, Sécurité publique Canada a modifié ses procédés à l'automne 2023.

Les hauts fonctionnaires de Sécurité publique Canada ne s'appuient plus autant qu'avant sur les cartables de renseignement. Au lieu de cela, un agent de liaison du SCRS affecté au ministère est chargé de trier et choisir le renseignement à l'intention des hauts fonctionnaires.

La création de ce poste d'agent de liaison a coïncidé avec le moment où la communauté de la sécurité nationale et du renseignement a migré vers la base de données centralisée du Centre de la sécurité des télécommunications (CST) sur le renseignement, dont j'ai discuté précédemment, qui permet de savoir qui a lu un produit de renseignement donné. L'agent de liaison du SCRS extrait les rapports de cette base de données et les transmet aux hauts fonctionnaires.

La présence de l'agent de liaison du SCRS permet à Sécurité publique Canada de savoir de manière constante qui a eu accès au renseignement.

Les témoins de Sécurité publique Canada m’ont affirmé que l’agent de liaison du SCRS connaît bien leurs centres d’intérêt et leurs besoins et qu’il comprend le contexte dans lequel le ministère opère. Ils considèrent que ce système est plus réactif que le précédent. Je ne peux pas dire si c’est le cas ou non, mais il faut surveiller de près le fonctionnement du nouveau système afin d’éviter que ne se répètent des problèmes tels que ceux survenus durant la pandémie.

En août 2023, Dominic LeBlanc est devenu ministre de la Sécurité publique. Entre ce moment et décembre 2024, date à laquelle il a quitté le portefeuille, lui et son personnel recevaient du renseignement du ministère par l’intermédiaire de l’agent de liaison du SCRS. Cela signifie que le renseignement que le ministre recevait et lisait faisait l’objet d’un suivi, ce qui me semble être une bonne pratique.

Le ministre recevait également du renseignement directement des organismes qui font partie du portefeuille de Sécurité publique Canada. M. LeBlanc m’a dit qu’il insistait pour que les dirigeants des organismes le contactent directement, à tout moment et pour toute situation urgente. Il recevait fréquemment des breffages oraux de la part des divers organismes. Il croit que les sujets abordés lors de ces breffages ont été consignés afin d’en garder la trace, bien qu’il ne puisse pas le confirmer.

## 14.8 Le Bureau du Conseil privé (BCP)

### Secrétariat de l’évaluation du renseignement du BCP (SER du BCP)

Le Secrétariat de l’évaluation du renseignement (SER du BCP) rassemble les évaluations du renseignement en provenance de toutes sources. Le premier ministre et son cabinet sont deux des principaux clients du SER du BCP, tout comme le sont le greffier du Conseil privé (le « **greffier** »), le conseiller à la sécurité nationale et au renseignement (CSNR), les ministres et les sous-ministres.

Le SER du BCP publie divers produits d’évaluation du renseignement, notamment le rapport quotidien de renseignement étranger (le « **rapport quotidien** »), qui est diffusé à grande échelle et présente trois ou quatre éléments de renseignement importants tirés du renseignement brut. Il publie également le rapport hebdomadaire de renseignement à l’intention du premier ministre (le « **rapport hebdomadaire** »), qui contient les faits saillants des rapports quotidiens ou encore du renseignement sur des événements à venir et des évaluations du renseignement national. Les rapports hebdomadaires peuvent être assez longs et font l’objet d’une évaluation par les pairs.

Nathalie Drouin, actuelle CSNR, a déclaré qu'elle travaillait avec le SER du BCP pour que les rapports quotidiens et hebdomadaires soient éventuellement abandonnés. Reposant sur des évaluations, ces rapports reprennent trop souvent des informations qu'elle a déjà transmises au premier ministre. D'ailleurs, il est possible qu'elle ne les lui communique pas lorsque le premier ministre a déjà vu les informations qu'ils contiennent. Cependant, lorsque le SER du BCP fournit un nouvel élément, elle l'intègre dans la trousse. Je traite du rôle du CSNR ci-dessous.

Le SER du BCP breffe aussi oralement le cabinet du premier ministre (CPM).

Tous les produits du SER du BCP destinés à être diffusés sont affichés, sur son site Web, sur le RCTS, et versés dans la base de données du CST. Aujourd'hui, le SER du BCP transmet le renseignement principalement par l'entremise du système du CST, car le suivi de la diffusion, du lectorat et de la rétroaction y est automatisé. Le SER utilise également un système « de poussées » (envoi de liens par courriel) à l'intention de certaines personnes désignées, en fonction du produit. Il répond aussi aux demandes d'informations de ses clients.

## Le Secrétariat de la sécurité et du renseignement du BCP (S&R du BCP)

Le Secrétariat de la sécurité et du renseignement du BCP (le « **S&R du BCP** ») reçoit des rapports produits par le SCRS, le CST et les partenaires du Groupe des cinq qui présentent des développements précis découlant du renseignement. Le renseignement reçu et signalé à l'intention des hauts fonctionnaires, y compris du personnel du premier ministre, est de nature opérationnelle ou tactique. Bridget Walshe, ancienne directrice des opérations au S&R du BCP, m'a dit qu'elle estime que le processus de partage de ce renseignement fait l'objet d'un suivi et est bien consigné.

La plupart des rapports reçus par le S&R du BCP sont diffusés au moyen d'outils électroniques, qui enregistrent automatiquement l'ouverture d'un document ou d'un rapport. Cependant, le CPM n'a pas accès au RCTS, de sorte qu'il a besoin de rapports imprimés avec une indication manuelle du lectorat.

Le S&R du BCP ne partage du renseignement avec le CPM que si une priorité opérationnelle ou une raison urgente le rend nécessaire. Le S&R du BCP n'est toutefois pas le principal mécanisme par lequel le CPM reçoit du renseignement.

## Le poste de conseiller à la sécurité nationale et au renseignement auprès du premier ministre (CSNR)

Jody Thomas, ancienne CSNR, a expliqué la manière dont elle recevait du renseignement lorsqu'elle occupait ce poste (de janvier 2022 à janvier 2024).

### La circulation du renseignement circule vers la CSNR

Premièrement, le SER du BCP lui fournissait chaque jour une trousse de renseignement pouvant comprendre jusqu'à 100 rapports. La trousse comprenait des informations sur des enjeux mondiaux importants qui l'intéressaient et qu'elle avait signalés, ainsi que des informations que des professionnels du renseignement estimaient qu'elle avait besoin de voir. Son personnel attirait son attention sur les rapports qui lui étaient expressément adressés.

Pour leur part, les produits de renseignement hautement classifiés à distribution restreinte lui étaient acheminés directement par un agent des relations avec la clientèle (ARC). Elle recevait quotidiennement des documents des ARC quotidiennement, voire plusieurs fois par jour. L'ARC restait sur place et l'observait pendant qu'elle lisait les documents, puis les emportait lorsqu'elle avait terminé. Ce renseignement concernait généralement des sujets déjà couverts par le SER du BCP. Les documents abordaient rarement des sujets dont elle n'avait pas déjà connaissance.

M<sup>me</sup> Thomas lisait sa trousse de renseignement chaque matin avant son breffage quotidien avec le greffier à 9 h. Si elle n'avait pas le temps de lire l'ensemble de la trousse, elle indiquait l'endroit où elle s'était arrêtée. Son personnel lisait alors le reste et lui signalait tout ce qu'il lui serait nécessaire de lire.

Comme d'autres sous-ministres, la CSNR recevait également du renseignement par le biais des comités de gouvernance interministériels (voir le chapitre 11, volume 3).

### La circulation du renseignement vers le premier ministre

La CSNR est la première responsable de déterminer ce que le premier ministre devrait voir, mais d'autres hauts fonctionnaires et d'autres membres du cabinet du premier ministre peuvent également porter des enjeux à son attention.

M<sup>me</sup> Thomas a indiqué que ce que le premier ministre avait besoin de voir changeait de jour en jour, selon les circonstances. Pour décider de ce qu'il devait voir, elle tenait compte de la pertinence et du caractère immédiat du renseignement, des événements à venir et du renseignement que le premier ministre connaissait déjà. Si elle voyait du renseignement exploitable dont le premier ministre devait être informé soit pour donner des instructions, soit pour comprendre les actions que le gouvernement prévoyait entreprendre, elle le lui signalait.

Un ARC remettait en main propre le renseignement destiné au premier ministre, selon des modalités typiquement convenues à l'avance avec son cabinet. M<sup>me</sup> Thomas s'assurait toujours que la greffière, la cheffe de cabinet du premier ministre et, généralement, le chef de cabinet adjoint reçoivent les mêmes produits. En moyenne, M<sup>me</sup> Thomas rencontrait le premier ministre au moins une fois par semaine.

Au cours du mandat de M<sup>me</sup> Thomas en tant que CSNR, le SER du BCP fournissait également au premier ministre et à son personnel des troupes d'évaluation du renseignement. M<sup>me</sup> Thomas ne participait pas à l'identification ni à l'approbation du contenu des troupes du SER du BCP. Le personnel du premier ministre assistait également à des breffages hebdomadaires avec le SER du BCP, ainsi qu'à des breffages fréquents de la CSNR et de la communauté du renseignement. Ces breffages portaient sur des enjeux dont, selon les membres de cette communauté, le premier ministre devait être informé.

Tant Nathalie Drouin, l'actuelle CSNR<sup>5</sup>, que M<sup>me</sup> Thomas sont d'avis que les troupes remises au premier ministre par le SER du BCP contiennent trop d'éléments. M<sup>me</sup> Thomas a indiqué que, lorsqu'elle identifiait un élément important, elle en soulignait les aspects les plus marquants pour que les hauts responsables du CPM les lisent.

M<sup>me</sup> Drouin a affirmé qu'elle essayait d'éviter que le renseignement soit transmis au premier ministre par différents canaux. Elle a expliqué que le processus par lequel le renseignement est partagé avec le CPM est de plus en plus systématique. Afin d'effectuer un meilleur suivi de ce qui se rend au premier ministre et à son cabinet, l'ensemble de l'information circule maintenant par l'entremise de la CSNR ou de son adjoint.

La CSNR détermine le contenu de la trousse de lecture hebdomadaire destinée au premier ministre. La CSNR et son adjoint déterminent quels produits de renseignement figurant dans leurs propres troupes de renseignement quotidiennes doivent être portés à l'attention du premier ministre, de son personnel et du greffier. Ils les remettent à un ARC.

Ces produits de renseignement sont ensuite intégrés à une trousse hebdomadaire de renseignement à l'intention du premier ministre et de son personnel. Le premier ministre lit cette trousse chaque semaine durant une plage horaire qui est réservée pour ce faire. Lorsqu'un ARC fournit du renseignement au premier ministre, il note toutes ses questions et les transmet à la CSNR et au CSNR adjoint. La CSNR ou le CSNR adjoint répondent aux interrogations du premier ministre en lui fournissant des informations soit de vive voix, soit par écrit (si la question est simple) dans la prochaine trousse de lecture qui lui est destinée. La CSNR et le CSNR adjoint fournissent également des breffages hebdomadaires au premier ministre et aux hauts responsables de son cabinet.

---

<sup>5</sup> Nathalie Drouin a été nommée CSNR en janvier 2024.

Cette procédure rationalisée permet à la CSNR de suivre le renseignement qui lui est transmis, de suivre ce qu'elle transmet au CPM et de savoir quelles personnes au sein du cabinet ont reçu ce renseignement. Le processus permet également de s'assurer que le premier ministre reçoit les informations pertinentes sans redondance.

M<sup>me</sup> Drouin a expliqué que décider quel renseignement aborder lors des breffages est un exercice difficile qui demande beaucoup de jugement, compte tenu de la grande quantité de renseignement reçu. Cette tâche représente un aspect fondamental du rôle du BCP, puisque, a dit M<sup>me</sup> Drouin, le temps des ministres et des sous-ministres est leur bien le plus précieux. M<sup>me</sup> Drouin et son équipe tiennent compte d'un certain nombre de facteurs, notamment de ce que le premier ministre s'apprête à faire, des actions à prévoir en réponse au renseignement, du fait que quelque chose dont il doit être informé est imminent, de la fiabilité du renseignement, de sa corroboration et de s'il s'agit de quelque chose que le premier ministre sait déjà.

Les directions du SCRS ou du CST signalent parfois un document à l'attention du premier ministre. M<sup>me</sup> Drouin a souligné que, parfois, la recommandation d'un organisme de transmettre du renseignement au premier ministre sera rendue désuète par la survenance d'autres événements ou parce que cela n'ajouterait pas à ses connaissances existantes puisqu'il a déjà été informé de la question. Si M<sup>me</sup> Drouin estime que lire un produit de renseignement signalé par un organisme ne constitue pas une bonne utilisation du temps du premier ministre, elle en discute généralement avec la personne qui a signalé le document en question et lui explique son raisonnement. Parfois, elle demande aussi que l'information lui soit fournie dans un format différent.

En théorie, si la direction du SCRS ou du CST et la CSNR ne parviennent pas à s'entendre sur l'envoi de renseignement au premier ministre, les dirigeants de ces organismes peuvent faire en sorte que la question se rende à leurs ministres respectifs ou au greffier. Ces ministres ou le greffier prendront alors la décision d'informer ou non le premier ministre.

Le premier ministre est en mesure de recevoir de l'information classifiée lorsqu'il voyage. M<sup>me</sup> Drouin voyage souvent avec lui et elle peut le breffer oralement lorsqu'il est en transit.

## Le Secrétariat des institutions démocratiques du BCP (SID)

Le Secrétariat des institutions démocratiques du BCP (le « **SID** ») ne fait pas partie de la communauté de la sécurité nationale et du renseignement. Allen Sutherland, secrétaire adjoint du Cabinet, a affirmé qu'il n'est pas un consommateur régulier de renseignement relatif à la sécurité nationale. Une grande partie de l'information que reçoit le SID provient de sources ouvertes. Le SID a néanmoins besoin de comprendre les tendances en matière de renseignement et le contexte de la menace pour mener à bien son travail d'élaboration des politiques. La majorité de son personnel possède

maintenant une autorisation de sécurité de niveau « Très secret ». Le SID reçoit régulièrement des évaluations du renseignement.

Le Secrétariat de la sécurité et du renseignement (S&R du BCP) sert d'intermédiaire entre le SID et les agences de sécurité nationale et de renseignement, car le S&R du BCP travaille directement avec ces agences sur le plan opérationnel. Des témoins du SID reçoivent également du renseignement en participant à des comités interdépartementaux comme le Comité des sous-ministres sur la gestion de l'intervention du renseignement, et ils participent à des réunions mensuelles avec le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (le « **Groupe de travail** ») (voir les chapitres 11 et 12, volume 3).

M. Sutherland a indiqué avoir accès aux informations dont il a besoin. Il ne veut pas nécessairement que des analystes de son équipe des politiques reçoivent du renseignement brut, car celui-ci pourrait les empêcher d'avoir une vue d'ensemble de la situation. Il préfère qu'ils effectuent leur travail à partir des meilleures évaluations possibles du renseignement. Il estime qu'il n'y a pas de lacune en matière d'information tant que le SID entretient des liens avec les agences de sécurité nationale et consulte ses homologues responsables des politiques. De son point de vue, il n'est pas nécessaire de mettre en place des mécanismes formels supplémentaires pour faciliter le partage de renseignement avec le SID.

## Le greffier du Conseil privé (le greffier)

Le greffier reçoit quotidiennement une trousse de renseignement provenant des agences de sécurité et de renseignement. Il peut aussi recevoir du renseignement supplémentaire directement de la direction de ces organismes. En tant que membre du Panel des cinq (voir le chapitre 12, volume 3), il reçoit également des informations sur le contexte de la menace de la part du Groupe de travail.

Janice Charette, qui a été greffière de mars 2021 à juin 2023<sup>6</sup>, a affirmé qu'elle recevait généralement une version épurée du renseignement que recevait M<sup>me</sup> Thomas. Des ARC lui fournissaient des informations sur une base hebdomadaire ou plus fréquemment, selon les besoins. Elle recevait également des breffages quotidiens et hebdomadaires produits par le Secrétariat de l'évaluation du renseignement du BCP (SER du BCP) et recevait un breffage oral de la part du SER du BCP chaque semaine.

M<sup>me</sup> Charette a indiqué que M<sup>me</sup> Thomas lui signalait parfois un élément de renseignement. Ensemble, elles décidaient ensuite si l'élément devrait être porté à l'attention du premier ministre. M<sup>me</sup> Charette pouvait également avoir d'autres informations, notamment sur des questions à venir ou sur les

---

<sup>6</sup> M<sup>me</sup> Janice Charette a également occupé le poste de greffière entre 2014 et 2016.

préoccupations du premier ministre, indiquant qu'un rapport précis devait être transmis au premier ministre. Selon elle, le premier ministre posait souvent des questions sur le renseignement reçu. M<sup>me</sup> Thomas et M<sup>me</sup> Charette répondaient à toutes ces questions avec le soutien de l'agence qui avait produit le renseignement.

M<sup>me</sup> Charette rencontrait le premier ministre généralement plusieurs fois par semaine.

## 14.9 Le cabinet du premier ministre (CPM)

Le cabinet du premier ministre s'appuie sur le BCP, et principalement sur le CSNR, pour sélectionner le renseignement et breffer son personnel.

Katie Telford, la cheffe de cabinet du premier ministre, a expliqué que la façon dont le renseignement circulait vers le CPM pendant la période visée par l'enquête de la Commission pouvait être divisée en quatre périodes clés : avant la pandémie, pendant la pandémie, après les élections de 2021 et après les reportages de 2023 portant sur l'ingérence étrangère.

Avant la pandémie, les hauts responsables du cabinet du premier ministre recevaient la majorité du renseignement sur papier. Le CPM recevait des troussees quotidiennes et hebdomadaires. Très peu de renseignement brut était communiqué. Dans les rares cas où du renseignement brut était soumis au personnel, un ARC le remettait généralement en main propre.

Pendant la pandémie, le CPM n'a pas reçu la même quantité de renseignement en format papier. Les troussees quotidiennes et hebdomadaires n'étaient plus diffusées. Lorsque le personnel du BCP ou les agences de sécurité estimaient que le CPM avait besoin de connaître un élément de renseignement, ils prenaient des dispositions particulières à cette fin. Dans certains cas, ils se rendaient au domicile de M<sup>me</sup> Telford ou encore lui demandaient de se rendre au bureau. Dans d'autres cas, le renseignement était reformulé pour atteindre un niveau de classification inférieur afin de pouvoir être transmis par voie électronique.

Après les élections de 2021, le système est devenu hybride. Pendant la pandémie, de nombreux hauts responsables ont eu accès à de la technologie leur permettant d'accéder à des documents de niveau « Secret », ce qui a facilité l'échange d'information. Cela s'est poursuivi après la pandémie. La communication de renseignement en format papier a aussi repris.

M<sup>me</sup> Telford a indiqué que le CPM a commencé à recevoir davantage de produits de renseignement brut au cours de cette période. Elle a attribué en partie ce phénomène à la CSNR de l'époque – chaque CSNR ayant son propre style et ses propres priorités – et en partie aux événements ayant cours dans le monde.

Après les fuites dans les médias en 2023, les protocoles d'échange de renseignement sont devenus beaucoup plus stricts. Désormais, le renseignement est transmis au cabinet du premier ministre par l'intermédiaire d'un ARC. L'ARC apporte à M<sup>me</sup> Telford une trousse d'information organisée et classée par ordre de priorité, et assure le suivi de chaque document qu'elle lit. L'ARC signale également les produits que le premier ministre a lus ou s'apprête à lire, ainsi que les commentaires qu'il a formulés sur le renseignement qu'il a lu. Même si le CPM dispose d'installations sécurisées pour conserver les documents, le renseignement ne reste pas sur les lieux. Ainsi, lorsque M<sup>me</sup> Telford n'arrive pas à tout lire en une séance, elle doit prendre rendez-vous avec l'ARC pour poursuivre sa lecture.

## 14.10 Le premier ministre

Le premier ministre reçoit généralement le lundi matin la trousse de lecture hebdomadaire préparée par le CSNR. Il consacre de 45 minutes à une heure à sa lecture. Cela lui donne une base générale de connaissances, dont certaines découlent d'informations hautement classifiées. Il demande parfois qu'un suivi soit fait sur une question particulière ou d'obtenir la confirmation que les informations ont été communiquées à d'autres personnes qui sont en mesure d'agir en conséquence. Lorsqu'il pose des questions précises à l'ARC, la réponse lui est généralement fournie lors de sa prochaine réunion avec le CSNR ou dans un document inclus dans sa prochaine trousse de lecture.

De plus, au moins une fois par semaine, le premier ministre rencontre des conseillers et des fonctionnaires pour discuter de certaines des questions les plus urgentes en matière de renseignement.

Le premier ministre a déclaré qu'il n'avait besoin que de voir les informations qui sont pertinentes pour son rôle. Selon lui, il s'agit de toute information qui a des répercussions immédiates sur les Canadiennes et les Canadiens ou qui les menace, qui est liée aux décisions que le gouvernement doit prendre en matière de politiques, ou qui est pertinente pour des interactions futures ou potentielles.

Selon le premier ministre, le système actuel répond bien à ses besoins. Il a souligné qu'il préférerait recevoir les informations de vive voix afin de pouvoir poser des questions et demander des précisions immédiatement à la CSNR et aux personnes qui sont responsables de la collecte et des opérations. Il a également besoin de prendre connaissance du renseignement qui est pertinent afin d'exercer son rôle de chef de parti.

Le premier ministre a déclaré qu'il fait confiance aux fonctionnaires de la communauté du renseignement et au CSNR pour décider ce qu'il devrait voir.

Ceux-ci discutent régulièrement du renseignement avec lui. Bien qu'il soit d'accord pour dire que le CSNR soit le premier responsable de déterminer ce qu'il doit voir, il ajoute lui aussi que d'autres personnes au sein de son cabinet ou des hauts fonctionnaires peuvent également attirer son attention sur certains sujets.

## 14.11 La responsabilité ministérielle

Comme je l'ai dit plus haut, ce n'est pas tout le renseignement qui doit être transmis au premier ministre. Le système de Westminster, en vigueur au Canada, prévoit que les ministres assument également des responsabilités. De plus, si un sous-ministre ou un dirigeant d'agence n'est pas d'accord avec la décision du CSNR de ne pas communiquer quelque chose au premier ministre, cette personne peut s'adresser directement à son ministre, qui est responsable envers le premier ministre de son propre ministère. Il est en mesure de discuter de la question à un plus haut niveau.

Je retiens de la preuve que des discussions sont en cours sur la manière dont les ministres exercent leurs responsabilités en matière d'ingérence étrangère.

Par exemple, le procès-verbal d'une réunion du Comité des sous-ministres sur l'ingérence étrangère du 20 avril 2023 indique que le rapporteur spécial indépendant s'interrogeait sur la responsabilité ministérielle. Ceci a conduit la CSNR à demander aux fonctionnaires du BCP de schématiser la façon dont le renseignement sur l'ingérence étrangère est diffusé aux ministres. Le procès-verbal indique que, même si le processus de gouvernance autour de l'ingérence étrangère semble bien fonctionner au niveau des sous-ministres et entre le premier ministre et son cabinet, la « lacune au niveau ministériel est préoccupante ».

Au printemps 2023, à la suite des fuites médiatiques portant sur l'ingérence étrangère en 2022 et 2023, le premier ministre a demandé aux services de renseignement de breffer quatre ministres (le ministre Blair, le ministre LeBlanc, la ministre Joly et l'ancien ministre Mendicino) sur le renseignement pertinent.

Des témoins m'ont dit qu'ils ont reconnu à ce moment que, si le premier ministre était breffé sur une grande partie de ces informations, d'autres ministres clés n'avaient pas reçu les informations en temps réel ou étaient demeurés, jusqu'à un certain point, dans l'ignorance quant aux allégations formulées dans les médias. La greffière a donc entrepris une série de rencontres afin que ces ministres soient mis au courant des informations qui avaient été transmises au premier ministre et qu'ils puissent discuter des mesures à prendre en réponse à celles-ci.

Bien qu'il s'agisse d'un exemple mineur, il peut illustrer un problème plus large de circulation du renseignement aux ministres. Je remarque cependant que le ministre LeBlanc m'a dit qu'à titre de ministre des Institutions démocratiques à l'époque, il n'aurait pas eu besoin de ce type d'information précise.

## 14.12 Les cas particuliers où des inquiétudes ont été soulevées

L'enquête de la Commission a mis en lumière quatre situations précises où le renseignement n'avait peut-être pas circulé adéquatement au sein du gouvernement. Ci-dessous, je passe en revue la preuve et présente mes constats sur ces incidents.

### Le Rapport spécial du BCP et le document sur le ciblage

Dans cette section, je me penche sur la diffusion de deux produits de renseignement au sein du gouvernement. L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) ont tous deux examiné ces documents et tiré certaines conclusions à leur sujet dans leurs rapports de 2024 sur l'ingérence étrangère.

Lorsque mes conclusions diffèrent des leurs, ce n'est pas une critique des constats qu'ils ont posés. Plutôt, ces différences sont probablement le résultat du dossier plus complet dont disposait la Commission et de mandats différents. La Commission a en effet eu plus de temps, plus de ressources et la possibilité de recueillir beaucoup plus de preuve que ces deux organismes de surveillance. Elle a également bénéficié du fruit de leurs efforts, ces rapports lui ayant été fort utiles.

Le document désormais connu sous le nom de « Rapport spécial du BCP » est un produit du Secrétariat de l'évaluation du renseignement du BCP (SER du BCP) portant sur l'ingérence étrangère de la RPC et préparé à la fin de 2021 et au début de 2022. Le document n'a jamais été finalisé. Ce Rapport spécial du BCP a été mentionné dans les médias au début de l'année 2023.

## L'origine du Rapport spécial du BCP

À l'automne 2021, David Morrison, alors conseiller intérimaire à la sécurité nationale et au renseignement auprès du premier ministre (CSNR)<sup>7</sup>, a demandé au SER du BCP, après avoir lu une évaluation du renseignement du SCRS sur l'ingérence étrangère de la RPC, de préparer un rapport.

M. Morrison a affirmé que l'évaluation du SCRS, à son avis, soulevait plus de questions que de réponses quant à l'ampleur et la portée du problème. Il voulait obtenir un produit qui lui donnerait une perspective globale sur l'ingérence étrangère de la RPC et qui l'aiderait à en évaluer la gravité.

M. Morrison a déclaré que le Rapport spécial du BCP lui était destiné. Il a souligné que même si « beaucoup a été dit par la suite, y compris par des organes de révision, quant à pourquoi ce document n'est pas parvenu à telle ou telle personne dans la sphère politique », son intention n'était pas celle-là lorsqu'il a commandé le Rapport spécial du BCP<sup>8</sup>.

Le SER du BCP a collaboré avec le SCRS pour produire ce rapport. Le SER l'a qualifié de « spécial » parce qu'une telle collaboration entre les deux organisations était relativement nouvelle et parce que le rapport combinait du renseignement d'origine nationale et étrangère. Cette pratique est devenue courante pour les produits du SER, mais elle était inhabituelle à l'époque.

En décembre 2021, le SER du BCP avait terminé une ébauche du rapport. La preuve démontre que M. Morrison a rencontré le SER le 16 décembre 2021 pour en discuter. Il a fait part de ses commentaires, notamment sur le ton, qu'il trouvait quelque peu hyperbolique, et a déclaré qu'il souhaitait recevoir une nouvelle ébauche. Il a également indiqué qu'il considérait que certaines des activités décrites étaient des activités diplomatiques légitimes et courantes.

M. Morrison a été nommé sous-ministre du Commerce international peu après la réunion de décembre 2021, et ainsi n'a plus été impliqué dans la préparation du Rapport spécial du BCP.

Il a depuis lu la deuxième version du Rapport spécial du BCP, en raison de la couverture médiatique de 2023 et des processus d'examen qui ont eu lieu par la suite. Selon lui, le rapport ne répond toujours pas à ses questions initiales sur l'ampleur, la portée et l'efficacité de l'ingérence étrangère menée par la RPC. Il ne pense pas qu'il aurait dû être transmis au premier ministre.

Le chef du SER du BCP à l'époque, Martin Green, a un souvenir différent quant à l'origine du Rapport spécial du BCP. Selon lui, c'est lui qui avait suggéré à M. Morrison que le SER du BCP produise un document englobant tout ce qui se passait au niveau international et national en lien avec l'ingérence

---

<sup>7</sup> M. David Morrison est actuellement sous-ministre des Affaires étrangères. Il a été conseiller à la politique étrangère et à la défense auprès du premier ministre de 2019 à 2022. À la fin du mois de juin 2021, il a également été nommé conseiller intérimaire du premier ministre à la sécurité nationale et au renseignement. Il a occupé cette fonction jusqu'en janvier 2022.

<sup>8</sup> Témoignage de David Morrison, 4 octobre 2024, Transcription, vol. 28, p. 101.

étrangère de la RPC. Il a compris que le Rapport spécial du BCP permettrait une discussion à un niveau élevé du gouvernement portant sur les opinions divergentes quant à ce qui constitue de l'ingérence étrangère et ce qui constitue une activité légitime d'influence étrangère.

### **La CSNR demande que le Rapport spécial du BCP fasse l'objet d'un examen de gouvernance**

Jody Thomas a succédé à M. Morrison en tant que CSNR le 11 janvier 2022. M. Green a parlé à M<sup>me</sup> Thomas de l'ébauche du Rapport spécial du BCP, lors d'une réunion qu'il a eue avec elle à la fin du mois de janvier 2022<sup>9</sup>. La lettre de M. Green à M<sup>me</sup> Thomas accompagnant le Rapport spécial du BCP indique que « [c]e rapport a été commandé par l'ancien CSNR intérimaire David Morrison afin de mieux comprendre l'ingérence étrangère de la Chine au Canada »<sup>10</sup>.

Cette lettre recommandait à M<sup>me</sup> Thomas de transmettre le rapport à certains sous-ministres et ministres, au Groupe de travail, à la greffière et à la sous-greffière du Conseil privé. M. Green a dit qu'il espérait que le rapport suscite des discussions à un niveau élevé et conduise à une orientation plus précise sur la question.

Lorsque M<sup>me</sup> Thomas a lu le Rapport spécial du BCP, elle l'a estimé utile, mais était d'avis qu'il ne contenait rien de particulièrement nouveau. Pour elle, il s'agissait plutôt d'un recueil d'informations sur l'ingérence étrangère de la RPC provenant de rapports antérieurs. Elle m'a dit avoir été préoccupée par le fait que certains termes utilisés étaient trop généraux et incendiaires, et qu'elle y décelait une tendance à l'exagération et à l'hyperbole plutôt qu'à s'en tenir aux faits. Elle estimait néanmoins que le rapport constituait une base utile pour des discussions liées aux politiques et a demandé qu'il soit soumis au processus « de gouvernance » habituel applicable aux produits de renseignement au sein du BCP.

M<sup>me</sup> Thomas a expliqué que la gouvernance est un élément essentiel du traitement du renseignement au sein du BCP et dans le monde du renseignement. Cela garantit que les produits de renseignement font l'objet d'un examen par les pairs avant qu'ils soient largement diffusés. Des comités existant au niveau des directeurs généraux et des sous-ministres adjoints examinent ainsi les documents avant qu'ils ne soient transmis à de hauts responsables comme les sous-ministres ou le premier ministre. M<sup>me</sup> Thomas a expliqué que ce processus d'examen par les pairs est essentiel pour garantir que la communauté de la sécurité nationale soit en accord avec l'évaluation et le renseignement sous-jacent. Or, diffuser le Rapport spécial

---

<sup>9</sup> M<sup>me</sup> Thomas a déclaré à la Commission que la réunion avait eu lieu le 27 janvier 2022, alors que d'autres éléments suggèrent qu'elle s'est tenue le 26 janvier 2022.

<sup>10</sup> Lettre d'accompagnement au rapport du SER sur les activités d'ingérence étrangère de la Chine, 20 janvier 2022, CAN011049\_0001.

du BCP comme le suggérait M. Green aurait contourné le processus normal de contrôle.

Lisa Ducharme, actuelle directrice des opérations au SER du BCP, a confirmé que si un produit est destiné aux sous-ministres ou au premier ministre, il doit d'abord faire l'objet d'une discussion au niveau des sous-ministres adjoints.

### **Le Rapport spécial du BCP ne fait pas l'objet d'un examen par la structure de gouvernance**

M<sup>me</sup> Thomas a expliqué que la discussion sur le Rapport spécial du BCP au sein du SER du BCP a été mise en suspens en raison d'événements importants survenus immédiatement après sa rencontre avec M. Green, soit l'arrivée du convoi de la liberté à Ottawa le 27 janvier 2022 et l'invasion de l'Ukraine par la Russie en février 2022. Ce n'est qu'au printemps 2022 que le rapport a fait l'objet d'une nouvelle discussion, avant l'envoi au Cabinet du mémoire au Cabinet portant sur les activités hostiles parrainées par des États en mai 2022.

M<sup>me</sup> Ducharme a déclaré qu'il n'est pas rare que des ébauches de rapport soient retardées ou demeurent inachevées. Cela se produit pour diverses raisons, notamment lorsque les ressources sont allouées ailleurs ou lorsqu'un changement d'orientation survient et fait en sorte que les ressources se concentrent sur d'autres événements. Elle a précisé que cela ne signifie pas que l'information qu'elles contiennent n'a pas été utile à ceux qui ont examiné les ébauches.

Puisque la CSNR n'approuve pas officiellement les produits du SER du BCP avant leur diffusion, M<sup>me</sup> Thomas ne pensait pas que le SER du BCP attendait son approbation pour diffuser le Rapport spécial du BCP. Le secrétaire adjoint du SER du BCP est celui qui est chargé de veiller à ce que les produits comme celui-ci soient dûment examinés par des pairs. M<sup>me</sup> Thomas a seulement appris que le rapport n'avait pas suivi le processus de gouvernance dans le cadre des examens du CPSNR et de l'OSSNR.

### **Le pouvoir du SER de diffuser le Rapport spécial du BCP**

M<sup>me</sup> Thomas a mentionné que le SER du BCP avait le pouvoir de diffuser le Rapport s'il le voulait. Le SER du BCP est indépendant de la CSNR et a le pouvoir de communiquer ses évaluations comme il le souhaite, ce qui garantit qu'il n'y a pas d'ingérence ou de perception d'ingérence, que ce soit sur le plan politique, bureaucratique ou des orientations en matière de politiques.

M. Green a déclaré qu'en raison du caractère délicat de la question, il ne se sentait pas à l'aise de partager le Rapport spécial du BCP davantage. Cependant, selon M<sup>me</sup> Thomas, le caractère sensible du renseignement ne change pas le processus de gouvernance. L'objectif de ce processus est de permettre à la communauté de la sécurité nationale et du renseignement, y compris les propriétaires du renseignement concerné, de se mettre d'accord sur la manière dont un produit a été élaboré et sur la manière dont il doit être diffusé.

## Le point de vue du premier ministre sur le Rapport spécial du BCP

Le premier ministre a maintenant lu le Rapport spécial du BCP. Il a affirmé que quoique certains détails soient nouveaux pour lui, son contenu général ne l'est pas. Le Rapport spécial du BCP n'ajoute rien qu'il ne savait déjà sur la façon dont la RPC se livre à des activités d'ingérence étrangère au Canada. Il a qualifié le Rapport spécial du BCP d'utile et d'une bonne compilation d'informations qui auraient été importantes pour quelqu'un qui venait d'entrer en fonction à titre de premier ministre.

Le premier ministre ne croit pas qu'examiner le Rapport spécial du BCP plus tôt aurait changé la réponse du gouvernement à l'ingérence étrangère. Les questions et l'information sur l'ingérence étrangère de la RPC compilées dans le Rapport n'étaient pas nouvelles. Selon lui, elles étaient connues du gouvernement et elles ont éclairé ses réponses sur le plan des politiques, comme la Stratégie de lutte contre les activités hostiles parrainées par des États, puis le projet de loi C-70, qui a été adopté sous le nom de *Loi sur la lutte contre l'ingérence étrangère*. Le chapitre 12 (volume 3) traite de ces deux initiatives.

## Le document sur le ciblage

Le document connu sous le nom de « document sur le ciblage » est un produit analytique du SCRS qui décrit la stratégie de la RPC visant à « cibler » des acteurs politiques canadiens pour mener des opérations d'influence. Les témoins du SCRS ont expliqué que, dans ce contexte, le terme « ciblage » signifie simplement que la RPC cherche à influencer quelqu'un. La « cible » n'est pas nécessairement au courant, complice ou menacée de quelque façon que ce soit. Le document sur le ciblage fait état de la façon dont la RPC classe les parlementaires en trois groupes :

- Ceux qui sont positifs à son égard.
- Ceux qui sont neutres et qui pourraient être convaincus d'être plus positifs à son égard.
- Ceux qui s'opposent à elle.

La Commission a eu accès au document sur le ciblage et a pu l'examiner dans son ensemble dans le cadre de son enquête.

## L'origine du document sur le ciblage

Le document sur le ciblage a été préparé par un analyste du SCRS en 2021, mais le SCRS n'a rendu ce document accessible que le 13 février 2023. Selon une réponse écrite fournie à l'OSSNR, le niveau de classification du rapport a rendu sa distribution difficile. L'auteur a continué de mettre de l'avant le document sur le ciblage, au sein du SCRS, lorsque les occasions se sont présentées, mais il n'a jamais été inscrit à l'ordre du jour du directeur.

Toutefois, à l'automne 2022, à la lumière de la discussion publique sur l'ingérence étrangère, l'auteur a obtenu les appuis nécessaires pour partager ce document sur le ciblage avec des personnes extérieures au SCRS et il a été mis à la disposition de certains fonctionnaires.

### **La CSNR examine le document sur le ciblage**

Jody Thomas, CSNR à l'époque, a reçu le document sur le ciblage dans sa trousse quotidienne de renseignement. Il a suscité chez elle des préoccupations.

Premièrement, la liste de diffusion était à la fois relativement longue et inexacte, certaines personnes y étant listées n'occupant plus certains postes. À une époque où le gouvernement faisait l'objet de fuites importantes d'information classifiée, M<sup>me</sup> Thomas était particulièrement préoccupée par la taille, l'inexactitude et le défaut d'actualisation de la liste de diffusion.

Deuxièmement, le document sur le ciblage incluait le nom des députés qui étaient « ciblés ». M<sup>me</sup> Thomas était préoccupée parce que cela allait à l'encontre de la pratique habituelle du SCRS de masquer les noms et survenait à un moment où il y avait d'importantes fuites d'information. Les noms étaient susceptibles d'être explosifs ou sensationnalistes s'ils faisaient l'objet d'une fuite. Janice Charette, greffière du Conseil privé à l'époque, a expliqué qu'il était important d'expurger les noms puisque l'objectif du document sur le ciblage était de révéler le comportement de l'acteur étatique hostile et non ses « cibles ». Dans le contexte des fuites dans les médias, il était particulièrement important de veiller à ce que les noms ne soient pas divulgués ni pris hors contexte.

Troisièmement, M<sup>me</sup> Thomas se demandait si le document sur le ciblage décrivait des activités d'ingérence ou des tentatives légitimes d'influence étrangère et elle voulait en discuter avec d'autres sous-ministres.

M<sup>me</sup> Thomas a donc demandé que la diffusion du document sur le ciblage soit temporairement interrompue.

### **Les sous-ministres examinent le document sur le ciblage**

Le document sur le ciblage a par la suite fait l'objet d'une discussion lors d'une réunion des sous-ministres le 24 février 2023. Le directeur du SCRS, la cheffe du Centre de la sécurité des télécommunications (CST), les sous-ministres des Affaires étrangères et de la Sécurité publique, la CSNR et la greffière y ont participé. Selon les témoins du BCP et du SCRS, les sous-ministres avaient les mêmes préoccupations que M<sup>me</sup> Thomas, notamment au sujet de la nature très sensible du produit. Ils ont convenu que la liste de diffusion devrait être réduite et que le SCRS devrait créer une version moins sensible, ne comportant pas certaines informations comme les noms des députés.

## Diffusion du document sur le ciblage expurgé

Il semble que les participants à cette rencontre de sous-ministres n'aient pas tous compris la même chose quant à la diffusion du document, certains croyant que la nouvelle version serait présentée au premier ministre.

Le SCRS est l'un de ceux qui semblent avoir compris que la version expurgée du document sur le ciblage était destinée au premier ministre. Il en a fait part à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et au Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) dans le cadre de leurs examens. Ces organes d'examen ont conclu que le document sur le ciblage devait être présenté au premier ministre, ce qui n'a pas été le cas. L'OSSNR a laissé entendre que c'était la CSNR qui avait décidé de ne pas le communiquer au premier ministre.

Ni l'OSSNR ni le CPSNR n'ont entendu M<sup>me</sup> Thomas, qui était la CSNR à l'époque, mais qui avait depuis pris sa retraite. La Commission a eu l'occasion de l'entendre.

M<sup>me</sup> Thomas et M<sup>me</sup> Charrette, qui étaient toutes deux présentes à la réunion du 24 février 2023, ont déclaré qu'elles n'ont jamais compris que le document sur le ciblage était destiné au premier ministre. De plus, M<sup>me</sup> Thomas a mentionné qu'elle n'avait jamais reçu du SCRS la version révisée de ce document.

La preuve révèle que l'analyste du SCRS avait préparé une version expurgée, mais que celle-ci n'a jamais été distribuée parce que la liste de diffusion n'a jamais été mise à jour. Il semble que la révision de la liste de diffusion soit passée entre les mailles du filet.

Le SCRS était chargé de fournir au CST une liste des destinataires pour que le document puisse être distribué par le biais du système du CST. Dans une réponse au CPSNR et à l'OSSNR, le SCRS a indiqué que, « en raison de priorités concurrentes qui se sont concrétisées au printemps et à l'été, le bureau du directeur n'a pas cru bon de soulever la question auprès du directeur »<sup>11</sup>. David Vigneault, alors directeur du SCRS, a seulement appris que le document révisé n'avait pas été distribué comme prévu dans le cadre des processus d'examen du CPSNR et de l'OSSNR.

M. Vigneault a déclaré à la Commission qu'il avait compris, à la lecture des rapports de l'OSSNR et du CPSNR, que M<sup>me</sup> Thomas avait pris la décision de ne pas communiquer le document au premier ministre parce qu'elle estimait que la conduite décrite relevait davantage de la diplomatie légitime que de l'ingérence étrangère. Il a toutefois indiqué ne pas en avoir eu personnellement connaissance, sa source d'information étant les rapports de l'OSSNR et du CPSNR.

---

<sup>11</sup> OSSNR, *Examen de la diffusion du renseignement ayant trait à l'ingérence politique étrangère exercée par la République populaire de Chine de 2018 à 2023* (Ottawa : 28 mai 2024), para. 129, COM0000365.

La preuve émanant du SCRS laisse entendre que la liste de diffusion révisée devait être créée par le bureau du directeur du SCRS et par la CSNR. Lorsqu'elle a été interrogée à ce sujet, M<sup>me</sup> Thomas a déclaré que la responsabilité de créer une nouvelle liste de diffusion incombait au SCRS, puisque c'est cette agence qui détient le renseignement.

Je retiens de la preuve que la CSNR n'a pas pris la décision de ne pas fournir le matériel au premier ministre. Elle n'a jamais reçu la version révisée et il semble que personne n'ait assuré de suivi.

À mon avis, la responsabilité de mettre à jour la liste de diffusion d'un produit du SCRS incomberait au SCRS. Bien que celui-ci ait été en mesure de solliciter l'avis de la CSNR, il lui incombait de soulever la question. Le bureau du directeur semble plutôt avoir perdu de vue qu'il était nécessaire de réviser la liste de diffusion.

Cela illustre la nécessité d'améliorer la communication et le suivi des projets de produits de renseignement, tant à l'interne au SCRS qu'entre les différents ministères.

### **Divergences de points de vue sur l'influence étrangère et l'ingérence étrangère**

Je constate aussi que les points de vue divergeaient sur l'importance du document sur le ciblage et, en particulier, sur la question de savoir si toutes les activités qui y étaient décrites, ou une partie de celles-ci, relevaient de l'ingérence étrangère ou d'une activité diplomatique légitime. De nombreux témoins ont déclaré qu'il est courant en diplomatie de dresser différentes listes de personnes impliquées dans le processus législatif en fonction de l'avis qu'elles ont à l'égard de certaines questions. Dresser ou posséder une liste de personnes impliquées dans le processus législatif ne constitue pas en soi de l'ingérence étrangère. Ce qui importe, ce sont les raisons pour lesquelles une telle liste est dressée et l'usage qui en sera fait, ce qui est très difficile à déterminer.

M<sup>me</sup> Thomas se souvenait d'avoir lu le document sur le ciblage et d'avoir été d'avis que le comportement qui y était décrit, soit de convaincre les parlementaires d'un pays de voter en faveur des intérêts d'un autre pays ou de modifier leur vote ou leur opinion sur une question, ne relevait pas nécessairement de l'ingérence étrangère. Elle a déclaré que les diplomates canadiens adoptent régulièrement un comportement semblable, et que le Canada doit faire preuve de prudence avant d'accuser des États d'ingérence étrangère lorsque lui-même fait des choses semblables dans d'autres pays. Autrement, le Canada pourrait mettre ses diplomates en danger.

M<sup>me</sup> Charette et John Hannaford, le greffier actuel, tous deux d'anciens ambassadeurs, ont exprimé leur accord. M<sup>me</sup> Charette se souvenait d'avoir obtenu des listes de personnes impliquées dans le processus législatif favorables et défavorables aux prises de position du Canada lorsqu'elle était Haute-commissaire au Royaume-Uni. David Morrison, sous-ministre des

Affaires étrangères, n'a pas non plus trouvé le document sur le ciblage alarmant, car le concept de listes de « cibles » est normal dans le monde de la diplomatie. Le problème n'est pas l'existence d'une telle liste, mais plutôt l'utilisation qui en est faite. Le document sur le ciblage, a-t-il fait remarquer, ne contenait pas d'informations voulant que des menaces pèsent sur des individus.

M<sup>me</sup> Thomas a indiqué dans son témoignage public que la communauté de la sécurité nationale et du renseignement se réunit fréquemment pour discuter des problèmes et des produits. Si un sous-ministre ou un chef d'agence n'est pas d'accord avec le point de vue collectif, il a à la fois la capacité et la responsabilité d'en parler à son ministre, qui, à son tour, doit rendre des comptes au premier ministre et est responsable de la direction des travaux de son ministère. Ainsi, s'il y avait eu un désaccord sérieux, le ministre de la Sécurité publique aurait dû en être informé (ce qui n'a pas été le cas).

Je souligne, et c'est là un point important, que la décision prise à l'issue de la rencontre des sous-ministres n'était pas de faire une croix sur le document sur le ciblage, malgré les différentes perspectives à son égard. Au contraire, la décision était de préparer une nouvelle version pour qu'il puisse être diffusé.

### **Que se serait-il passé si le document sur le ciblage avait été remis au premier ministre?**

Je conclus également que le document sur le ciblage n'aurait pas changé la réponse du gouvernement à l'ingérence étrangère s'il avait été remis au premier ministre en mars 2023.

Des témoins du SCRS, dont M. Vigneault, ont affirmé que si le document avait été remis au premier ministre, ce n'aurait été qu'à titre informatif, et non en vue d'une action particulière. En plus de transmettre le document aux hauts fonctionnaires, le SCRS avait l'intention d'utiliser une version non classifiée pour informer les députés.

Néanmoins, M. Vigneault estime que le premier ministre aurait dû recevoir le document sur le ciblage, car il s'agissait d'une analyse importante décrivant les activités de la RPC visant des représentants élus au Canada. Selon lui, si le premier ministre avait lu le document, celui-ci aurait pu lui être utile afin de déterminer comment la communauté de la sécurité nationale et du renseignement et le gouvernement devraient continuer d'évaluer les activités de la RPC. L'objectif était de susciter une discussion entre le SCRS, le premier ministre, le cabinet du premier ministre et la CSNR.

M<sup>me</sup> Charette a fait remarquer qu'au moment de sa publication en 2023, les informations contenues dans le document sur le ciblage étaient périmées depuis deux ans. M<sup>me</sup> Thomas a exprimé son accord, déclarant que la situation aurait pu être différente si le document sur le ciblage avait été porté à l'attention du CSNR en 2021, lors de sa préparation initiale.

Le premier ministre a reçu le document sur le ciblage dans le cadre des travaux de la Commission. Selon lui, ce document montre que les diplomates de la RPC recherchent des informations sur les députés et les catégorisent, ce qui n'est pas particulièrement révélateur et fait partie du travail des diplomates dans tous les pays du monde. Même si le document sur le ciblage contient quelques éléments intéressants, aucun d'entre eux ne modifie sa perception du comportement, de l'objectif ou de l'intervention de la RPC en matière d'influence et d'ingérence étrangères. Le document n'ajoute rien d'important à sa compréhension de la situation.

### Terminologie du ciblage

Finalement, au-delà des questions entourant sa diffusion, je conclus que le document sur le ciblage constitue un bon exemple d'un problème que j'ai remarqué dans plusieurs des rapports de renseignement que j'ai consultés, à savoir le défaut d'utiliser des termes clairs et précis. Ici, le mot « cible » est employé pour désigner une personne qu'un État étranger cherche à influencer (que ce soit de manière légitime ou illégitime). Le même mot, « cible », dans d'autres contextes, désigne une personne qu'un État étranger harcèle. « Cible », encore dans d'autres contextes, peut identifier une personne sur laquelle le SCRS mène une enquête.

Pour quiconque, mis à part les lecteurs les plus chevronnés de renseignement – et peut-être même pour eux –, cette situation suscitera de la confusion et des malentendus. La communauté du renseignement devrait faire des efforts afin de clarifier des termes comme ceux-ci et s'assurer que cela est communiqué aux lecteurs.

### La motion sur les Ouïghours

Le 22 février 2021, le député Michael Chong a présenté une motion à la Chambre des communes déclarant que les actions de la RPC à l'égard des Ouïghours et d'autres musulmans turciques du Xinjiang constituaient un génocide (la « **motion sur les Ouïghours** »). La Chambre des communes a adopté la motion sur les Ouïghours.

Dans la foulée, le Canada et la RPC ont imposé des sanctions ciblées de type « œil pour œil ». Comme je l'explique au chapitre 11 (volume 3), les sanctions ciblées interdisent aux personnes dans un pays et aux ressortissants de ce pays qui sont à l'étranger d'entretenir des relations commerciales et financières avec la personne ou l'entité sanctionnée. Elles peuvent aussi restreindre la capacité de la personne sanctionnée à se rendre dans le pays. Les sanctions peuvent viser des entités, des personnes et des membres de leurs familles.

Le 22 mars 2021, le Canada, les États-Unis, le Royaume-Uni et l'Union européenne ont imposé des sanctions à l'encontre de quatre responsables

de la RPC soupçonnés d'être impliqués dans la persécution des Ouïghours au Xinjiang.

Le 27 mars 2021, la RPC a réagi en imposant des sanctions à M. Chong et à tous les membres du Sous-comité des droits internationaux de la personne du Comité permanent des affaires étrangères et du développement international de la Chambre des communes.

Deux ans plus tard, le 1<sup>er</sup> mai 2023, le Globe and Mail a publié un article fondé sur du renseignement présumé du SCRS qui aurait fait l'objet d'une fuite, affirmant que M. Chong avait été la cible d'efforts d'ingérence étrangère de la part de la RPC en 2021. L'article suggérait qu'un agent du ministère de la Sécurité de l'État de la RPC avait cherché à obtenir des informations sur les proches d'un député canadien qui pouvaient vivre en RPC en vue d'autres sanctions potentielles.

M. Chong était au courant des sanctions prises par la RPC contre lui en réponse à son rôle de leader pour présenter la motion sur les Ouïghours en 2021. Cependant, jusqu'à la parution de l'article du Globe and Mail, il n'avait pas entendu qu'un diplomate travaillant au consulat de la RPC à Toronto avait été chargé de mener des recherches sur lui et ses proches à Hong Kong. Il s'est dit troublé par le fait que le renseignement n'ait donné lieu à aucune action pendant deux ans et qu'il n'en a pas été informé.

La Commission a examiné la façon dont l'information a circulé au sein du gouvernement depuis le moment où le SCRS a signalé pour la première fois le renseignement sur M. Chong en 2021 jusqu'au moment où le SCRS l'a breffé en mai 2023.

### **Comment le renseignement a-t-il circulé au sein du gouvernement**

Avant mai 2021, le SCRS a distribué à Bill Blair, alors ministre de la Sécurité publique, et à d'autres destinataires désignés, des produits de renseignement sur l'intérêt démontré par la RPC envers des députés, dont M. Chong et Kenny Chiu. La liste de diffusion de ces produits de renseignement comprenait : le BCP, dont le greffier (Ian Shugart) et le CSNR (Vincent Rigby), AMC (dont la sous-ministre Marta Morgan), le ministère de la Défense nationale (dont la sous-ministre Jody Thomas), le CST (dont sa cheffe Shelly Bruce) et Sécurité publique Canada (dont le sous-ministre Rob Stewart et le ministre Blair). Le SCRS a utilisé le Réseau canadien Très secret (RCTS) pour transmettre les produits par courriel aux destinataires désignés, ou aux contacts ministériels, pour qu'ils les distribuent aux destinataires nommément désignés.

Trois de ces produits font référence à M. Chong. La Commission a demandé au gouvernement de produire des versions caviardées de ces trois documents afin de pouvoir les divulguer au public. Le gouvernement a refusé de les produire pour des raisons de confidentialité liées à la sécurité nationale. En l'absence de versions publiques de ces trois produits de renseignement, les audiences de la Commission ont été marquées par une certaine confusion compréhensible au sujet de ces documents.

Par souci de clarté, je peux confirmer que ni le document sur le ciblage, ni le Rapport spécial du BCP, dont il a été question plus haut dans ce chapitre, ne figurent parmi ces trois produits. Chaque produit est plutôt un rapport de renseignement du SCRS.

Le renseignement disponible récolté à différents moments indique que :

- Certains députés, dont M. Chong et M. Chiu, suscitaient de l'intérêt de multiples acteurs menaçants de la RPC, dont le ministère de la Sécurité d'État (MSE).
- Un diplomate de la RPC menait des recherches sur un parlementaire supposé être M. Chong.
- Des fonctionnaires de la RPC cherchaient à mener des recherches sur certains députés ayant voté en faveur de la motion sur les Ouïghours, dont M. Chong, avec l'intention de leur imposer des sanctions.
- La RPC aurait cherché à obtenir des informations sur les proches de M. Chong en RPC et aurait voulu invoquer des sanctions à leur rencontre.

M. Blair a déclaré qu'il n'avait jamais reçu les trois produits de renseignement diffusés avant mai 2021 et faisant référence à M. Chong, ni aucun autre produit de renseignement diffusé via le RCTS. Ces produits de renseignement ont été diffusés pendant la pandémie alors qu'il ne recevait plus d'informations classifiées via le RCTS.

D'autres personnes ne se souviennent pas d'avoir reçu ou lu ces rapports à l'époque.

La sous-ministre Marta Morgan ne se souvient pas d'avoir lu ces rapports en particulier, mais elle a déclaré qu'AMC suivait de près la réponse qui émanerait de la RPC à la suite de la motion sur les Ouïghours.

Le sous-ministre Rob Stewart ne se souvenait pas avoir reçu les produits de renseignement, mais il était presque certain de les avoir reçus, étant donné la grande quantité de documents de ce type qu'il recevait de sous-ministre.

Ni David Morrison, conseiller de la politique étrangère et de la défense auprès du premier ministre à l'époque, ni Vincent Rigby, le CSNR de l'époque, ne se souviennent avoir vu ces produits de renseignement.

En réponse au renseignement, le SCRS a décidé de donner des breffages défensifs non classifiés (parfois appelés « breffages sur la sécurité préventive », voir le [chapitre 15](#)) aux députés Chong et Chiu afin de les sensibiliser aux menaces d'ingérence étrangère posées par la RPC.

Le SCRS a déterminé que le seuil justifiant de prendre une mesure de réduction de la menace (une « **MRM** »), ce qui lui aurait permis d'échanger des informations classifiées avec les députés, n'était pas atteint. Pour prendre une MRM, le SCRS doit avoir des motifs raisonnables de croire que l'activité visée par la mesure constitue une menace et que la MRM réduira cette menace. Dans ces cas, comme les menaces ne portaient pas sur l'intégrité

physique des deux députés et qu'échanger des informations avec eux n'aurait pas permis de modifier le comportement de l'acteur menaçant, le SCRS a estimé que le seuil n'était pas atteint.

Le 31 mai 2021, le SCRS a de nouveau transmis, via le RCTS, une note de gestion d'enjeux (NGE) au CSNR, au ministre de la Sécurité publique, à la cheffe de cabinet du ministre, Zita Astravas, et au sous-ministre de la Sécurité publique. La NGE expliquait le plan du SCRS d'offrir des breffages défensifs. La NGE indiquait que les deux députés étaient la cible d'acteurs menaçants issus de la RPC et que l'intérêt de la RPC envers M. Chong incluait un intérêt pour ses proches qui pourraient se trouver en RPC.

M. Rigby se souvenait avoir vu la NGE lors de sa première diffusion.

M. Stewart ne se souvenait pas l'avoir reçue, mais pensait qu'elle avait dû être incluse dans son cartable de renseignement.

Le ministre Blair et sa cheffe de cabinet, M<sup>me</sup> Astravas, affirment ne pas avoir reçu la NGE.

Le 20 juillet 2021, le SCRS a publié une longue évaluation du renseignement portant sur l'ingérence étrangère de la RPC au Canada. Ce produit a été diffusé plus largement dans la communauté de la sécurité nationale et du renseignement. Il mentionnait brièvement le renseignement discuté ci-dessus voulant que la RPC s'intéresse à M. Chong, mais ne le citait pas nommément. La partie pertinente indique qu'un fonctionnaire de la RPC a cherché à obtenir des informations sur les membres de la famille d'un député canadien qui pourraient se trouver en RPC en vue d'éventuelles sanctions, et que cet effort visait presque certainement à faire de ce député un exemple et à dissuader d'autres personnes d'adopter des positions hostiles à la RPC.

Le ministre Blair a déclaré avoir vu cette évaluation du renseignement, notamment le paragraphe selon lequel les fonctionnaires de la RPC s'intéressaient aux proches des députés canadiens qui pourraient vivre en RPC dans le but de leur imposer d'autres sanctions potentielles. Il ne savait pas que le paragraphe concernait M. Chong jusqu'à ce que les médias en fassent état en 2023. Le ministre Blair n'a pas donné suite à ce rapport auprès du SCRS ni d'autres personnes.

M<sup>me</sup> Astravas ne se souvient pas avoir reçu l'évaluation, mais a indiqué qu'elle devait l'avoir vue, puisqu'elle recevait tous les documents transmis au ministre Blair.

M. Morrison se souvenait d'avoir lu l'évaluation en septembre 2021, lorsqu'il était CSNR par intérim. Il ne savait pas que le député mentionné était M. Chong. Il a trouvé l'évaluation plutôt insuffisante dans son ensemble, car elle soulevait plus de questions qu'elle n'apportait de réponses, ce qui l'a incité à demander à son équipe plus d'informations sur les efforts d'ingérence étrangère de la RPC au Canada. Le Secrétariat de l'Évaluation du renseignement du BCP, en réponse à cette demande, a produit le Rapport spécial du BCP que j'ai abordé plus tôt dans ce chapitre.

Comme le ministre Blair, divers autres témoins du gouvernement, y compris de hauts responsables du cabinet du premier ministre (CPM) et le premier ministre, ont également appris pour la première fois, par l'entremise de l'article du 1<sup>er</sup> mai 2023, que la RPC avait démontré un intérêt pour M. Chong en 2021. L'article a donné lieu à une série de réunions entre de hauts fonctionnaires, des ministres et du personnel ministériel.

## Réponse du gouvernement au renseignement

Avant la promulgation de la *Loi concernant la lutte contre l'ingérence étrangère*<sup>12</sup>, qui a conféré au SCRS des pouvoirs supplémentaires pour partager des informations classifiées dans certaines circonstances, la capacité du SCRS à échanger des informations classifiées à l'extérieur du gouvernement fédéral était limitée. Le seul mécanisme lui permettant de communiquer des informations classifiées à une personne n'ayant pas l'autorisation de sécurité requise, comme M. Chong, était une MRM (voir le chapitre 11, volume 3). Comme je l'explique ci-dessus, le SCRS a conclu que le seuil requis pour prendre une MRM n'était pas atteint, car il n'avait pas de motifs raisonnables de croire que l'activité de la RPC constituait une menace.

Comme mentionné ci-dessus, en réponse au renseignement de 2021, le SCRS a fourni un breffage défensif non classifié à M. Chong en juin 2021. Le SCRS s'est aussi entretenu avec lui par la suite<sup>13</sup>. Lors de ces rencontres, le SCRS n'a pas révélé le renseignement concernant l'intérêt manifesté par la RPC à son égard. Cependant, le directeur du SCRS à l'époque, David Vigneault, m'a dit que, même si elles n'étaient pas classifiées, les interactions du SCRS avec M. Chong étaient influencées par la connaissance qu'avaient les représentants du SCRS de l'ensemble des informations classifiées. Selon lui, cela leur permettait de contextualiser adéquatement les informations fournies à M. Chong.

Un représentant des bureaux régionaux du SCRS, qui était présent lors du breffage défensif, a dit avoir compris que M. Chong était bien informé des actions que pourrait prendre la RPC en lien avec sa fonction. Bien qu'il n'ait pas assisté au breffage ni aux réunions qui ont eu lieu par la suite, M. Vigneault a lui aussi compris, d'après les documents liés à ces rencontres, que les interactions étaient fructueuses et que M. Chong était conscient des risques d'ingérence étrangère.

M. Chong m'a dit que le breffage défensif lui avait permis d'obtenir des conseils généraux sur la manière de se protéger contre l'ingérence étrangère, mais qu'il n'avait pas été informé qu'un diplomate de la RPC menait des recherches sur lui ou sa famille dans le but d'imposer des sanctions. Il m'a

---

<sup>12</sup> Déposée au Parlement en tant que projet de loi C-70. Voir au chapitre 12 (volume 3).

<sup>13</sup> Un document du SCRS indique que le breffage a eu lieu le 25 juin 2021, alors que M. Chong a affirmé, lors de son témoignage, qu'il avait eu lieu le 24 juin 2021. À mon avis, il n'y a pas lieu de s'interroger sur ce point.

aussi dit qu'à la suite de ce breffage, il a rencontré le SCRS à plusieurs autres occasions, au cours desquelles il a fourni des informations.

Comme indiqué ci-dessus, le 1<sup>er</sup> mai 2023, le Globe and Mail a publié un article fondé sur du renseignement présumé du SCRS qui aurait fait l'objet d'une fuite, affirmant que M. Chong avait été la cible d'efforts d'ingérence étrangère de la part de la RPC en 2021.

Le 2 mai 2023, le premier ministre, M<sup>me</sup> Thomas (elle était alors CSNR) et M. Vigneault (il était alors directeur du SCRS), ont rencontré M. Chong pour discuter de l'article. Le premier ministre a dit à M. Chong qu'une partie de l'article était vraie et que d'autres parties étaient exagérées. Il a aussi déclaré avoir dit à M. Chong qu'il voulait que M. Chong obtienne le plus d'informations possible de la part des hauts fonctionnaires.

Immédiatement après la rencontre qu'a eue M. Chong avec le premier ministre, M. Vigneault et M<sup>me</sup> Thomas l'ont breffé en vertu de l'autorité du SCRS en matière de MRM. Cela leur a permis de faire référence à des documents classifiés.

M. Vigneault a dit à M. Chong que les rapports des médias ne reflétaient pas fidèlement l'évaluation du SCRS de 2021. Il n'y avait aucune information suggérant un risque d'atteinte à l'intégrité physique de M. Chong ni à celle de sa famille. Ainsi, certains récits des médias étaient incomplets ou incorrects. Surtout, il a indiqué à M. Chong que la façon dont les médias interprétaient le mot « cible » contenu dans les rapports de renseignement ne correspondait pas à l'utilisation qu'en fait le SCRS. Par exemple, dans le domaine du renseignement, une « cible » peut signifier une personne « d'intérêt » et non pas nécessairement une cible « à des fins préjudiciables ». J'ai traité de cette terminologie problématique dans la section précédente de ce chapitre.

Avant de mener une MRM, le SCRS procède à une évaluation des risques fondée sur quatre catégories, à savoir les risques opérationnels, de réputation, de politique étrangère et juridiques de l'action proposée. Le SCRS estimait que le breffage de MRM pour M. Chong comportait un risque élevé.

Marco Mendicino, qui était ministre de la Sécurité publique à l'époque du breffage de MRM de 2023, m'a dit que, bien que le renseignement n'ait pas révélé l'existence d'une menace physique contre M. Chong et sa famille, le breffage de MRM était nécessaire en raison des allégations qui circulaient dans les médias au sujet d'une telle menace.

Entre 2021, lorsque le SCRS a fourni à M. Chong un breffage préventif de sécurité non classifié, et 2023, lorsque M. Vigneault et M<sup>me</sup> Thomas l'ont breffé sur des informations classifiées en utilisant le pouvoir du SCRS en matière de MRM, la nature de l'information sur l'intérêt de la RPC envers M. Chong n'a pas changé. Je me questionne quant à savoir comment le seuil pour prendre une MRM ait pu être atteint en 2023 sans qu'il ne l'ait été en 2021, mais mon mandat n'est pas d'examiner l'exercice par le SCRS de ses pouvoirs.

Le SCRS n'a de politique concernant précisément le partage d'informations à la police lorsque des menaces à la vie sont identifiées. J'ai entendu des témoignages du SCRS selon lesquels, lorsqu'il dispose d'informations voulant qu'il existe une menace d'atteinte à l'intégrité physique ou à la vie d'une personne, il contacte immédiatement les autorités policières par le biais des canaux établis. Les forces de l'ordre peuvent alors informer la personne de la menace, en vertu de leur « devoir de mise en garde ».

Brian Clow, chef de cabinet adjoint du premier ministre, a assisté à une réunion avec des ministres et hauts fonctionnaires lors de laquelle cet incident a fait l'objet d'une discussion. Les notes prises par M. Clow lors de cette rencontre confirment que le SCRS ne pensait pas qu'il y avait une menace d'atteinte à l'intégrité physique d'un député ni à celle de sa famille. Le ministre LeBlanc, qui était à cette époque ministre de la Sécurité publique, s'est rappelé qu'au cours de cette réunion, il a cherché à comprendre quel type de recherche était prétendument effectuée et s'il s'agissait d'un euphémisme pour désigner une activité clandestine ou simplement une recherche de documents de source ouverte. Il se souvenait d'avoir entendu parler de recherche sur des documents de source ouverte, ce qui, à son avis, était différent du discours public qui référerait à une « menace ». D'après ce qu'il a compris de la réunion, il existait un certain écart entre l'explication du SCRS à propos de la recherche et ce que M. Chong et d'autres percevaient comme des menaces.

En 2023, le SCRS a aussi fourni des breffages de MRM qui lui ont permis de divulguer des informations classifiées sur les efforts d'ingérence étrangère de la RPC à la députée Jenny Kwan, au député Erin O'Toole et à l'ancien député Kenny Chiu. Je décris ces démarches plus en détail au [chapitre 15](#).

### **Les choses auraient-elles été différentes si le renseignement du SCRS avait été plus largement diffusé en 2021?**

Plusieurs témoins m'ont dit que s'ils avaient reçu ou lu le rapport de renseignement du SCRS sur l'intérêt de la RPC pour M. Chong en 2021, le gouvernement n'aurait pas réagi différemment.

Les rapports du SCRS quant aux recherches de la RPC sur M. Chong et sa famille décrivent les sanctions économiques comme une possibilité. Le sous-ministre aux Affaires étrangères, David Morrison, a déclaré que la RPC voulait en savoir plus sur certains députés canadiens d'origine chinoise et a cherché à mener des recherches sur eux. Selon lui, le simple fait d'effectuer des recherches sur des politiciens ne constitue pas de l'ingérence étrangère. C'est ce que font tous les diplomates. Il a aussi déclaré que les sanctions sont une pratique diplomatique courante.

M. Morrison a expliqué qu'après la motion sur les Ouïghours, le Canada et la RPC se sont imposé des sanctions réciproques. AMC a discuté avec le SCRS du fait que les sanctions économiques de la RPC contre le Canada représentaient un outil légitime de la conduite des affaires d'État et des affaires diplomatiques. Ces sanctions peuvent légitimement viser la famille de la personne ciblée.

Vincent Rigby, CSNR en 2021, a déclaré qu’au cours de sa carrière dans le domaine de la sécurité et du renseignement, il a appris « à ne pas appuyer sur le bouton de panique », mais plutôt à attendre et à voir comment une situation pourrait évoluer. Selon lui, les rapports de renseignement étaient encore de l’ordre du « voyons comment cela évolue », parce que ce qui se passait n’était pas clair.

Michael MacDonald, secrétaire adjoint au Secrétariat de la sécurité et du renseignement du BCP, a déclaré que le comportement décrit dans le renseignement n’était pas nécessairement répréhensible.

Martin Benjamin, directeur général et chef du renseignement d’AMC en 2021 (maintenant à la retraite), aurait transmis le renseignement aux bureaux géographiques compétents d’AMC, mais, en l’absence de renseignement exploitable, il ne s’attendait pas à ce qu’AMC prenne des mesures contre des diplomates chinois.

Rob Stewart, ancien sous-ministre de la Sécurité publique, a expliqué que la NGE de mai 2021 (concernant les breffages défensifs à MM. Chong et Chiu) aurait été incluse dans la conversation élargie entre Sécurité publique Canada et le SCRS au sujet de la réponse du SCRS. Cette information, toutefois, n’aurait pas été considérée comme une révélation. Ce type de NGE n’est pas inhabituel. M. Stewart considère les NGE comme un moyen de transmettre des informations. Elles ne nécessitent pas d’action. Il y aurait vu une indication que la menace d’ingérence étrangère augmentait, ce qui pourrait éclairer les décisions politiques.

David Vigneault m’a dit que les médias avaient fait du sensationnalisme avec le renseignement concernant M. Chong et qu’ils avaient présenté l’information sans la contextualiser. Selon l’évaluation du SCRS, il n’y a jamais eu de menace physique envers M. Chong ni envers quiconque. Bien que le renseignement fût important et qu’il ait donné lieu à un breffage défensif non classifié, il ne s’agissait pas du « plus gros drapeau rouge de tous les temps », comme les médias l’ont laissé entendre.

Le ministre Blair a déclaré qu’après avoir pris connaissance de l’évaluation de juillet 2021, il n’avait aucune inquiétude quant à la sécurité de qui que ce soit. Il a mentionné que ce document illustre leurs préoccupations communes à propos de l’ingérence étrangère et que les activités que rapportait le renseignement correspondaient à ce qu’il avait dit publiquement, notamment dans la lettre qu’il avait adressée aux parlementaires à ce sujet en décembre 2020. Pour le ministre Blair, une recherche sur un député en vue d’imposer des sanctions ne soulève aucune inquiétude. Le Canada impose aussi des sanctions à des ressortissants étrangers.

Pour sa part, M. Chong a déclaré que s’il avait su la nature de l’intérêt que lui portait la RPC, il aurait informé ses proches qu’ils étaient potentiellement visés. Il a indiqué qu’il aurait été plus attentif à la situation lorsqu’il participait à des réunions près du consulat de la RPC à Toronto. Il a aussi mentionné qu’il aurait enregistré un débat réunissant tous les candidats sur un appel Zoom.

## Conclusions

À mon avis, lorsqu'il existe des informations spécifiques indiquant qu'un État envisage de prendre des mesures punitives à l'encontre d'une personne ou de personnes qui lui sont liées, il est important de veiller à ce que cette personne soit informée.

Je reconnais qu'en l'espèce, il se peut qu'il n'y ait jamais eu de menace d'atteinte à l'intégrité physique de M. Chong ou à celle d'un membre de sa famille. Cependant, je reconnais également qu'il est très difficile, voire impossible, de savoir avec certitude ce qu'un État hostile a l'intention de faire avec les informations qu'il recueille. Nous pouvons le savoir ou finir par le comprendre après coup, mais cela ne nous aide pas à déterminer si une personne doit être informée au moment où le renseignement est recueilli.

Je crois donc que le SCRS a eu raison d'offrir un breffage défensif à M. Chong en 2021, même si le renseignement décrivait une activité diplomatique légitime. Il n'a toutefois pas été informé spécifiquement de l'intérêt de la RPC pour sa famille et lui, car il s'agissait d'informations classifiées. À mon avis, dans une telle situation, il faut s'efforcer de fournir le plus d'informations possible à la personne visée.

En termes clairs, je ne suggère pas que la sécurité des sources humaines, des sources techniques ou des méthodes de renseignement soient compromises au bénéfice d'informer les personnes visées. Il faut plutôt s'efforcer de trouver des moyens de communiquer autant d'informations que possible à la personne concernée.

Il ressort de la preuve que les informations relatives à l'intérêt de la RPC pour plusieurs députés après la motion sur les Ouïghours n'ont pas circulé comme elles auraient dû au printemps 2021.

Je reconnais que dans le contexte plus large des rapports de renseignement, les rapports du SCRS antérieurs à mai 2021 ont pu être considérés comme peu significatifs. Cependant, la note de gestion des enjeux (NGE) de mai 2021 a été envoyée spécifiquement pour informer le ministre de la Sécurité publique du renseignement détenu par le SCRS et de son plan d'action, et l'information n'est jamais parvenue au ministre.

Il semble qu'il y ait eu une divergence entre le point de vue du SCRS sur les NGE et celui des destinataires de ces NGE. Cela démontre un problème dans la manière dont les produits de renseignement étaient distribués à l'époque. Cela montre aussi qu'il ne faut pas se fier à un produit de renseignement écrit, sans en faire le suivi, comme moyen d'informer un ministre ou un décideur de haut rang. À mon avis, l'envoi d'un produit écrit n'est pas suffisant. Si la question est suffisamment importante pour que le ministre en soit informé, un suivi devrait être assuré et il faudrait breffer le ministre.

## Le mandat du SCRS

De la preuve a été administrée concernant une demande du SCRS à la Cour fédérale pour l'obtention d'un mandat. Or, un délai extrêmement important s'est écoulé entre le moment où le ministère a reçu la demande d'autorisation et le moment où il l'a approuvée.

Le gouvernement a revendiqué la confidentialité à des fins de sécurité nationale quant à l'objet du mandat. J'ai déterminé que je pouvais tirer les conclusions qui s'imposaient sans qu'il soit nécessaire de divulguer l'objet du mandat dans le rapport public. Il n'a donc pas été nécessaire de faire trancher par la Cour fédérale la question de la sécurité nationale soulevée par le gouvernement.

### La procédure d'approbation de mandat

La *Loi sur le Service canadien du renseignement de sécurité* impose que toutes les demandes de mandat soient approuvées par le ministre de la Sécurité publique. Les mandats pouvant être accordés au SCRS comptent parmi les outils d'enquête les plus puissants et intrusifs dont dispose l'État. Ils permettent un vaste éventail d'activités hautement intrusives qui, par leur nature même, sont destinées à ne jamais être révélées. C'est en partie pour cette raison que la procédure pour obtenir la délivrance d'un mandat s'avère à la fois complexe et exigeante sur le plan du travail requis, impliquant de nombreuses étapes internes et plusieurs niveaux d'approbation.

Cette procédure est la suivante.

Lorsqu'une demande est prête, le SCRS l'expédie à Sécurité publique Canada. Les fonctionnaires du ministère l'examinent et rédigent un résumé comportant une recommandation au ministre d'approuver ou non la demande. Lorsque tout est en ordre, le sous-ministre signe ce document de consultation et le transmet au cabinet du ministre pour que le ministre l'examine. Le cabinet du ministre peut poser des questions ou demander des informations supplémentaires auprès des équipes du SCRS ou de Sécurité publique Canada. Si le ministre approuve la demande, le ministère de la Justice la dépose ensuite auprès de la Cour fédérale, où un juge tient une audience pour décider s'il délivre ou non le mandat.

### Comment la procédure d'approbation de mandat s'est déroulée dans ce cas-ci

Dans ce cas-ci, la procédure interne du SCRS pour la préparation de la demande de mandat a duré plusieurs mois. J'ai entendu des témoignages selon lesquels le SCRS a dû prendre en compte des considérations particulières lors de la préparation de cette demande de mandat.

La date à laquelle la demande a été soumise à Sécurité publique Canada est désignée dans le cadre des travaux de la Commission comme le « Jour 0 ».

L'affidavit au soutien de la demande de mandat a été rédigé plusieurs mois avant le Jour 0 et a été mis à jour un mois avant le Jour 0. La demande a été envoyée à Sécurité publique Canada avec une lettre du directeur du SCRS, David Vigneault, recommandant au ministre d'approuver la demande dans un délai de six jours.

M. Stewart, le sous-ministre de la Sécurité publique de l'époque, a expliqué que le SCRS donnait généralement des délais courts pour que les décisions ministérielles sur les demandes de mandat soient prises, reflétant le fait qu'un travail important a déjà été accompli avant que la demande n'arrive à Sécurité publique Canada. Il a toutefois précisé que ces délais étaient indicatifs, et non des échéances strictes. Il a aussi souligné que la demande a été présentée pendant la pandémie. Lorsque la présentation d'une demande au ministre n'était pas chose facile, de telles échéances relevaient plus de l'idéal que de la réalité.

Tous les mandats s'accompagnaient de délais assez courts, en raison à la fois de l'examen préalable et du désir du SCRS d'« aller de l'avant ».

M. Stewart a déclaré que mettre un délai plus long que deux semaines garantissait pratiquement que la demande disparaîtrait au « bas de la pile ».

M. Stewart, à titre de sous-ministre, a signé le document de consultation le Jour 4. Il a ensuite fait en sorte que le dossier soit transmis au cabinet du ministre à Ottawa par l'agent de liaison ministériel, accompagné d'une note de présentation demandant que le ministre l'autorise le jour même. Le ministre se trouvait à Toronto à ce moment-là.

M. Vigneault a témoigné qu'il ne comprenait pas pourquoi l'approbation était demandée pour le jour même, puisqu'il ne s'agissait pas d'une situation urgente. Le SCRS prévoit généralement un délai de dix jours pour que le ministre examine et approuve une demande de mandat. M. Stewart a déclaré qu'il n'aurait pas prêté une attention particulière à la date indiquée. Plutôt, il l'aurait simplement transmise. Il estimait qu'elle ne devait pas être interprétée comme signifiant que le mandat devait être traité de manière urgente.

M. Rochon, ancien sous-ministre adjoint principal du Secteur de la sécurité nationale et de la cybersécurité, a déclaré que l'on s'attend généralement à ce que le ministre approuve une demande de mandat dans un délai d'une à deux semaines. M. Stewart a fait remarquer que si le mandat avait été urgent, une procédure différente aurait été suivie : le directeur du SCRS lui aurait dit qu'il s'agissait d'un cas urgent.

Selon M. Stewart, une fois le dossier transmis au cabinet du ministre, il revenait essentiellement à celui-ci et au SCRS de coordonner sa présentation au ministre. L'agent de liaison ministériel était responsable de suivre la demande et de rappeler au cabinet du ministre la nécessité d'obtenir sa signature. Toutefois, M. Stewart ne se souvenait pas et ne savait pas précisément si l'agent avait rappelé l'existence de la demande d'autorisation de mandat alors que celle-ci était en attente au cabinet du ministre.

Zita Astravas, cheffe de cabinet du ministre Blair à l'époque, ne se rappelle pas à quelle date exactement elle a reçu la demande de mandat pour la première fois. Elle a indiqué que cela peut ne pas être le Jour 4. M<sup>me</sup> Astravas ne se souvient pas avoir vu la date de retour demandée du Jour 4, mais elle ne conteste pas que cette information figurait dans les documents qu'elle a reçus. Je note qu'au moment des travaux de la Commission, M<sup>me</sup> Astravas avait quitté le cabinet du ministre Blair et travaillait dans le secteur privé. Par conséquent, la Commission ne dispose d'aucune trace de ses courriels ou de ses inscriptions au calendrier pour la période en question.

Selon la procédure habituelle, le SCRS a breffé M<sup>me</sup> Astravas sur la demande d'autorisation avant qu'elle ne soit transmise au ministre. Ce breffage a eu lieu le Jour 13 et est désigné dans le cadre des travaux de la Commission comme le « breffage initial ».

M<sup>me</sup> Astravas a posé des questions sur le mandat lors de ce breffage initial. Elle a déclaré qu'en tant que cheffe de cabinet, il faisait partie de ses fonctions de poser des questions sur les documents que le ministre devait approuver, comme celui-ci, afin de s'assurer qu'ils étaient prêts à lui être présentés. Les questions de M<sup>me</sup> Astravas portaient sur le fait de savoir si les activités décrites dans la demande d'autorisation atteignaient le seuil requis pour qu'un mandat soit délivré, et sur d'autres informations particulières qui lui avaient été communiquées lors du breffage initial. M<sup>me</sup> Astravas a mentionné qu'à une autre occasion, elle a aussi reçu un breffage concernant la liste Vanweenan<sup>14</sup>, et sur la manière dont les personnes figurant sur cette liste pourraient être affectées par l'exécution du mandat. Il n'y a aucune trace d'un breffage particulier à ce sujet dans les documents obtenus par la Commission.

M<sup>me</sup> Astravas a déclaré qu'elle a posé ces questions pour son information uniquement, et non au nom du ministre. Elle n'avait pas l'intention de laisser entendre que le mandat risquait de ne pas être approuvé tant que ses questions n'auraient pas reçu de réponses. Une haute fonctionnaire du SCRS s'est dit d'accord avec M<sup>me</sup> Astravas. Michelle Tessier, qui avait assisté au breffage initial, a indiqué qu'elle avait l'impression que M<sup>me</sup> Astravas posait ces questions dans un objectif « de suivi et de compréhension ». Elle a noté qu'à ce moment-là, M<sup>me</sup> Astravas n'avait pas encore lu l'affidavit; elle recevait un breffage et posait des questions pour avoir de l'information. D'après M<sup>me</sup> Tessier, les questions de M<sup>me</sup> Astravas visaient à « tester » pour s'assurer qu'il y avait suffisamment d'informations pour conclure que les activités

---

<sup>14</sup> La *Loi sur le SCRS* oblige le SCRS à identifier les personnes « connues » qui peuvent être directement affectées par les mesures autorisées par un mandat (par exemple, s'il est proposé d'intercepter leurs communications). L'appellation « liste Vanweenan » est tirée du nom d'un arrêt de 1988 de la Cour suprême du Canada, où la Cour a conclu que l'une des parties appelantes, M<sup>me</sup> Vanweenan, était une personne « connue » au sens d'une disposition similaire du *Code criminel* s'appliquant aux demandes d'écoute électronique, parce qu'elle était connue des autorités policières et parce qu'il y avait des motifs raisonnables et probables de croire que ses communications pourraient être utiles à l'enquête : *R c Chesson*, [1988] 2 RCS 148.

décrites dans la demande dépassaient le seuil requis pour utiliser un outil aussi intrusif qu'un mandat.

Dans un courriel interne du SCRS, l'auteur de l'affidavit, qui était également présent au breffage initial mais qui n'a pas témoigné devant moi, semble avoir eu une impression différente. Il a exprimé son avis selon lequel la demande risquait de ne pas être signée par le ministre, et qu'il était donc nécessaire de fournir des arguments supplémentaires pour expliquer pourquoi le SCRS avait besoin d'obtenir le mandat.

M<sup>me</sup> Tessier s'est dite en désaccord avec les commentaires de l'auteur de l'affidavit. Elle n'a pas perçu les questions de M<sup>me</sup> Astravas comme constituant une condition pour qu'elle fasse progresser la demande d'autorisation. Dans son esprit, « il n'y a jamais eu d'indication » que M<sup>me</sup> Astravas ne soumettrait pas la demande de mandat au ministre tant qu'elle n'aurait pas obtenu des réponses à ses questions.

M<sup>me</sup> Tessier a expliqué que, du point de vue du SCRS, il fallait répondre aux questions de M<sup>me</sup> Astravas, car elles pourraient très bien être des questions que le juge chargé d'examiner la demande de mandat pourrait poser.

Le SCRS a éventuellement donné suite aux questions posées par M<sup>me</sup> Astravas lors du breffage initial. Le dossier classifié contient plusieurs échanges de courriels internes au SCRS datant des Jours 14 à 21 qui documentent ces démarches. Au cours de ce suivi, le SCRS a cherché à obtenir des informations sur une affaire qui aurait été « absolument cruciale » pour le SCRS si elle avait été fondée, car, le cas échéant, elle aurait dû être mentionnée dans l'affidavit afin que le SCRS respecte son obligation de franchise envers la Cour fédérale<sup>15</sup>. Cette obligation de franchise était au centre des préoccupations du SCRS à l'époque, parce que la Cour fédérale avait rendu une décision en formation plénière dans laquelle elle concluait que le SCRS avait manqué à cette obligation en lien avec plusieurs demandes de mandat.

La préoccupation du SCRS en lien avec la question mentionnée ci-dessus n'était en fait qu'un malentendu : l'événement qui préoccupait le SCRS n'avait pas eu lieu et cette question a été résolue au Jour 21. La preuve dont je dispose n'indique pas si M<sup>me</sup> Astravas en a été informée ni si, ou quand, elle a reçu des réponses aux questions qu'elle avait posées lors du breffage initial.

En effet, le dossier contient peu d'informations utiles sur ce qui s'est passé dans les semaines qui ont suivi le Jour 21 jusqu'au Jour 48, lorsque le directeur du SCRS a discuté de la demande de mandat avec M<sup>me</sup> Astravas. Le SCRS ne se souvient pas d'échanges réciproques concernant ce mandat. M. Vigneault a déclaré que la discussion du Jour 48 ne portait pas sur la question de savoir s'il y avait lieu d'aller de l'avant avec la demande, mais

---

<sup>15</sup> Cette obligation exige que les parties qui se présentent devant un tribunal dans le cadre d'une procédure *ex parte* (c'est-à-dire en l'absence de l'autre partie) fassent preuve de la bonne foi la plus absolue dans les représentations qu'elles font, notamment en présentant de manière complète et sincère tous les faits importants pertinents.

plutôt sur comment gérer la complexité du dossier sur le plan de la logistique, comme l'établissement de la liste de diffusion. M<sup>me</sup> Astravas a indiqué que cette discussion aurait pu être le breffage sur la liste Vanweenan.

Le breffage du ministre a ensuite été fixé à environ une semaine plus tard, au Jour 54. Le ministre Blair a examiné la demande d'autorisation de mandat dans des locaux sécurisés juste avant son breffage et l'a approuvée le jour même. M. Vigneault se souvient que le ministre Blair n'a pas montré ou exprimé d'hésitation à autoriser la demande de mandat lorsqu'elle lui a été présentée.

### **Quand le ministre Blair a-t-il appris l'existence du mandat?**

Le ministre Blair a témoigné qu'il n'avait appris l'existence d'un mandat exigeant son examen dans des locaux sécurisés que deux ou trois jours avant son breffage ministériel.

Plusieurs mois avant son breffage, le ministre Blair avait été breffé au sujet de l'objet du mandat, mais il n'avait pas été informé à ce moment-là que le SCRS demanderait la délivrance d'un mandat. Il s'attendait à ce que le SCRS poursuive son enquête, mais personne n'a fait mention, lors de ce premier breffage, de l'intention du SCRS de demander un mandat.

Peu avant son breffage, le ministre Blair a appris qu'il devrait se rendre dans des locaux sécurisés à Toronto pour examiner une demande d'autorisation de mandat, mais il ne savait pas sur quoi portait le mandat, car cette information ne pouvait être divulguée ailleurs que dans un cadre sécurisé. Néanmoins, compte tenu du breffage antérieur, il n'a pas été surpris lorsqu'il a pris connaissance de la demande de mandat et de son sujet.

M<sup>me</sup> Astravas a déclaré que le ministre Blair ne savait pas que la demande de mandat attendait son approbation jusqu'à ce qu'il la voie pour la première fois le Jour 54. Toutefois, elle croyait qu'il était conscient, d'après ses discussions antérieures avec le SCRS, que le SCRS s'apprêtait à demander la délivrance d'un mandat à ce sujet.

### **Retard dans le processus d'approbation de mandat**

Les représentants du SCRS ont déclaré que le retard mis à obtenir la signature du ministre était hautement inhabituel, surtout à la lumière des nombreuses discussions précédant la présentation de la demande de mandat. Les agents opérationnels du SCRS ont trouvé cela très frustrant. M<sup>me</sup> Tessier a déclaré que les représentants du SCRS veulent toujours que les opérations se déroulent rapidement, mais elle-même n'était pas inquiète.

Ni le personnel du SCRS ni celui de Sécurité publique Canada n'a soulevé quelque préoccupation au sujet du retard auprès du ministre Blair ou de M<sup>me</sup> Astravas au cours de la période de 35 jours comprise entre le Jour 13 (le breffage initial) et le Jour 48 (la discussion entre le directeur du SCRS et M<sup>me</sup> Astravas) et n'a pas non plus laissé entendre qu'il s'agissait d'une

question urgente. Aucun document n'indique que le SCRS ou Sécurité publique Canada aurait évoqué la question de la demande d'autorisation de mandat avec le cabinet du ministre au cours de cette période, ce qui est surprenant.

La procédure normale en cas de problème concernant le contenu ou le délai de traitement d'une demande d'autorisation de mandat aurait été que le personnel opérationnel du SCRS responsable de la demande communique avec ses homologues de Sécurité publique Canada. Aucune preuve n'indique que cela a été fait ici. Les seuls courriels exprimant des inquiétudes quant à ce retard sont internes au SCRS.

M. Vigneault a déclaré qu'il laissait la procédure suivre son cours. Son personnel ne lui a fait part d'aucune urgence. Il a compris qu'il s'agissait d'un mandat « plus compliqué » et n'était pas surpris que le ministre y « réfléchisse à tête reposée ». Ce n'était pas un sujet sur lequel M. Vigneault « talonnait le ministre, la cheffe de cabinet ou le sous-ministre ». Ce n'est que plus tard, après le témoignage du ministre devant le Comité permanent de la procédure et des affaires de la Chambre en juin 2023, qu'il a appris que le ministre Blair n'avait pris connaissance de la demande d'autorisation de mandat que le jour où il l'avait signée.

Par ailleurs, les représentants de Sécurité publique Canada n'ont jamais évoqué le mandat avec le ministre après avoir envoyé la demande à son cabinet. Ils considéraient que la question relevait de la compétence du cabinet du ministre et qu'elle devait être traitée par celui-ci et par le SCRS. Pour eux, le SCRS avait une relation directe avec le ministre et pouvait soulever la question au besoin.

Bien que M<sup>me</sup> Astravas ait assisté à un certain nombre de breffages avec le ministre et le directeur du SCRS dans des espaces sécurisés entre les Jours 13 et 54, elle ne se souvient pas avoir abordé cette demande d'autorisation de mandat à l'une ou l'autre de ces occasions. L'ordre du jour de ces réunions était établi par le directeur du SCRS, et elle n'était pas certaine si tous les participants avaient les endoctrinements nécessaires pour discuter de cette demande d'autorisation de mandat.

Lors des audiences publiques de la Commission, le ministre Blair a convenu qu'il avait approuvé deux autres demandes de mandat vers la même époque, et qu'il s'est rendu dans un local isolé pour l'information sensible cloisonnée (un « LIISC ») dans ce but. Pour être clair, bien que les mandats en question aient été approuvés pendant la pandémie, aucun n'a été approuvé entre le Jour 13 et le Jour 54. Ils ont plutôt été approuvés quelques semaines plus tôt, alors que la pandémie sévissait. Rien n'indique que le ministre Blair se soit rendu dans un LIISC pour examiner ou approuver des demandes de mandat autres que le présent mandat entre les jours 13 et 54. S'il l'avait fait, il aurait été surprenant que personne du SCRS, de Sécurité publique Canada ou de son propre cabinet ne l'ait informé qu'une autre demande de mandat était en attente. Il existe de la preuve indiquant qu'il s'est rendu dans un LIISC au cours de cette période, mais à d'autres fins.

Les deux demandes de mandat auxquelles M. Blair a fait référence étaient des demandes de renouvellement de mandats existants, et non de nouvelles demandes. M<sup>me</sup> Astravas a déclaré que le renouvellement de mandats est un processus plus rapide que les demandes visant de nouveaux mandats puisque le ministre est déjà familier avec les documents, qui ont déjà été approuvés par un tribunal. Le ministre Blair a convenu que le processus de renouvellement était habituellement « un peu plus simple ». Il a également souligné que les demandes de renouvellement d'un mandat peuvent être assez urgentes, puisque le SCRS doit obtenir l'approbation de la Cour fédérale avant l'expiration des autorisations existantes.

Quoi qu'il en soit, je comprends que la preuve suggère qu'une demande d'autorisation de mandat est généralement reçue et approuvée par le ministre dans un délai de deux semaines. Dans ce cas-ci, le ministre Blair a déclaré qu'il avait été en mesure d'examiner et d'approuver la demande en quelques heures.

M<sup>me</sup> Astravas explique le délai d'approbation du mandat par le fait qu'il n'était pas identifié comme un point prioritaire dans les ordres du jour de breffage par le directeur du SCRS. Elle a aussi souligné que Sécurité publique Canada gérait plusieurs autres problèmes pendant cette période, notamment la pandémie, ce qui signifie qu'ils participaient à des réunions du comité du Cabinet liées à la COVID-19 tous les jours pendant plusieurs heures à l'époque. Elle a aussi mentionné le retrait du Canada d'Afghanistan, la sécurité des frontières, le contrôle des armes à feu, la fusillade en Nouvelle-Écosse, la sécurité économique, la mise à jour de la liste des organisations terroristes et les risques pour la sécurité résultant de la technologie 5G. Les représentants de Sécurité publique Canada ont fait valoir un point semblable.

M<sup>me</sup> Astravas a estimé que le temps écoulé entre l'approbation de la demande de mandat par le ministre et l'audience du tribunal pour l'autorisation indiquait qu'il ne s'agissait pas d'une question urgente. Les affaires urgentes étaient généralement portées devant le tribunal dans les heures ou les jours qui suivent l'autorisation. Je note qu'il s'agit là d'une observation faite en rétrospective et qu'elle ne connaissait pas ce fait au moment pertinent.

Le ministre Blair ne pouvait pas se prononcer quant à savoir si le retard était anormal ici. Il s'attendait à ce que tous les représentants concernés – M<sup>me</sup> Astravas, M. Vigneault et M. Stewart – veillent à ce qu'il voit ce qu'il devait voir. Il a souligné que l'urgence des demandes d'autorisation de mandat dépend de différents facteurs, notamment le fait qu'il s'agisse de renouvellements ou de nouvelles demandes.

### **Allégations d'ingérence**

M<sup>me</sup> Astravas a déclaré qu'elle avait été franche avec le personnel du SCRS tout au long de l'examen de la demande. Elle a déclaré qu'elle divulguait toujours au directeur du SCRS toute connaissance personnelle qu'elle pouvait avoir d'un élément lié à une affaire, et qu'elle l'avait fait dans le cas présent.

Dans les échanges de courriels internes du SCRS qui ont eu lieu entre les Jours 13 et 48, l’auteur de l’affidavit a exprimé sa frustration à l’égard du temps qu’il fallait pour obtenir une réponse du cabinet du ministre et il s’est dit préoccupé par la possibilité d’ingérence dans le processus. Des préoccupations semblables ont été exprimées par divers participants aux audiences publiques de la Commission. Ces préoccupations sont légitimes et compréhensibles compte tenu du délai très inhabituel écoulé entre le jour 0 et le jour 54. De plus, de l’ingérence dans une demande de mandat serait très grave.

M<sup>me</sup> Astravas a catégoriquement nié avoir voulu retarder la délivrance du mandat. Elle a réaffirmé avoir fait part de ses connaissances personnelles pertinentes au SCRS avant la demande d’autorisation et lorsqu’elle a été présentée au cabinet du ministre, ainsi qu’au ministre Blair. M. Vigneault a confirmé que M<sup>me</sup> Astravas lui avait fait part de cette connaissance et a déclaré qu’il considérait cela comme un signe de transparence de sa part.

Le ministre Blair a déclaré que le mandat n’avait jamais risqué de ne pas être approuvé et qu’il n’avait tenu compte que de ses responsabilités légales pour évaluer la demande, sans tenir compte d’autres facteurs. Le fait qu’il connaisse ou non une personne figurant sur la liste Vanweenan n’était pas pertinent pour son examen.

Tant le ministre Blair que M<sup>me</sup> Astravas ont déclaré catégoriquement qu’ils n’avaient informé personne de la demande de mandat, y compris au Bureau du Conseil privé ou au cabinet du premier ministre.

Les représentants du SCRS n’avaient pas l’impression que le ministre Blair ou M<sup>me</sup> Astravas avaient des réserves au sujet du mandat. Lorsqu’on lui a demandé de commenter les préoccupations de l’auteur de l’affidavit, M<sup>me</sup> Tessier a déclaré qu’elle n’avait jamais eu l’impression qu’il y avait eu une quelconque ingérence de la part de M<sup>me</sup> Astravas, ou une quelconque tentative d’empêcher la demande de mandat d’aller de l’avant :

---

[l’auteur de l’affidavit a] parfaitement le droit d’avoir cette opinion, mais tout ce que je peux dire à cet égard, c’est que dans toutes mes interactions avec Zita au sujet de ce dossier ou dans le dossier en général, je n’ai pas eu l’impression qu’il y avait eu une quelconque (...) ingérence. Je suis très claire à ce sujet. On ne m’a jamais dit que cela ne devrait pas aller de l’avant. Comme je l’ai dit (...), il n’y a jamais eu la moindre allusion dans les discussions que j’ai eues, à savoir que nous ne pouvions pas aller de l’avant avec ce dossier. En fait, ce serait plutôt le contraire. Je ne pense pas qu’ils veuillent être perçus comme s’ingérant dans un dossier »<sup>16</sup>.

---

---

<sup>16</sup> Témoignage de Michelle Tessier, été 2024, transcription de l’audience tenue à huis clos.

M. Vigneault s’est montré tout aussi catégorique en rejetant les allégations d’ingérence. Il a fait remarquer qu’à moins que les choses ne changent radicalement dans les années à venir, si le ministre de la Sécurité publique devait refuser d’approuver une demande de mandat pour des raisons illégitimes, le directeur du SCRS le saurait, et cela serait extrêmement problématique. Cela concorde avec les témoignages que j’ai entendus au sujet du renseignement impliquant des députés de l’opposition. M. Vigneault m’a dit qu’il serait plus compliqué de communiquer du renseignement sur les partis de l’opposition au gouvernement au pouvoir. J’aborde ce point plus en détail au [chapitre 15](#).

## Approbaton du mandat

Le mandat a été approuvé par la Cour fédérale environ trois semaines après le Jour 54.

## Conclusions

Je suis dans une étrange position face à cet enjeu. Rien dans la preuve n’explique en fait le délai très inhabituel qui s’est écoulé entre le moment où la demande de mandat a été remise à la cheffe de cabinet du ministre, M<sup>me</sup> Astravas, et le moment où elle a été portée à l’attention du ministre. Je ne comprends pas pourquoi personne, que ce soit au sein du SCRS ou de Sécurité publique Canada, n’a tiré le signal d’alarme et n’a demandé s’il manquait quelque chose dans la demande de mandat ou si celle-ci posait problème. Il me semble que toutes les personnes impliquées ont failli à la tâche. Lorsqu’un ministre de la Sécurité publique ignore qu’il doit examiner une demande de mandat, il ne peut accomplir les obligations que lui impose la loi.

Toutefois, même si le retard est en soi inacceptable, la preuve ne fait état d’aucun acte répréhensible au-delà d’un manque de diligence. Il n’y a pas non plus quelque indication dans la preuve dont je dispose voulant que l’exécution du mandat ait été compromise.

Cet incident démontre cependant qu’il était urgent et nécessaire d’instaurer des procédures plus systématiques et rigoureuses pour faire le suivi et garder une trace des demandes d’autorisation de mandats du moment où elles quittent les mains du SCRS jusqu’à leur présentation à la Cour fédérale. Je retiens des témoignages des fonctionnaires actuels de Sécurité publique Canada et du ministre LeBlanc, ancien ministre de la Sécurité publique, qu’un tel processus est maintenant en place au ministère et que les demandes de mandat font l’objet d’une supervision et d’un suivi. À mon avis, de telles procédures s’avèrent essentielles.

Les mandats, comme je l’ai déjà mentionné ci-dessus, constituent des outils d’enquête puissants et importants. Très souvent, ils sont soumis à des contraintes de temps. Tout retard dans l’approbation d’une demande de mandat peut risquer de mettre en péril une enquête du SCRS en repoussant considérablement le début de la surveillance. Cela pourrait susciter des questions quant à l’intégrité du processus qui, si elles s’avéraient fondées, constitueraient de graves préoccupations.

## 14.13 Conclusion

Comme l'ont expliqué les chapitres précédents, de nombreuses entités au sein du gouvernement fédéral jouent un rôle dans la réponse à l'ingérence étrangère. Ces organismes génèrent une grande quantité d'informations, et les mécanismes qui permettent de communiquer ces informations au sein de l'appareil gouvernemental sont complexes.

Ce chapitre ne s'est intéressé qu'à la façon dont le renseignement circule au sein de la fonction publique et des ministères. Comme l'ont aussi expliqué les chapitres précédents de ce rapport, des organismes extérieurs au gouvernement jouent également des rôles clés dans la réponse à l'ingérence étrangère. Ces acteurs ont eux aussi besoin d'accéder à de l'information pour s'acquitter de leurs responsabilités. Dans le chapitre suivant, j'examine la manière dont l'information relative à l'ingérence étrangère est communiquée aux parlementaires et aux partis politiques.

## CHAPITRE 15

# Communication d'informations aux parlementaires et aux partis politiques

15.1	Introduction	66
15.2	Breffages non classifiés à l'intention des parlementaires	66
15.3	Prestation de breffages aux parlementaires dans le cadre de l'autorité du SCRS en matière de mesures de réduction de la menace	74
15.4	Une préoccupation concernant la communication d'information aux parlementaires : la cybercampagne du Advanced Persistent Threat 31 qui ciblait les membres de l'Alliance interparlementaire sur la Chine	81
15.5	Communication d'informations par le Bureau du Conseil privé	87
15.6	Communication d'informations par Affaires mondiales Canada	88
15.7	Informers les représentants des partis politiques durant une élection	90
15.8	Breffages classifiés aux chefs de parti politique	91
15.9	Communication d'informations par le Centre canadien pour la cybersécurité	96
15.10	L'effet du projet de loi C-70	96
15.11	Conclusion	97

**Les informations peuvent être incomplètes :** des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.

## 15.1 Introduction

Au **chapitre 14**, j'ai présenté la façon dont les organismes et les ministères du gouvernement fédéral échangent de l'information et la manière dont ils coordonnent leurs réactions face à l'ingérence étrangère. Dans ce chapitre-ci, j'examine la manière dont ils communiquent ces informations à l'extérieur du gouvernement.

Ce chapitre se concentre sur des acteurs qui peuvent à la fois faire l'objet d'ingérence étrangère et jouer un rôle pour la contrer, soit les parlementaires et les partis politiques.

## 15.2 Breffages non classifiés à l'intention des parlementaires

Dans un Précis analytique de novembre 2021, le Service canadien du renseignement de sécurité (le « **SCRS** ») a écrit :

---

[r]econnaître adéquatement l'ingérence étrangère et déterminer ce qu'ils doivent faire lorsqu'ils estiment en faire l'objet sont les principaux défis que doivent relever les députés. Nombre d'interactions entre les députés et des représentants étrangers semblent entrer dans la « zone grise » de l'ingérence étrangère, où la nature et les motifs de ces interactions sont ambigus. Cela complique la tâche consistant à établir une distinction entre, d'une part, les interactions relevant de la diplomatie légitime et, d'autre part, les tentatives clandestines et trompeuses de cultiver ou d'influencer des députés ou de s'assurer de leur collaboration<sup>17</sup>.

---

---

<sup>17</sup> Service canadien du renseignement de sécurité, *Rencontres du SCRS avec des représentants élus dans le dossier de l'ingérence étrangère : un projet d'importance nationale*, PAS n° 2021-22/89 (3 novembre 2021), p. 5, CAN003712\_R01.

J'ai entendu que les fonctionnaires et les dirigeants politiques reconnaissent qu'informer les parlementaires, leur personnel politique et les représentants des partis au sujet de l'ingérence étrangère est un élément important des efforts du Canada pour protéger nos institutions démocratiques. En pratique, toutefois, communiquer des informations à ces groupes n'est pas simple.

Cette complexité provient en partie de l'enjeu lié à la classification des informations et de la nécessité de protéger les sources et les méthodes employées pour obtenir le renseignement. Seuls quelques parlementaires détiennent une autorisation de sécurité, ce qui impose des restrictions relatives aux informations que le gouvernement peut leur communiquer. La communication d'informations sensibles aux parlementaires comporte des risques uniques sur le plan de la divulgation. Alors que la plupart des gens peuvent faire l'objet de poursuites s'ils divulguent des informations classifiées, les parlementaires qui s'expriment à la Chambre des communes ou au Sénat peuvent être protégés par le privilège parlementaire. Sans me prononcer sur l'importance ou la portée de ce privilège, je peux affirmer qu'il change nécessairement l'évaluation des risques que doit faire le gouvernement lorsqu'il détermine quoi divulguer, et à quel moment.

Les breffages non classifiés sur l'ingérence étrangère offerts aux parlementaires sont une façon pour le gouvernement de composer avec cette situation. Communiquer des informations non classifiées présente moins de risques et permet au gouvernement de s'adresser à plus de gens, bien que la quantité et la profondeur des informations qu'il peut communiquer s'en trouvent limitées.

## Breffages défensifs (breffages préventifs de sécurité)

Les breffages défensifs, aussi appelés « breffages préventifs de sécurité » ou « **BPS** », sont l'un des outils qu'utilise le SCRS pour interagir avec les gens et leur communiquer des informations. Ces breffages non classifiés peuvent être offerts à des élus et, dans certains cas, à leur personnel. Ils servent à les informer sur l'ingérence étrangère au Canada ainsi que sur les manières de la reconnaître et de s'en protéger.

Aucune information classifiée n'est transmise lors de BPS. Cependant, puisque leur contenu découle d'informations classifiées, le SCRS demande habituellement à ceux qui les reçoivent de ne rien divulguer de l'information reçue. Cela dit, aucune règle ne leur interdit de le faire.

Il n'existe pas de contenu standardisé pour les BPS, bien que les responsables utilisent un tableau-synthèse<sup>18</sup> non classifié qui décrit le mandat du SCRS en matière d'ingérence étrangère et renseigne sur ce qui

---

<sup>18</sup> Dans ce contexte, un tableau-synthèse est un diagramme faisant état des éléments importants d'un concept. Par exemple, un tel document, remis au Panel des cinq, portait sur l'activation du Protocole public en cas d'incident électoral majeur relativement aux avis publics.

constitue – ou non – de l'ingérence étrangère. Les breffages portent sur des sujets comme la manière dont les États tentent de s'ingérer, la nature clandestine de l'ingérence étrangère et les mesures que peuvent adopter les élus pour se protéger et protéger leur personnel. Souvent, la teneur du breffage est adaptée à la personne qui le reçoit et peut être modifiée au fil de la conversation.

Les BPS donnés aux députés Michael Chong et Kenny Chiu au printemps de 2021, que j'ai abordés au [chapitre 14](#), sont des exemples de breffages ciblés. Le but de ces breffages était de sensibiliser les députés à la menace d'ingérence étrangère, de leur fournir des conseils sur les pratiques exemplaires et de leur permettre d'exprimer leurs préoccupations. Selon le député Chong, il s'agissait d'un breffage à caractère général sur l'ingérence étrangère.

## Campagne de breffages préventifs de sécurité (BPS) en 2021

À l'été de 2021, le SCRS s'est lancé dans une campagne nationale de BPS à l'intention de députés du Parti libéral du Canada (le « **Parti libéral** »), du Parti conservateur du Canada (le « **Parti conservateur** ») et du Nouveau Parti démocratique du Canada (le « **NPD** »). Le SCRS s'est d'abord adressé aux députés de circonscriptions hautement prioritaires et à ceux qui étaient susceptibles de subir les effets directs d'activités d'ingérence étrangère.

Les députés participants ont donné au SCRS une rétroaction positive. Les informations communiquées en ont surpris certains, tandis que d'autres ont affirmé qu'ils reconnaissaient les activités décrites. Plusieurs ont affirmé que tous les députés auraient avantage à assister à ces breffages. Par la suite, plusieurs députés ont cherché à communiquer de nouveau avec le SCRS.

Idéalement, le SCRS aurait offert un breffage à tous les députés en 2021, mais cela n'a pas été possible, notamment en raison des horaires et des disponibilités. Identifier une approche adéquate a aussi fait l'objet de discussions au sein du gouvernement. En fin de compte, le SCRS a accordé la priorité aux députés qui bénéficieraient le plus de ces breffages. Lorsqu'il apprenait qu'une personne en particulier était visée par un État étranger, le SCRS, selon le cas, la convoquait à un BPS ou prenait une mesure de réduction de la menace (une « **MRM** »). Plus loin, je donne davantage de précisions sur le recours aux MRM par le SCRS pour offrir des breffages aux parlementaires.

Selon une note de service datée du 22 septembre 2022, le SCRS a décidé de poursuivre les breffages à tous les échelons du gouvernement. Le SCRS continue à donner des BPS de sa propre initiative et sur demande.

## Breffages non classifiés à l'intention de tous les parlementaires

### **2019-2020 : le Bureau du conseil privé demande l'autorisation de donner des breffages non classifiés à tous les parlementaires**

En décembre 2018, le Comité des parlementaires sur la sécurité nationale et le renseignement (le « **CPSNR** ») a recommandé que les parlementaires reçoivent des breffages sur les risques que pose l'ingérence étrangère et sur l'extrémisme au Canada dès leur assermentation, et à intervalle régulier par la suite. Le CPSNR a réitéré cette recommandation dans son rapport annuel de 2019. Le sergent d'armes de la Chambre des communes a aussi préconisé ce genre de breffages depuis 2019<sup>19</sup>.

Pour donner suite à la recommandation du CPSNR, le SCRS et ses partenaires au gouvernement ont commencé à élaborer un plan pour offrir des breffages aux parlementaires. Selon les témoins du SCRS, les intervenants au dossier convenaient que le contenu des breffages devait être élaboré par une équipe multidisciplinaire dont les membres proviendraient de différents organismes et ministères. Ceux-ci ont préparé plusieurs versions de la présentation.

Dans une note de service datée du 16 décembre 2019, le greffier du Conseil privé a demandé au premier ministre d'autoriser que des breffages non classifiés sur l'ingérence étrangère soient donnés aux députés et aux sénateurs. Il y précisait que ces breffages pouvaient à la fois accroître la sensibilisation et donner des stratégies pour atténuer les risques liés à l'ingérence étrangère. Le greffier a ajouté que le SCRS avait préparé un breffage d'introduction non classifié et a joint les documents en question à sa demande.

La note de service portait la mention « Décision requise », ce qui signifie que le personnel politique au cabinet du premier ministre (le « **CPM** ») prend généralement connaissance du document, formule ses propres recommandations et achemine le tout au premier ministre pour qu'il prenne une décision. Chaque année, le CPM reçoit environ un millier de documents de cette nature. Certains ne lui sont transmis que pour son information, mais la plupart requièrent une décision. Les témoins du CPM ont affirmé qu'il n'est pas inhabituel qu'il s'écoule des mois avant que le CPM étudie et s'attarde à une note de service.

Le CPM a reçu la note en décembre 2019. Les témoins du CPM m'ont dit que le personnel a estimé, dans l'ensemble, que les breffages devaient aller de l'avant. Toutefois, le document ne s'est pas rendu au premier ministre. Selon ce qu'on m'a dit, l'attention du gouvernement a été détournée vers la

---

<sup>19</sup> Le sergent d'armes assure la sécurité de la Chambre des communes et des députés lorsqu'ils y siègent et lorsqu'ils sortent de l'enceinte parlementaire.

pandémie de COVID-19, qui a éclaté peu après. De plus, les parlementaires ne se trouvaient plus à Ottawa, car la Chambre ne siégeait plus.

Le 22 décembre 2020, le conseiller à la sécurité nationale et au renseignement auprès du premier ministre (le « **CSNR** ») a réitéré la proposition dans une note de service au premier ministre. Il y proposait aussi une série de breffages classifiés pour les chefs des partis reconnus à la Chambre des communes, annexant à sa note des modèles de lettres offrant ces breffages aux chefs des partis d'opposition. J'y reviens plus loin dans ce chapitre.

La note de service de décembre 2020 a aussi fait l'objet de discussions au sein du personnel du CPM, qui appuyait toujours cette initiative. Des discussions se sont tenues en 2021 au sein du CPM portant sur la marche à suivre pour les breffages et sur la manière de les proposer aux chefs des partis d'opposition dans les lettres qui leur seraient transmises au sujet des breffages. Toutefois, la note n'a pas été présentée au premier ministre pour qu'il prenne une décision avant le déclenchement de l'élection de 2021, le 15 août 2021.

Ainsi, le premier ministre n'a jamais reçu la note de service de décembre 2019 ni celle de décembre 2020. Dans son témoignage, il a affirmé que ni le Bureau du Conseil privé (le « **BCP** ») ni le SCRS n'avaient pris de mesures pour porter ce dossier à son attention ni cherché à accorder la priorité aux deux notes de service. Katie Telford, cheffe de cabinet du premier ministre, a affirmé dans son témoignage que le greffier ou le CSNR portent les dossiers urgents directement à l'attention du premier ministre. À son avis, l'absence d'une telle démarche signifie que la fonction publique ne considérait pas l'initiative comme urgente à ce moment, en comparaison avec d'autres dossiers.

À mon avis, les breffages auraient dû aller de l'avant, et je trouve insatisfaisantes les explications avancées par le CPM pour justifier l'omission de s'assurer que les notes de service soient portées à l'attention du premier ministre. L'absence de suivi par le CPM ne peut pas et ne doit pas être justifiée par le simple fait que le greffier et le CSNR étaient en mesure de porter directement le dossier à l'attention du premier ministre.

### **2022-2024 : reprise des efforts pour offrir des breffages à tous les parlementaires**

En janvier 2022, il semble que l'idée de donner des breffages non classifiés à tous les parlementaires a refait surface au BCP. Une version provisoire d'une troisième note de service au premier ministre a été rédigée à cet effet au nom de la CSNR. Toutefois, la note n'a jamais été achevée ni acheminée. Jody Thomas, la CSNR d'alors, a affirmé dans son témoignage à la Commission qu'elle n'en avait aucun souvenir.

À l'été de 2023, le sergent d'armes a demandé au SCRS de breffer tous les caucus. David Vigneault, alors directeur du SCRS, a déclaré que le SCRS ne

pouvait pas agir ainsi unilatéralement. Les représentants du SCRS m'ont expliqué que même s'il avait pu donner des breffages non classifiés de lui-même, le SCRS souhaitait plutôt que ce soit l'ensemble de la communauté du renseignement qui offre des breffages aux parlementaires, parce que l'ingérence étrangère suscitait un intérêt accru.

Le SCRS et Sécurité publique Canada ont élaboré ensemble le contenu des breffages. En collaboration avec le Centre canadien pour la cybersécurité (le « CCC ») et la Gendarmerie royale du Canada (la « GRC »), Sécurité publique Canada a ensuite rédigé les documents de breffage.

Les représentants du SCRS m'ont dit qu'il n'avait pas été possible d'organiser les breffages aux caucus avant la pause estivale de la Chambre des communes. Les démarches ont repris à l'automne 2023.

Le 7 novembre 2023, dans une note de service, le personnel de Sécurité publique Canada a demandé au ministre Dominic LeBlanc<sup>20</sup> d'approuver les documents de breffage. Après avoir demandé à son personnel d'obtenir l'avis de l'Administration de la Chambre des communes, le ministre a donné son approbation.

Brian Clow, chef de cabinet adjoint au CPM, a affirmé dans son témoignage que lorsque le CPM a reçu le *Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada* du CPSNR au printemps 2024<sup>21</sup>, le personnel du CPM, le premier ministre et la CSNR ont eu des discussions au sujet des breffages et ont convenu qu'ils devaient avoir lieu, ce qui a été le cas.

Soit dit en passant, je me demande si les breffages auraient eu lieu si le CPSNR n'avait pas produit son rapport.

En juin 2024, les caucus ont assisté tour à tour au breffage, auquel participaient des représentants du SCRS, de Sécurité publique Canada, de la GRC et du CCC. Il comportait un exposé de 20 à 25 minutes suivi d'une période de questions. La formule « un caucus à la fois » visait à permettre aux parlementaires de poser leurs questions en l'absence des autres partis politiques. Il s'agissait d'un breffage à caractère général sur la nature de l'ingérence étrangère et les objectifs des États. Des exemples d'activités d'ingérence étaient aussi donnés. Les députés ont été invités à poser au sergent d'armes les questions qu'ils pourraient avoir subséquemment, ce qu'un des caucus a fait.

---

<sup>20</sup> M. LeBlanc a été ministre de la Sécurité publique de juillet 2023 à décembre 2024, soit tout au long de l'enquête et des audiences de la Commission. Le député David McGuinty, ancien président du Comité de parlementaires sur la sécurité nationale et le renseignement, a remplacé M. LeBlanc dans ses fonctions de ministre de la Sécurité publique en décembre 2024.

<sup>21</sup> La version classifiée du rapport spécial du CPSNR a été remise au premier ministre le 22 mars 2024. Brian Clow a indiqué que le CPM avait reçu le rapport en avril : Témoignage de Brian Clow, 15 octobre 2024, Transcription, vol. 34, p. 27.

Selon les fonctionnaires présents, il semble que les breffages aient été bien accueillis. Réceptifs, les députés semblaient avoir de nombreuses questions. De 50 % à 60 % des membres de chaque caucus y ont assisté.

Dans son témoignage, M. LeBlanc, ministre de la Sécurité publique à ce moment, a affirmé qu'il entendait demander à la Sécurité publique de déterminer, avec le sergent d'armes, si les partis souhaitaient un breffage mis à jour. Des collègues lui ont dit que les breffages étaient intéressants et leur avaient donné la possibilité de poser des questions à des experts non partisans.

### **Qui avait le pouvoir d'approuver la prestation des breffages non classifiés destinés à tous les parlementaires?**

D'après la preuve qui m'a été présentée, il y avait une part d'incertitude entourant l'identité de la personne qui pouvait décider de fournir des breffages non classifiés à tous les parlementaires, et celle qui devait donner son accord. Le SCRS donnait des BPS à certains parlementaires de son propre chef, mais s'il souhaitait s'adresser à l'ensemble des parlementaires, ses représentants demandaient d'abord l'approbation du premier ministre, puis celle du ministre de la Sécurité publique.

Dans son témoignage, l'ancien directeur du SCRS, M. Vigneault, a affirmé que le SCRS était autorisé à offrir des breffages aux députés sur une base individuelle, mais qu'il aurait été très inhabituel pour lui de s'adresser à un caucus entier. Une telle démarche exigerait du SCRS qu'il collabore avec des fonctionnaires parlementaires comme le sergent d'armes. Le SCRS ne prendrait pas l'initiative de breffer un caucus. Il faudrait que la Sécurité publique et le BCP donnent leur aval et que ce dernier soit impliqué compte tenu de la collaboration directe avec le Parlement que cela implique.

M. Clow a affirmé à la Commission que le SCRS a le pouvoir de breffer des députés à son gré sans avoir à demander l'autorisation du premier ministre. À son avis, il n'a jamais été nécessaire que le premier ministre donne suite à la note de service de 2019 ou à celle de 2020. Il a toutefois reconnu que le CPM n'a pas communiqué cette information au BCP et que, avec le recul, il aurait fallu qu'il le fasse. Je suis d'accord avec lui que cela aurait dû se faire, et je ne comprends pas pourquoi cela n'a pas été le cas. Il est difficile d'expliquer qu'une telle demande soit restée sans réponse pendant des années.

Cela dit, je m'interroge également quant à savoir pourquoi cette demande a cheminé vers le premier ministre plutôt que vers le ministre de la Sécurité publique. Même si le BCP devait être impliqué, il me paraît évident que, si le SCRS voulait lancer une campagne de breffages, l'étape intermédiaire logique aurait été de passer par le ministre dont il relève, soit le ministre de la Sécurité publique, plutôt que de s'adresser directement au premier ministre. Cela peut témoigner d'une certaine confusion à propos des rapports entre les différents intervenants et leurs responsabilités respectives relativement aux

enjeux liés à la lutte contre l'ingérence étrangère, et de la confusion quant aux rôles de Sécurité publique Canada et du BCP, dont j'ai traité au [chapitre 14](#).

Le ministre LeBlanc a reconnu dans son témoignage qu'habituellement, les fonctionnaires n'ont pas affaire aux caucus des partis d'opposition et que cela pourrait constituer pour eux une situation inhabituelle ou inconfortable. À son avis, les fonctionnaires ne lui ont pas demandé en novembre 2023 d'approuver la tenue de breffages en raison d'une exigence technique ou légale, mais plutôt parce que ces breffages sortaient du cadre de leurs activités habituelles.

La preuve du premier ministre indique que le pouvoir d'offrir des breffages aux parlementaires relève du Parlement et des agences de sécurité nationale et de renseignement, et non du gouvernement. À son avis, la tenue des breffages ne nécessitait pas son approbation. Il incombe au CSNR d'évaluer les besoins et de consulter les organismes de sécurité quant à la manière dont les breffages seront donnés et aux informations qui pourront être communiquées.

L'actuelle CSNR, Nathalie Drouin, a affirmé dans son témoignage qu'elle a le pouvoir, en collaboration avec le sergent d'armes, de demander que des breffages soient donnés, bien qu'elle ne les dirige pas nécessairement elle-même. Le coordonnateur national de la lutte contre l'ingérence étrangère à Sécurité publique Canada est maintenant chargé de coordonner les breffages non classifiés à l'intention des caucus de la Chambre des communes et des groupes du Sénat.

### **Incidence du retard dans la prestation de breffages aux caucus**

J'ai entendu des témoignages qui portaient sur l'incidence de ne pas avoir tenu des breffages à l'intention des caucus dès 2019.

Tout en reconnaissant qu'il aurait été préférable que les breffages non classifiés commencent avant le mois de juin 2024, plusieurs témoins ont expliqué qu'en fin de compte, ce retard pourrait n'avoir eu qu'une incidence limitée. En particulier, ils ont souligné le caractère général des informations communiquées lors de tels breffages, informations que les parlementaires auraient pu obtenir de plusieurs autres sources, y compris une lettre sur l'ingérence étrangère envoyée à tous les parlementaires en décembre 2020 par le ministre de la Sécurité publique de l'époque, Bill Blair.

En revanche, il est manifeste que différents intervenants gouvernementaux estimaient dès 2018 qu'il y avait lieu d'offrir aux parlementaires, plus régulièrement, des breffages portant sur l'ingérence étrangère. J'ai aussi entendu des témoignages de députés voulant que même des informations de base puissent leur être utiles, car elles leur permettent de prendre des mesures pour se protéger ou les amener à aller chercher des conseils et du soutien. Je comprends très bien ce point de vue et, comme je l'ai déjà mentionné, je ne vois pas pourquoi ces breffages ont été retardés si longtemps alors qu'ils étaient demandés.

## Besoin d'une plus grande transparence gouvernementale

Plusieurs députés qui ont témoigné ont déclaré qu'il était nécessaire que le gouvernement partage davantage d'informations. En d'autres termes, ils souhaitent une « politique de la lumière », qui s'éloigne d'une regrettable « culture du secret », l'idée étant qu'une plus grande transparence pourrait faire progresser la sécurité nationale. Par exemple, un député a indiqué que la divulgation stratégique d'informations pourrait contrer les menaces d'ingérence étrangère.

### 15.3 Prestation de breffages aux parlementaires dans le cadre de l'autorité du SCRS en matière de mesures de réduction de la menace

Depuis 2015, le SCRS a le pouvoir de prendre des mesures pour réduire les menaces à la sécurité du Canada dans certaines circonstances. Ces activités, désignées par le terme « mesures de réduction de la menace » (MRM), peuvent consister à fournir de l'information à des personnes. Le SCRS a utilisé les MRM pour informer des personnes sur l'ingérence étrangère. Je discute des MRM plus en détail au chapitre 13 (volume 3).

Les breffages de MRM peuvent être similaires aux breffages préventifs de sécurité (BPS). Toutefois, lors d'un breffage sur les MRM, le SCRS peut fournir de l'information plus précise, notamment de l'information classifiée, même si le destinataire n'a pas l'autorisation de sécurité nécessaire.

Si la MRM est évaluée comme présentant un risque élevé, le ministre de la Sécurité publique doit l'approuver avant qu'elle ne puisse être réalisée. Des exigences juridiques doivent également être satisfaites, notamment avoir un motif raisonnable de croire que l'activité pour laquelle la MRM est requise constitue une menace à la sécurité du Canada, et que la MRM est raisonnable et proportionnelle à la menace. Faire approuver une MRM pour divulguer de l'information classifiée à un parlementaire prend du temps et est fastidieux.

S'il suit ce processus et satisfait aux exigences, le SCRS pourrait utiliser son pouvoir en matière de MRM pour informer un chef de parti sur les activités d'ingérence étrangère qui ciblent les membres de son caucus.

Dans les autres chapitres de ce rapport, je parle de plusieurs exemples de MRM dans le cadre desquelles le SCRS a fourni de l'information classifiée aux parlementaires dans le but de réduire la menace d'ingérence étrangère.

Par exemple, au chapitre 11 (volume 3), j'aborde une MRM de 2021 que le SCRS a mise en œuvre en réponse aux activités d'ingérence étrangère

menées par l'Inde. Elle consistait à informer d'anciens députés et des députés actuels sur les activités d'ingérence étrangère de l'Inde au Canada.

Au [chapitre 14](#), je traite d'une MRM de mai 2023 par laquelle le député Michael Chong a été informé du renseignement dont disposait le SCRS quant à l'intérêt que lui portait la République populaire de Chine (la « **RPC** »). Cette MRM a eu lieu à la suite de fuites dans les médias à ce sujet.

Au chapitre 7 (volume 2), je réfère à une MRM que le SCRS a entreprise pour réduire la menace d'ingérence étrangère posée par le gouvernement du Pakistan dans la période précédant les élections de 2019. Cette MRM comprenait des rencontres avec des candidats et des élus pour discuter de l'activité préoccupante.

J'ai aussi entendu des preuves sur des MRM en cours ou que le SCRS a récemment envisagé de mettre en œuvre. L'une des MRM projetées prévoit la communication d'information classifiée à un député sur de l'ingérence étrangère potentielle qui le ciblerait.

## La directive ministérielle

Après les reportages dans les médias en 2023, que j'aborde au chapitre 1 (volume 2), le premier ministre a annoncé qu'il demanderait au ministre de la Sécurité publique d'émettre des directives au SCRS voulant que toute l'information sur des menaces à l'endroit de parlementaires ou de leur famille soit transmise aux paliers supérieurs, peu importe sa crédibilité ou sa fiabilité.

L'ancien directeur du SCRS, M. Vigneault a expliqué que des discussions avec Sécurité publique Canada ont alors commencé en vue de rédiger cette directive. Le SCRS était préoccupé par le contenu de l'ébauche de la directive, puisqu'elle exigeait qu'il divulgue *toute* l'information recueillie relativement aux menaces envers les parlementaires, peu importe si l'information est corroborée, vérifiée ou crédible. Même si l'on avait dit à M. Vigneault qu'il aurait la chance de parler de ses préoccupations au ministre, la Directive ministérielle sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires (la « **Directive ministérielle** ») a été émise le lendemain, avec le contenu que le SCRS trouvait préoccupant. Il va sans dire que la rapidité de cette réaction montre combien le ministre comprenait le besoin d'agir rapidement après les reportages dans les médias, ce qu'il a fait.

La Directive ministérielle ordonne au SCRS, lorsque possible, « d'informer les parlementaires des menaces à la sécurité du Canada qui les visent »<sup>22</sup>. Selon le SCRS, ceci reflète la priorité accordée par le gouvernement aux activités

---

<sup>22</sup> Directive ministérielle sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires, para. 3, CAN021931.

que le SCRS menait déjà au moyen d'outils comme les BPS et les MRM. La Directive ministérielle a vu le jour à un moment où les activités des acteurs de menace hostiles s'intensifiaient. Elle donne des précisions sur les attentes du gouvernement relativement à la manière dont le SCRS était censé intervenir auprès des parlementaires.

Le premier ministre m'a dit que la Directive ministérielle était une réponse directe à ce que M. Chong a soulevé pendant son breffage de mai 2023. Avec le recul, M. Trudeau s'est demandé si la Directive ministérielle constituait la politique appropriée, soulignant qu'elle avait été mise en place en réponse à des articles dans les médias et à des événements politiques, plutôt qu'à la suite d'une démarche délibérée et rigoureuse d'élaboration de politique. Plus particulièrement, il a estimé qu'elle obligeait les fonctionnaires à acheminer de l'information qui pouvait être relativement peu fiable ou de faible importance à un palier bien supérieur à ce qu'elle méritait. La Directive ministérielle était toutefois importante, pour démontrer que le gouvernement prenait la question au sérieux et que les menaces à l'égard des parlementaires ne seraient pas tolérées.

À la lumière de cette Directive ministérielle, le SCRS a identifié des députés, actuels et anciens, envers qui la RPC avait un intérêt marqué, notamment Jenny Kwan, Erin O'Toole et Kenny Chiu. Le SCRS a décidé de donner des breffages à ces députés, à l'aide de contenu qui leur était propre, en réponse à la Directive ministérielle.

## Le breffage sur les mesures de réduction de la menace donné à Erin O'Toole et le discours à la Chambre des communes

Le 26 mai 2023, à la suite de la Directive ministérielle, le SCRS a mené des MRM distinctes à l'intention des députés Jenny Kwan et Erin O'Toole.

Le SCRS a interprété la Directive ministérielle comme l'obligeant à informer les parlementaires de toutes les menaces qui les visaient, même si celles-ci n'étaient pas nécessairement crédibles, corroborées ou vérifiées. Bien que le SCRS n'ait pas communiqué de l'information qu'il savait non crédible, il a communiqué de l'information non vérifiée ou non corroborée.

Les représentants du SCRS ont témoigné que la rédaction des notes pour le breffage de M. O'Toole avait été très minutieuse afin de donner du contexte à l'information classifiée qui lui serait fournie. Il s'agissait notamment d'établir une distinction claire entre les cas où le SCRS disposait d'une base solide pour son évaluation et ceux où les informations n'étaient pas vérifiées ou corroborées.

Cependant, le SCRS a aussi reconnu que le breffage avait duré longtemps, avait été donné oralement, contenait beaucoup d'informations, et que M. O'Toole ne pouvait pas prendre de notes. La docteure Nicole Giles, sous-

ministre adjointe principale et directrice adjointe pour la politique et le partenariat stratégique au SCRS, a expliqué que lorsque M. O'Toole s'est rappelé ce breffage par la suite, il peut avoir eu de la difficulté à distinguer les informations qui avaient été vérifiées ou corroborées des informations qui ne l'avaient pas été.

M. O'Toole a témoigné que le breffage ne lui a pas donné le sentiment d'être mieux préparé à affronter la menace d'ingérence étrangère. Il lui a donné une meilleure idée du type de renseignement qui était recueilli, mais il ne lui a pas indiqué de mesures de précaution ou de meilleures pratiques à adopter.

Le 30 mai 2023, M. O'Toole s'est exprimé à la Chambre des communes et a révélé ce qui lui avait été dit lors du breffage de MRM. Il dit l'avoir fait pour officialiser ce qu'il percevait être des violations à sa capacité de s'acquitter de ses tâches comme parlementaire, de grandes lacunes dans le système et des risques en matière d'ingérence étrangère auxquels font face les parlementaires. M. O'Toole estime que puisqu'il s'est exprimé devant la Chambre des communes, son discours était protégé par le privilège parlementaire.

M. O'Toole m'a dit avoir été très prudent pour que son discours demeure très général. Il a affirmé qu'il était important pour lui de ne pas révéler les sources d'information du renseignement, et qu'il avait demandé des conseils juridiques à un avocat d'expérience en matière de sécurité nationale avant de livrer son discours. M. O'Toole voyait ce discours comme un moyen responsable de communiquer ses préoccupations de façon officielle et de faire preuve d'ouverture tout en protégeant l'information classifiée.

Malgré cela, le SCRS a conclu que M. O'Toole, lors de son discours, a divulgué de l'information classifiée, notamment de l'information non vérifiée, sans avoir les autorisations nécessaires. Après le discours, cela a été communiqué au premier ministre dans une note de service de la conseillère à la sécurité nationale et au renseignement auprès du premier ministre (CSNR). La note de service précisait que l'information donnée par le SCRS à M. O'Toole avait été mal interprétée ou exagérée dans certaines parties du discours. La note de service comprenait aussi un tableau comparant les déclarations de M. O'Toole à la Chambre et l'information qu'il avait reçue du SCRS. Ce tableau reposait sur un examen de sécurité nationale mené par le SCRS après le discours pour établir le préjudice potentiel à la sécurité nationale que la divulgation de l'information classifiée avait pu entraîner.

Je souligne qu'en fin de compte, le gouvernement a fourni à la Commission une version de cette note de service qui peut être divulguée publiquement, mais cette version n'était pas à ma disposition quand M. O'Toole a témoigné devant moi. Par conséquent, il n'a pas pu voir le tableau ou y réagir. Cependant, lors de son témoignage, il a soutenu ne pas avoir mal interprété ou exagéré quoi que ce soit.

M. Vigneault considère certains des commentaires publics de M. O'Toole inexacts, quoiqu'il lui accorde le bénéfice du doute et qu'il reconnaît que

M. O'Toole ne pouvait pas prendre de notes pendant le breffage. Des témoins du SCRS ont eu le sentiment que M. O'Toole avait compris le renseignement et l'information qui lui avaient été présentés, mais qu'il n'avait peut-être pas compris toute l'information contextuelle fournie. Le premier ministre Trudeau a trouvé le discours de M. O'Toole frustrant, étant d'avis que M. O'Toole avait déformé ce qu'on lui avait dit et donné l'impression que le renseignement était plus fiable qu'il ne l'était.

Lorsque nous lui avons demandé s'il était possible que M. O'Toole ait fait référence à certains reportages dans les médias plutôt qu'à l'information que lui avait fournie le SCRS, Jody Thomas, qui occupait le poste de CSNR à l'époque, a dit qu'elle croyait qu'au moins une partie de ses propos étaient tirés de ce que le SCRS lui avait dit.

## Le Protocole de gouvernance

À la suite du discours de M. O'Toole, en mai 2023, Sécurité publique Canada et le SCRS ont décidé de suspendre les breffages dans le cadre de la Directive ministérielle pour plutôt élaborer un Protocole de gouvernance (le « **Protocole** ») qui offrirait à la communauté de la sécurité nationale et du renseignement l'occasion de revoir les messages véhiculés dans les breffages et le renseignement sur lequel ceux-ci reposent, avant que les breffages aient lieu. Bien que la Directive ministérielle soit destinée au SCRS, celui-ci a dit qu'il avait besoin que toute la communauté du renseignement pense stratégiquement à l'information à fournir lors des breffages. Le Protocole était destiné à corriger l'exigence de divulguer *toute* l'information recueillie relativement aux menaces qui visent les parlementaires, qu'elle soit ou non corroborée, vérifiée ou crédible.

Marie-Hélène Chayer, du Bureau du Conseil privé (BCP), et secrétaire adjointe au Cabinet pour le Conseil de la sécurité nationale, a dit qu'il appartenait à la communauté de la sécurité nationale de trouver la bonne façon d'expliquer l'information aux parlementaires. Par exemple, la signification de certains termes n'était pas toujours claire. Le Protocole comprend maintenant un processus de gouvernance impliquant plusieurs comités et différentes rondes de consultations dont le but est d'en arriver à un produit aussi utile que possible.

Dans le cadre du Protocole, le SCRS prépare une trousse de breffage qui contient de l'information, dont du renseignement classifié, sur la menace spécifique qui vise les parlementaires, ainsi que les principaux messages que les représentants du SCRS utiliseront pour les informer. Les membres du Comité tactique des sous-ministres adjoints sur les opérations de sécurité nationale examinent le renseignement et travaillent sur la trousse de breffage. Elle est ensuite envoyée au Comité des sous-ministres sur la gestion de l'intervention du renseignement (le « **CSMGIR** ») pour consultation. Le Protocole ne précise pas les délais pour toutes ces étapes. Selon moi, il le

devrait, parce que le temps peut être compté dans les circonstances envisagées par le Protocole.

Dans le cadre de ce processus, la communauté de la sécurité nationale et du renseignement peut donner des conseils au directeur du SCRS, répondre aux préoccupations relatives aux principaux messages et coordonner une approche pour informer les ministres. Les témoins du BCP et du SCRS ont dit que le Protocole a permis d'assurer que les breffages reflètent l'ensemble plus large d'informations à la disposition du gouvernement et la coordination entre les différents ministères concernés pour l'élaboration du contenu approprié.

J'ai entendu lors des témoignages que de vifs débats ont eu lieu jusqu'à maintenant au sein des comités qui participent à ce processus, que ces débats ont mis en lumière les perspectives des différents ministères et qu'ils ont aidé à veiller à ce que l'information soit communiquée efficacement aux personnes qui ne font pas partie de la communauté du renseignement. Dans certains cas, ces débats ont mené à des précisions dans le texte des breffages.

Le Protocole reconnaît aussi la possibilité que des conflits d'intérêts surviennent pendant le processus de consultation, et que parfois, les participants puissent avoir un intérêt dans le résultat. Il prévoit :

---

Modification relative aux conflits d'intérêts : les fonctionnaires, le personnel exempté et les ministres œuvrent au Parlement et en marge de celui-ci. Il se peut qu'une personne qui participe à ce processus ait un intérêt dans son résultat. De temps à autre, des modifications au protocole pourraient être nécessaires pour limiter la diffusion d'un document ou pour modifier une étape dans le but d'éviter un conflit d'intérêts réel ou apparent. Si le SCRS relève une préoccupation de ce genre, il doit la soulever auprès de Sécurité publique Canada pour convenir avec lui d'un processus révisé aux fins du cas précis en question<sup>23</sup>.

---

Le SCRS a dit que ce point illustre bien les défis qu'il doit surmonter dans ses enquêtes concernant la sphère politique et dans ses interactions avec celle-ci. La sphère politique constitue un groupe unique, dont les membres se connaissent bien. Cette partie du Protocole pourrait potentiellement permettre aux membres du CSMGIR de ne pas conseiller leur ministre, comme le prévoit le Protocole, dans la mesure où le conseiller pourrait placer le ministre dans une situation de conflit d'intérêts potentiel.

Même si son approbation n'était pas requise, le ministre LeBlanc a reçu le Protocole pour approbation. Il l'a approuvé le 19 septembre 2023.

---

<sup>23</sup> Mise à jour – Breffages à venir à l'intention des parlementaires sur les mesures de réduction de la menace (13 septembre 2023), p. 15, CAN028170\_0001.

Dès que le Protocole a été achevé, le SCRS a recommencé à divulguer de l'information aux parlementaires, tout d'abord avec l'ancien député Kenny Chiu, en septembre 2023.

## Considérations particulières pour fournir de l'information classifiée aux parlementaires

Fournir de l'information classifiée aux parlementaires représente un enjeu très délicat pour le SCRS, étant donné que les parlementaires peuvent choisir de recourir au privilège parlementaire pour divulguer de l'information. Le SCRS m'a dit que le gouvernement cherche actuellement à déterminer les meilleurs moyens d'aborder l'enjeu de ce qui doit être fait lorsque le risque que des informations classifiées soient divulguées est trop important.

La Directive ministérielle exige du SCRS qu'il prenne des mesures, notamment des mesures de réduction de la menace (MRM), quand il est mis au courant d'une menace. Lorsqu'il doit décider des mesures à prendre, le SCRS considère la nature de l'information, sa source et le risque d'exposer la source. Le SCRS évalue aussi si d'autres options qu'une MRM, comme un breffage préventif de sécurité (BPS), pourraient permettre d'atteindre le même résultat sans divulguer de l'information classifiée. D'autres partenaires de la communauté de la sécurité nationale et du renseignement peuvent aider à trouver d'autres options lorsque les risques d'utiliser de l'information classifiée sont trop élevés.

Michelle Tessier, ancienne directrice adjointe des opérations du SCRS, a fait remarquer que cet enjeu montrait le besoin d'augmenter la sensibilisation à l'égard du processus de collecte du renseignement. Elle a exprimé le souhait que les personnes, en comprenant mieux les conséquences de révéler de l'information classifiée, seraient moins susceptibles d'en exposer la source. Mme Tessier a dit qu'il était également important d'assurer une meilleure compréhension des limites intrinsèques du renseignement. Cependant, M. Vigneault a souligné que la communication d'information aux parlementaires est un sujet très délicat pour le SCRS puisque le SCRS doit toujours tenir compte de leur privilège parlementaire.

## 15.4 Une préoccupation concernant la communication d'information aux parlementaires : la cybercampagne du *Advanced Persistent Threat 31* qui ciblait les membres de l'Alliance interparlementaire sur la Chine

### Courriels aux membres de l'Alliance interparlementaire sur la Chine en 2021

La preuve présentée devant moi montre que la Menace persistante avancée 31 (la *Advanced Persistent Threat 31*, ou l'« **APT 31** ») est un regroupement de cyberacteurs malveillants qui travaillent pour le compte du ministère de la Sécurité d'État de la République populaire de Chine (RPC). Ce groupe se spécialise dans l'espionnage et l'ingérence étrangère de manière plus générale. Il constitue une menace de cyberespionnage omniprésente qui cible les gouvernements de nombreux pays occidentaux, y compris le Canada. Il a des intérêts de longue date et continus à l'égard des représentants du gouvernement et des parlementaires canadiens.

En janvier 2021, l'APT 31 a mené une campagne de courriels qui ciblait des membres de l'Alliance interparlementaire sur la Chine (la *Inter-Parliamentary Alliance on China*, ou l'« **IPAC** »), une organisation de parlementaires du monde entier qui partagent l'opinion selon laquelle la RPC représente une menace à laquelle il faut s'opposer avec des moyens plus robustes et qui tiennent davantage compte des risques. L'APT 31 a envoyé des courriels d'hameçonnage ciblé aux membres de l'IPAC dans plusieurs pays, y compris au Canada, qui intégraient des liens de suivi. L'idée étant la suivante : en ouvrant les courriels, les destinataires permettaient à l'APT 31 d'utiliser le lien de suivi pour confirmer la validité de l'adresse courriel utilisée et recueillir certaines informations de base, telle que l'adresse IP de l'appareil. Ce genre de courriel est parfois le précurseur d'une activité pouvant subséquemment être menée par un acteur menaçant. Toutefois, un tel courriel ne peut pas compromettre une adresse courriel ou un dispositif électronique à lui seul.

Plusieurs parlementaires canadiens sont membres de l'IPAC et ont reçu des courriels de l'APT 31. Les courriels ont été envoyés à la fois aux adresses courriel parlementaires et personnelles.

Comme je l'explique plus bas, les parlementaires qui ont été ciblés par cette campagne de courriels en ont appris l'existence au printemps de 2024. Cet incident, et l'absence d'avis aux parlementaires, soulève des questions quant à savoir si ceux qui ont été ciblés auraient dû en être informés, et dans l'affirmative, qui était responsable de les informer.

## Détection de la campagne de courriels de l'APT 31 et mesures prises à l'encontre de celle-ci

Il est important d'expliquer la manière dont le gouvernement a répondu à la menace avant d'aborder les questions à savoir comment les parlementaires ont été mis au courant de la campagne de l'APT 31 et si le gouvernement aurait dû les informer de celle-ci plus tôt.

Le 22 janvier 2021, le Centre canadien pour la cybersécurité (le « **CCC** ») du Centre de la sécurité des télécommunications (le « **CST** ») a reçu une information d'un partenaire de confiance concernant une campagne de courriels visant des parlementaires. Le CCC ne savait pas quels parlementaires étaient ciblés. L'information dont il disposait consistait en des détails techniques liés au trafic sur le réseau.

La même journée, le CCC a envoyé par courriel un rapport de cyberévénement non classifié aux fonctionnaires des technologies de l'information de la Chambre des communes (les « **TI de la Chambre** »). Le rapport mentionnait que des courriels contenant des liens de suivi avaient été envoyés à des comptes courriel parlementaires. Il fournissait aussi de l'information technique et recommandait que les TI de la Chambre prennent certaines mesures à cet égard. Les instructions contenues dans le rapport mentionnaient que les TI de la Chambre devaient obtenir l'autorisation du CCC pour transmettre cette information à d'autres personnes.

Bien que le CCC ait été au courant de l'implication de l'APT 31, le rapport n'attribuait pas les activités à ce groupe étant donné qu'il s'agissait d'une information classifiée. La priorité du CCC était de transmettre des informations aux TI de la Chambre pour atténuer l'incident de leur côté. Pour permettre au CCC de transmettre rapidement l'information technique initiale aux TI de la Chambre, le rapport a été envoyé à un niveau non classifié.

Les TI de la Chambre ont mené une enquête et ont identifié huit députés ayant été ciblés. Elles ont communiqué avec eux pour leur demander s'ils avaient reçu les courriels. Aucun des députés n'a signalé les avoir reçus. Les TI de la Chambre ont par la suite appris que les courriels avaient été mis en quarantaine par le système et n'avaient pas atteint leurs cibles.

Les TI de la Chambre ont également avisé la Direction des services d'information du Sénat (les « **TI du Sénat** »). Contrairement à celui de la Chambre des communes, le système du Sénat n'avait pas mis tous les courriels en quarantaine et quelques-uns se sont retrouvés dans les boîtes courriel des sénateurs. Les TI du Sénat se sont assurés que ces courriels soient détruits. En fin de compte, les TI du Sénat ont conclu que l'attaque avait été un échec puisque les courriels ont été mis en quarantaine ou supprimés avant d'être ouverts.

Alors que la priorité initiale était d'atténuer le risque, il était important pour le CCC de sensibiliser et d'informer les TI de la Chambre au sujet de l'identité de l'auteur de menace derrière cette campagne de courriels. Ainsi, le

17 février 2021, le CCC leur a envoyé un deuxième rapport mentionnant que des acteurs sophistiqués menaient des activités de reconnaissance sur des réseaux de dispositifs connus pour se connecter au réseau virtuel privé de la Chambre des communes. Des représentants du CCC et du SCRS ont rencontré les TI de la Chambre afin de leur présenter un exposé de niveau « Secret » la même journée. Ils ont avisé les TI de la Chambre qu'ils soupçonnaient l'APT 31 d'être responsable de la campagne de courriels et leur ont fourni de l'information au sujet des liens suspectés entre l'APT 31 et la RPC, de ses tactiques et de ses cibles antérieures. L'organisation de cette réunion a pris du temps en raison des répercussions de la pandémie sur l'organisation et la tenue de réunions classifiées.

Ni les TI de la Chambre ni le CCC n'a informé les TI du Sénat de l'implication de l'APT 31 à ce moment-là. Contrairement à la Chambre des communes, le Sénat n'avait pas de protocole d'entente établi avec le CCC à cette époque. Les TI du Sénat n'ont été mises au courant de la participation de l'APT 31 qu'en avril 2024 par les médias, puis en mai ou juin de la même année par les représentants de la Chambre des communes. Lors de leurs témoignages, les représentants du Sénat ont affirmé que le fait de savoir que la campagne était liée à un État étranger n'aurait pas changé les mesures qui ont été prises.

Immédiatement après la réunion du 17 février 2021, des fonctionnaires du CCC ont soulevé des préoccupations aux dirigeants du CCC selon lesquelles les TI de la Chambre n'avaient pas reçu suffisamment d'information pour saisir l'importance de la menace. D'autres réunions ont eu lieu entre le SCRS, le CCC et les TI de la Chambre les 19 et 22 février 2021 afin de discuter de l'ampleur de l'incident. Dans le cadre de ces réunions, les TI de la Chambre ont fourni au SCRS et au CCC des données d'analyse.

Il y a eu d'autres communications entre les TI de la Chambre, le CCC et le SCRS au cours des jours qui ont suivi. Dans un cas, le CCC a demandé des copies des courriels en question aux TI de la Chambre. Les TI de la Chambre n'ont pas fourni les courriels, car ils n'avaient pas obtenu le consentement des députés pour le faire. Les TI de la Chambre disent ne pas avoir demandé ce consentement puisque les courriels ne sont jamais parvenus aux députés.

Au cours des jours suivants, les TI de la Chambre ont identifié un total de 14 députés dont les boîtes courriel avaient été ciblées. Les TI de la Chambre ont estimé que certains députés ont possiblement reçu des courriels dans leur boîte courriel personnelle. Deux boîtes courriel du Sénat ont également été identifiées. Les représentants du Sénat m'ont fait savoir que les sénateurs qui avaient reçu les courriels les avaient supprimés. Le 1<sup>er</sup> mars 2021, les TI de la Chambre ont avisé le CCC qu'au moins une adresse IP relevée dans le rapport du CCC était associée au réseau domiciliaire d'un utilisateur du réseau de la Chambre des communes.

Quelques semaines plus tard, le CCC a détecté qu'un dispositif se trouvant à la Chambre des communes était connecté à une infrastructure soupçonnée d'être malveillante et a envoyé aux TI de la Chambre un rapport demandant des informations supplémentaires afin de pouvoir évaluer la situation.

Cependant, les TI de la Chambre ont déterminé que le dispositif concerné en était un personnel situé dans une partie du réseau de la Chambre des communes destiné aux appareils personnels, et que l'appareil n'avait pas été détecté à l'intérieur du réseau du bureau. Pour cette raison, du point de vue des TI de la Chambre, ce dispositif ne constituait pas une menace à l'infrastructure parlementaire.

Le 3 juin 2021, le SCRS a informé les TI de la Chambre que les parlementaires ciblés étaient tous des membres de l'IPAC et a remis une liste complète des parlementaires canadiens qui en étaient membres. Un an plus tard, en juin 2022, le *Federal Bureau of Investigation* (le « **FBI** ») des États-Unis a appris que l'APT 31 ciblait des membres de l'IPAC et a avisé les gouvernements dont les législateurs avaient été touchés, y compris au Canada. Les représentants de la Chambre des communes n'étaient pas au courant que le FBI avait communiqué cette information au gouvernement.

## Manière dont les parlementaires ont eu connaissance de la campagne de l'APT 31

Les parlementaires ont eu connaissance de la campagne de l'APT 31 pour la première fois en avril 2024, bien qu'au moins un ancien député ciblé n'ait été mis au courant de la situation qu'en mai 2024.

Le 25 mars 2024, la mise sous scellés d'un chef d'accusation aux États-Unis visant plusieurs membres de l'APT 31 et faisant référence à la campagne ciblant l'IPAC a été levée. Le secrétariat de l'IPAC, situé à Londres, a pris connaissance du chef d'accusation et a rencontré le FBI à la mi-avril. Le FBI a examiné la liste de distribution et a relevé 122 adresses courriel qu'il croyait avoir été ciblées par l'APT 31.

L'IPAC a des coprésidents nationaux en poste dans chaque pays où il exerce ses activités. Au Canada, il s'agit de Garnett Genuis, député conservateur, et de John McKay, député libéral. La fin de semaine du 19 avril 2024, le directeur général de l'IPAC a téléphoné à M. Genuis et lui a donné un breffage sur l'information obtenue du FBI. Durant cet appel, M. Genuis a appris que c'était sa boîte courriel personnelle qui avait été ciblée. Le 24 avril 2024, le directeur général de l'IPAC et M. Genuis ont discuté une deuxième fois par téléphone, cette fois-ci avec M. McKay. Plus tard ce jour-là, le directeur général et les coprésidents canadiens de l'IPAC ont donné un breffage par téléphone aux membres canadiens de l'IPAC. Le directeur général a aussi envoyé un courriel fournissant de l'information concernant l'attaque à tous les parlementaires touchés.

Le 29 avril 2024, M. Genuis a soulevé une question de privilège à la Chambre des communes au sujet de la campagne de l'APT 31 et du fait que des fonctionnaires n'avaient pas avisé les parlementaires. Le président a statué qu'il y avait à première vue une atteinte au privilège et a renvoyé la question au Comité permanent de la procédure et des affaires de la Chambre (voir le chapitre 2, volume 2).

## Nature de la menace

Dans la mesure où le CCC a détecté la présence d'acteurs menaçants de la RPC, comme l'APT 31, sur des réseaux canadiens, leurs activités correspondent à de l'espionnage et à de la collecte de renseignement. Le cyberespionnage est utilisé pour recueillir de l'information qui permettra de retirer un avantage économique et diplomatique. Par conséquent, à moins d'une raison précise de croire que des cyberacteurs comme l'APT 31 accèdent à un réseau en vue d'une attaque, le CST a, par le passé, évalué ce type d'activité sous l'angle de l'espionnage.

De même, Affaires mondiales Canada (« **AMC** ») perçoit les cyberactivités de l'APT 31 comme étant de l'espionnage. La légalité de l'espionnage est une question juridique complexe allant au-delà du mandat de la Commission. Pour les fins de ce rapport, il suffit de mentionner que, selon certains, l'espionnage n'est pas forcément contraire aux normes internationales.

Bien que l'espionnage ne constitue pas en soi de l'ingérence étrangère, un cyberacteur pourrait se servir de l'information obtenue grâce à de l'espionnage pour se livrer ultérieurement à des activités d'ingérence étrangère.

En novembre 2021, le SCRS a conclu que la campagne avait été un échec.

Déterminer l'intention derrière ce type d'activité en ligne peut être difficile. Appelée à commenter un courriel de 2023 d'un analyste du CCC, Alia Tayyeb, cheffe adjointe du SIGINT, a opiné que des adversaires étrangers peuvent retirer un avantage légitime en matière de renseignement lorsqu'ils recueillent les adresses courriel de députés. Dans ce cas spécifique, rien n'indiquait que la cyberactivité avait été menée dans le but précis de s'ingérer dans les processus démocratiques. Toutefois, un courriel malveillant peut être utilisé pour établir un point d'appui sur un réseau.

De même, le SCRS a évalué que l'intention avait pu être de se familiariser avec le travail qu'effectue l'IPAC, permettant ainsi à la RPC de manœuvrer pour réagir à ses annonces futures si elles devaient être critiques à son égard. Il est possible que l'intention ait aussi été de recueillir de l'information sur des membres de l'IPAC afin de les mettre dans l'embarras ou de les discréditer.

## Les parlementaires auraient-ils dû être avisés?

J'ai entendu diverses opinions à savoir si les parlementaires auraient dû être avisés de la campagne de l'APT 31.

En tant que cibles de la campagne de courriels, M. McKay et M. Genuis ont estimé qu'ils auraient dû être avisés lorsqu'elle a eu lieu, mais ils n'étaient pas d'accord quant à qui avait la responsabilité de le faire. Selon M. McKay, le responsable était la Chambre des communes. M. Genuis a fait valoir que cette responsabilité relevait du gouvernement.

Caroline Xavier, cheffe du CST, a témoigné que si la campagne de l'APT 31 se produisait aujourd'hui, des mesures seraient « assurément » prises pour offrir un breffage aux parlementaires ciblés, et ce, en raison de la Directive ministérielle maintenant en vigueur. Les breffages seraient offerts par le SCRS ou par la Chambre des communes. Tant Nathalie Drouin, la CSNR, que la cheffe du CST considèrent la campagne de l'APT 31 comme étant le type d'activité visée par la Directive ministérielle. Ce point de vue donne à penser que la campagne de l'APT 31 constitue un type de menace qui devrait faire l'objet d'un breffage à l'intention des parlementaires.

Bo Basler, du SCRS, m'a dit que, si une campagne similaire avait lieu aujourd'hui, il faudrait probablement que le SCRS, le CCC et les fonctionnaires de la Chambre des communes discutent de la question pour déterminer si les parlementaires devraient en être avisés.

Cependant, les TI de la Chambre avaient un point de vue légèrement différent. Les témoins des TI de la Chambre ont soutenu que des centaines de millions de tentatives d'attaques ont lieu au cours d'une année. Il serait impossible d'un point de vue opérationnel de donner un breffage pour chacune d'elles. Les TI de la Chambre n'ont pas informé les députés de l'APT 31 parce que la campagne avait été un échec : le groupe n'ayant jamais atteint ses cibles. Un breffage serait généralement donné si une cyberattaque avait une incidence sur les dispositifs ou les informations d'un député.

Tous les sénateurs ciblés ont été informés en janvier ou février 2021, mais les TI du Sénat ont dû attendre jusqu'en avril ou mai 2024 pour apprendre que la campagne était attribuée à l'APT 31. Comme je l'ai mentionné plus haut, les TI du Sénat ont reconnu qu'elles n'auraient pas pris de mesures différentes s'ils avaient su que l'APT 31 en était responsable.

## Qui a la responsabilité d'aviser les parlementaires d'une cybermenace?

L'incident relatif à l'APT 31 renvoie à la question plus générale de savoir qui était responsable d'informer les parlementaires de ce type de cybermenace et à qui incombe cette responsabilité à l'heure actuelle. La preuve montre qu'au moment de la campagne de courriels, il n'était pas facile de savoir, dans la mesure où ils auraient dû être breffés, qui était responsable d'offrir un breffage aux parlementaires ciblés.

M. Vigneault, directeur du SCRS à ce moment-là, a affirmé que, malgré le fait que le SCRS ait participé à de nombreuses réunions avec les TI de la Chambre, le CCC était l'organisme responsable à l'échelle du gouvernement.

Toutefois, M<sup>me</sup> Xavier a affirmé dans son témoignage que, pendant l'incident, elle s'attendait à ce que les TI de la Chambre continuent de collaborer avec le CCC pour réagir à la campagne. Elle a fait valoir que le CCC disposait seulement d'informations quant aux adresses IP ciblées. Seules les TI de la

Chambre pouvaient déterminer quels parlementaires avaient été visés. Les TI de la Chambre ont fait remarquer que le CCC ne leur avait pas conseillé d'aviser les parlementaires.

Selon plusieurs témoins, cette question ne se soulèverait pas aujourd'hui puisque, si le CST obtenait du renseignement concernant une menace visant des parlementaires, la Directive ministérielle et le Protocole de gouvernance seraient suivis. D'ailleurs, au début de septembre 2023, M<sup>me</sup> Xavier a formulé une directive décrivant ses attentes selon lesquelles le CST doit aider le SCRS à exercer ses fonctions prévues dans la Directive ministérielle.

Les témoins du CST m'ont dit que le CST ne serait pas susceptible d'offrir un breffage direct à des individus en vertu de la Directive ministérielle. Les témoignages ont révélé que les clients du CST ont le pouvoir de déterminer quelles mesures prendre de leur propre chef, y compris offrir un breffage à un parlementaire. Le CST communique normalement de l'information classifiée aux fournisseurs de services de TI qui possèdent une autorisation de sécurité ou fournit de conseils sur les mesures à prendre.

Il pourrait être envisageable d'accorder au CST ainsi qu'à d'autres agences et ministères des pouvoirs supplémentaires leur permettant de communiquer avec les parlementaires. On m'a informée qu'une discussion était en cours au Comité des sous-ministres sur les interventions en matière de renseignement (voir le chapitre 11, volume 3) pour savoir si la Directive ministérielle, au lieu de ne s'appliquer qu'au SCRS, devrait s'étendre à l'ensemble de la communauté de la sécurité nationale et du renseignement. Bien qu'il soit évident que le SCRS a le pouvoir de communiquer avec les parlementaires au sujet de menaces, il est moins évident de savoir si des ministères peuvent communiquer directement avec ces derniers. Quoi qu'il en soit, le SCRS m'a informée que, si le CST l'informe d'une menace, il s'assurera qu'une discussion ait lieu afin de déterminer si les parlementaires doivent en être informés et établir l'entité qui devra le faire.

## 15.5 Communication d'informations par le Bureau du Conseil privé

J'ai aussi entendu des témoignages selon lesquels, outre les breffages préventifs de sécurité (BPS) ou les breffages donnés par le SCRS en vertu de son pouvoir de prendre des mesures de réduction de la menace (MRM), il arrive parfois que des fonctionnaires du Bureau du conseil privé (BCP) rencontrent des députés afin de les informer sur la menace d'ingérence étrangère. Michael MacDonald, ancien secrétaire-adjoint du Cabinet au BCP pour la sécurité et le renseignement, a affirmé dans son témoignage que, bien que les MRM du SCRS exercent une certaine influence en raison de la gravité que la plupart des personnes ressentent lorsqu'ils interagissent avec le

SCRS, le BCP peut aussi discuter d’ingérence étrangère avec les parlementaires. Les fonctionnaires adaptent leur stratégie selon la situation.

Par exemple, les témoignages ont révélé que le cabinet du premier ministre (CPM) a demandé à la CSNR de rencontrer un député afin de discuter de divers sujets, y compris les façons dont les États étrangers peuvent tenter de manipuler des parlementaires. Bien que la CSNR n’ait pas le pouvoir de donner un breffage défensif ou de mettre en œuvre une MRM, le CPM a estimé que cette approche pouvait s’avérer utile. La CSNR a expliqué qu’elle était très limitée quant aux informations qu’elle pouvait communiquer. Selon ma compréhension, la CSNR ne pouvait pas inclure d’informations classifiées ou de détails spécifiques.

## 15.6 Communication d’informations par Affaires mondiales Canada

Il est ressorti des témoignages qu’AMC peut également communiquer de l’information à propos d’ingérence étrangère soupçonnée aux députés dans certains cas précis. La preuve dont je dispose décrit deux événements survenus en 2023 où de l’information obtenue grâce à son Mécanisme de réponse rapide (le « **MRR du Canada** ») a été communiquée à des parlementaires.

### Désinformation ciblant M. Chong

Comme je l’explique au [chapitre 14](#), à l’été 2023, le MRR du Canada a détecté qu’une campagne avait répandu de fausses informations au sujet du contexte identitaire, des positions politiques et du patrimoine familial de Michael Chong. Le MRR du Canada a conclu avec un niveau de confiance élevé que la campagne était liée à la République populaire de Chine (RPC) et ont estimé qu’entre deux et cinq millions d’utilisateurs de WeChat avaient vu le contenu faux ou trompeur. Après que le Comité des sous-ministres sur la gestion de l’intervention du renseignement (CSMGIR) avait discuté de la question, le BCP et le SCRS ont donné un breffage au premier ministre à propos de cette campagne.

Le 9 août 2023, les hauts fonctionnaires d’AMC ont donné un breffage à M. Chong au sujet de la désinformation le ciblant. Des informations concernant la campagne ont aussi été divulguées publiquement.

M. Chong m’a informée qu’il s’était senti protégé et rassuré à la suite de la décision du gouvernement de divulguer les informations. Selon lui, il s’agissait d’un bon exemple des façons dont les choses devraient être rendues publiques. Il aurait toutefois aimé que le gouvernement agisse plus rapidement.

## Campagne de camouflage de pourriels

En septembre 2023, le MRR du Canada a été informé par l'un de ses homologues étrangers qu'un réseau de robots affilié à la RPC avait publié des milliers de commentaires sur les comptes Facebook et Twitter de plus de 40 députés<sup>24</sup>. Les commentaires affirmaient que Xin Liu, une figure critique bien connue du Parti communiste chinois<sup>25</sup>, avait accusé ces députés de violations criminelles et éthiques, notamment de « corruption politique », de « scandales sexuels » impliquant des personnes mineures et de corruption d'électeurs durant une campagne électorale<sup>26</sup>. Souscrivant à l'évaluation faite par son homologue étranger, le MRR du Canada a convenu que cette activité inhabituelle constituait une campagne de « camouflage de pourriels<sup>27</sup> » menée par un réseau de robots probablement contrôlé par le ministère chinois de la Sécurité publique, un organisme d'application de la loi de la RPC.

Le MRR du Canada a estimé qu'un nombre extrêmement restreint de Canadiennes et de Canadiens avaient pris connaissance des messages et que la campagne avait donc vraisemblablement eu peu d'effet sur les députés. En revanche, le MRR du Canada a estimé que les répercussions pour M. Liu étaient vraisemblablement très importantes. Le MRR du Canada a fait rapport sur la campagne de camouflage de pourriels le 15 septembre 2023. Je mentionne également cette campagne de camouflage de pourriels au chapitre 10 (volume 3), afin d'illustrer la manière dont la désinformation peut être une puissante tactique d'ingérence étrangère.

Lors de sa réunion du 6 octobre 2023, le CSMGIR a discuté de la question et a approuvé une trousse de breffage destinée aux députés. Le 23 octobre 2023, AMC a transmis un avis à l'ensemble des députés et envoyé un courriel à tous les députés visés par la campagne de camouflage de pourriels.

---

<sup>24</sup> Les cibles comprenaient le premier ministre, le chef de l'opposition, plusieurs membres du Cabinet et des députés d'arrière-ban de l'ensemble des partis et répartis dans de multiples régions géographiques du Canada.

<sup>25</sup> Xin Liu est un commentateur vidéo de Vancouver qui a participé au mouvement démocratique de la Chine en 1989. Il alimente un blog vidéo populaire sur YouTube et compte un grand bassin d'abonnés sur Twitter/X. Il critique fréquemment les pratiques de gouvernance du secrétaire général Xi Jinping du Parti communiste chinois.

<sup>26</sup> CAN025903\_001, p. 1.

<sup>27</sup> Le camouflage de pourriels consiste à diffuser du contenu et de la propagande de façon clandestine et trompeuse sous forme de pourriels, parmi d'autres contenus plus bénins et susceptibles d'intéresser les gens de par son côté accessible et humain.

## 15.7 Informer les représentants des partis politiques durant une élection

Le gouvernement a pris divers moyens pour communiquer de l'information aux partis politiques quant à l'ingérence étrangère en période électorale.

### Breffages classifiés aux représentants de parti détenant une cote de sécurité

Comme je l'ai mentionné au chapitre 8 (volume 2), en 2019 et en 2021 le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (le « **Groupe de travail** ») a donné des breffages de niveau « Secret » aux représentants des partis conservateur, libéral et néo-démocrate détenant l'autorisation de sécurité requise. Les breffages comportaient des informations de sources ouvertes, ainsi que certaines informations classifiées sur les types de tactiques d'ingérence étrangère employées. Il n'y était pas question d'éléments de renseignement ou d'acteurs menaçants précis. Comme il ne s'agissait pas d'information spécifique, les breffages avaient été classifiés au niveau « Secret » plutôt qu'à un niveau plus élevé.

Les membres du Groupe de travail ont expliqué que les breffages avaient deux objectifs. Le premier était de donner un peu plus d'information que ce que l'on pouvait trouver dans les sources publiques sur les tactiques et les techniques d'ingérence étrangère employées, afin de sensibiliser davantage les partis politiques et leur permettre d'identifier l'ingérence étrangère dans leurs processus. Le deuxième objectif était d'établir une voie de communication bidirectionnelle pour permettre aux partis politiques de signaler leurs préoccupations au Groupe de travail, le cas échéant.

Les représentants des partis libéral, conservateur et néo-démocrate détenant l'autorisation de sécurité requise m'ont dit que l'information qu'ils avaient reçue était d'ordre général et contextuel sur les menaces. Aucun renseignement précis ou exploitable ne leur a été communiqué. Les membres du Groupe de travail ont convenu que le type d'information dont il a été question durant ces breffages n'était pas immédiatement utilisable.

## Breffages non classifiés aux partis politiques

Le gouvernement a aussi donné des breffages non classifiés à l'intention des partis politiques. Comme j'en ai parlé au chapitre 12 (volume 3), le BCP et le Groupe de travail ont proposé aux représentants des différents partis politiques des breffages non classifiés lors de presque toutes les élections partielles depuis juin 2023. Comme je le mentionne dans ce chapitre, la participation à ces breffages a été faible. Le Groupe de travail a fait des efforts pour présenter des exemples concrets de ce à quoi l'ingérence étrangère peut ressembler dans le contexte électoral canadien. Il n'est pas encore possible de dire si les partis participeront à ces séances et s'ils trouveront que l'information communiquée est plus utile.

J'encouragerais fortement les représentants des partis politiques à assister à ces breffages lorsqu'ils sont donnés, et j'inciterais vivement le BCP et le Groupe de travail à s'assurer que les breffages soient aussi éloquents, précis et utiles que possible.

### 15.8 Breffages classifiés aux chefs de parti politique

#### Le rôle spécial des chefs de parti

Les chefs de parti politique ont des pouvoirs et des responsabilités uniques dans le cadre du système démocratique canadien, ce qui peut leur conférer un rôle important dans la lutte contre l'ingérence étrangère.

En vertu de la *Loi électorale du Canada*, les chefs des partis politiques ont le pouvoir discrétionnaire de décider qui est autorisé à se présenter pour le parti lors d'une élection. Ces derniers doivent approuver les candidats et peuvent désigner un candidat sans qu'une course à l'investiture soit tenue.

Après l'élection des députés, les chefs de parti attribuent les postes et les fonctions au sein du caucus. Le chef du parti au pouvoir décide qui siège au Cabinet et qui devient secrétaire parlementaire. Les chefs de l'opposition, quant à eux, distribuent les portefeuilles de porte-parole et désignent ceux qui occupent des postes comme celui de whip et de leader parlementaire. Bien que les chefs de parti ne puissent pas expulser un député du Parlement, ils peuvent l'expulser du caucus. Sur un plan plus informel, les chefs de parti peuvent s'entretenir avec leurs députés pour discuter de leurs préoccupations, formuler leurs attentes et leur transmettre des avertissements.

Un certain nombre de témoins ont référé à ces pouvoirs comme étant des outils potentiels pour lutter contre l'ingérence étrangère ciblant les parlementaires. Par exemple, un chef de parti ayant des doutes sur l'intégrité de l'un de ses députés peut le destituer de ses fonctions, autres que celle de député, ou décider dès le départ de ne pas lui confier de telles fonctions. Les chefs peuvent exprimer leurs préoccupations à leurs députés au sujet des relations que ceux-ci peuvent entretenir, par exemple avec des fonctionnaires étrangers.

Cependant, j'ai également entendu que, pour que les chefs prennent de telles mesures, il peut s'avérer nécessaire qu'ils aient accès à du renseignement pour être informés d'un problème. La communication rapide de renseignement aux chefs peut revêtir une importance particulière en période électorale, lorsque davantage d'options s'offrent à eux, comme ne pas permettre à un candidat de se présenter sous la bannière du parti.

Dans le cas du parti au pouvoir, il est possible de communiquer ce type de renseignement assez facilement au chef puisque le premier ministre peut recevoir un breffage en fonction des besoins. Toutefois, la situation est plus délicate lorsque le renseignement concerne un député ou un candidat de l'opposition. Le premier ministre Trudeau a affirmé que, bien qu'il puisse être breffé, il serait malaisant pour lui en tant que chef d'un parti politique d'être impliqué dans une discussion pour déterminer si un membre d'un autre parti politique devrait être autorisé à se présenter comme candidat ou à jouer un rôle donné. Le premier ministre a plutôt suggéré que chaque chef de parti soit tenu responsable de la résilience des processus du parti vis-à-vis des acteurs menaçants.

## Défis liés aux breffages aux chefs de parti

Il n'est pas aussi simple qu'il n'y paraît de donner accès à du renseignement aux partis d'opposition. De fait, traditionnellement, les chefs de l'opposition n'ont pas un accès régulier à du renseignement classifié au sujet des membres de leur caucus ou des candidats.

L'un des défis qui se posent dans la transmission d'information classifiée aux chefs de parti, qui bien souvent siègent au Parlement, concerne l'ensemble des risques dont j'ai parlé précédemment dans ce chapitre à propos de la communication de documents classifiés aux parlementaires en général. Comme les autres parlementaires, les chefs de parti bénéficient d'un privilège parlementaire qui peut (je ne me prononce pas sur cette question) les mettre à l'abri de toute responsabilité en cas de divulgation d'informations sensibles sans autorisation, si cela est fait dans l'enceinte du Parlement.

Des défis se posent également pour les chefs de parti qui reçoivent du renseignement, en particulier s'ils se font dire qu'ils sont limités dans l'utilisation qu'ils peuvent en faire en raison de préoccupations concernant la

sécurité. Lorsqu'une telle situation se produit, un chef de parti peut avoir l'impression de ne pas pouvoir faire grand-chose.

Même lorsqu'une mesure peut être prise, la communication d'un renseignement de nature sensible au sujet d'un député peut placer un chef dans une situation difficile puisque toute décision concernant ce député peut devoir être prise sans que ce dernier ait eu droit à une procédure juste et équitable. Après tout, il peut s'avérer impossible pour un chef d'expliquer à une personne les raisons pour lesquelles elle ne pourra pas se présenter pour le parti, et encore moins de donner à cette personne l'occasion de se défendre des accusations qui pèsent contre elle. En outre, le retrait inexplicé d'un candidat sur un bulletin de vote ou au sein d'un caucus pourrait susciter des soupçons importants. Cela étant, il peut tout de même être prudent de prendre des mesures, même si elles sont injustes. Tout dépend des circonstances propres à chaque situation.

Malgré tous ces défis, la nécessité perçue d'informer les chefs de l'opposition a mené le gouvernement à envisager des manières de donner un accès aux informations classifiées à l'ensemble des chefs de parti.

## Offrir des autorisations de sécurité de niveau « Très secret » aux chefs de l'opposition

Comme j'en ai discuté plus tôt dans ce chapitre, le conseiller à la sécurité nationale et au renseignement auprès du premier ministre (CSNR) a suggéré, dans une note de service préparée en décembre 2020, d'offrir des breffages de niveau « Secret » aux chefs de l'opposition. Finalement, cette recommandation n'a pas été suivie.

En mai 2023, les chefs de l'opposition se sont fait offrir la possibilité d'obtenir une autorisation de sécurité de niveau « Très secret » afin de pouvoir lire l'annexe classifiée du rapport préparé par le rapporteur spécial indépendant sur l'ingérence étrangère. Les chefs détenant une autorisation de sécurité ont aussi pu, plus tard, lire la version classifiée du *Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratique du Canada* de 2024 du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR). Je constate également que, conformément au mandat de la Commission, le gouverneur en conseil pourrait rendre accessibles les compléments classifiés de mes deux rapports (initial et final) à tous les chefs de parti reconnu à la Chambre des communes détenant le niveau d'autorisation de sécurité requis<sup>28</sup>.

Lorsque les audiences publiques de la Commission ont eu lieu, seuls les chefs du NPD et du Parti vert avaient donné suite à cette offre. Je sais cependant, d'après des rapports publics, que le chef du Bloc Québécois

---

<sup>28</sup> Décret du Conseil Privé no 2023-0882, division (a)(i)(G).

détient maintenant lui aussi une autorisation de sécurité de niveau « Très secret ». Le chef du Parti conservateur a déclaré publiquement qu'il n'allait pas présenter de demande d'autorisation de sécurité. Néanmoins, son chef de cabinet a obtenu une autorisation de sécurité de niveau « Très secret ».

Jusqu'à présent, les breffages aux chefs de partis de l'opposition sont donnés sur une base ponctuelle et coordonnés par le CSNR et son adjoint. Le BCP prépare une trousse de renseignement à l'intention des chefs de parti de l'opposition, en se fondant à la fois sur les questions de sécurité d'ordre général et sur les éléments d'information particuliers que chacun des chefs a besoin de savoir. Les chefs de partis de l'opposition ont ensuite l'occasion de poser des questions. Les chefs du NPD et du Parti vert ont tous deux reçu des breffages classifiés.

Dans une note de service datée de mai 2024 et destinée au premier ministre, la CSNR Nathalie Drouin mentionne que le BCP se prépare à présenter un protocole sur la prestation régulière de breffages classifiés aux chefs de tous les partis reconnus. Lors des audiences publiques, M<sup>me</sup> Drouin a affirmé que le BCP mettrait la touche définitive au protocole sur les breffages réguliers classifiés (au moins deux fois par année) à tous les partis représentés à la Chambre, en plus de breffages ponctuels. Le chef de cabinet du chef du Parti conservateur a lui aussi reçu des breffages classifiés.

## Breffages sur du renseignement précis au printemps de 2024

Au printemps 2024, le gouvernement possédait du renseignement concernant les partis d'opposition qui ont exigé qu'il renouvelle ses efforts pour donner des breffages classifiés spéciaux ad hoc aux chefs de parti.

Dans une note de service destinée au premier ministre et datée du 2 mai 2024, intitulé « Breffages classifiés ad hoc », il est question de renseignement sur des activités d'ingérence étrangère visant les partis d'opposition. Le renseignement indiquait qu'un État étranger cherchait à influencer les processus politiques.

Le renseignement a été porté à l'attention de la CSNR et transmis ensuite au greffier du Conseil privé, au premier ministre et au Comité des sous-ministres sur la gestion de l'intervention du renseignement (le CSMGIR). Certains éléments de ce renseignement portaient sur des allégations de nature grave. M<sup>me</sup> Drouin a dit que le gouvernement a déterminé qu'il était nécessaire d'organiser des breffages classifiés avec certains chefs de l'opposition ou leurs représentants. Elle a souligné que la note de service datée du 2 mai 2024 visait à informer le premier ministre que les autres chefs de parti se verraient offrir un breffage, et non pas à obtenir son autorisation.

La note de service précisait que le SCRS allait préparer des breffages classifiés de niveau « Très secret », ce qui permettrait aux partis ayant été

informés de prendre les mesures qui s'imposent. Elle indiquait également que le BCP et le SCRS travailleraient avec les chefs des partis politiques pour déterminer les éléments d'information pouvant être divulgués ainsi que l'approche que les partis pourraient suivre pour régler les problèmes sans compromettre les sources de renseignement. M<sup>me</sup> Drouin a expliqué que l'information contenue dans la note reflétait le point de vue du BCP selon lequel les breffages étaient nécessaires malgré les risques que les informations puissent être utilisées et partagées de façon inappropriée.

## La difficulté des chefs d'opposition qui ne sont pas breffés

J'ai entendu que le fait qu'un chef de parti n'ait pas d'autorisation de sécurité représentait un enjeu pour le gouvernement.

Le cabinet du premier ministre a demandé à des fonctionnaires s'il était possible de communiquer de l'information à un parti d'opposition même si son chef ne disposait pas d'une autorisation de sécurité. J'ai entendu que des discussions sont en cours pour porter à l'attention d'un parti politique des rapports de renseignement sur l'ingérence étrangère, y compris de la désinformation.

Le premier ministre a parlé d'un cas où la CSNR lui a fourni de l'information sur une situation d'ingérence étrangère potentielle importante impliquant des partis d'opposition. Cette information, a-t-il dit, était explosive. Selon lui, il a dit à la CNSR, au SCRS et à d'autres qu'ils avaient besoin d'un plan d'intervention. Il leur a aussi souligné qu'il n'était pas bon pour la démocratie qu'il puisse utiliser, dans son double rôle de premier ministre et de chef du Parti libéral, à de l'information sur une situation d'ingérence étrangère potentielle impliquant des partis d'opposition, puisqu'on pourrait être porté à croire qu'il se sert de cette situation pour les mettre dans l'embarras.

Le premier ministre a dit qu'il avait offert des breffages classifiés à tous les chefs de parti afin qu'ils soient mieux placés pour prendre des mesures et protéger leurs députés, dont certains pourraient être vulnérables ou impliqués, sciemment ou non, dans des activités d'ingérence étrangère. Le chef du Parti conservateur n'ayant pas d'autorisation de sécurité, le premier ministre a demandé au SCRS et à d'autres d'essayer de l'informer afin qu'il puisse être averti et prêt à prendre des décisions pour protéger son parti et ses membres. Or, la manière de communiquer cette information pose un défi. Par exemple, le premier ministre a témoigné que les chefs de cabinet ont des pouvoirs plus limités que les chefs de partis et qu'ils ne sont pas tenus de rendre compte au public de la même manière.

Le député Chong a suggéré que les membres du Conseil privé du Roi puissent recevoir de l'information classifiée en vertu de leur serment et de leur rôle, sans avoir à demander une autorisation de sécurité. Ce privilège s'appliquerait à lui-même et au chef du Parti conservateur.

Le premier ministre m’a dit que le titre de membre du Conseil privé n’équivaut pas à une autorisation de sécurité et n’accorde pas l’accès à de l’information classifiée en général. Ce titre leur permet d’accéder à de l’information qui se rapporte à leurs tâches et à leurs rôles en tant que membres du Conseil privé du gouvernement. C’est pourquoi, par exemple, Marco Mendicino, qui était ministre de la Sécurité publique d’octobre 2021 à juillet 2023 – et par conséquent, membre du Conseil privé –, a été obligé d’obtenir une nouvelle autorisation de sécurité afin d’examiner les documents qui se rapportaient à son témoignage à huis clos devant la Commission.

## 15.9 Communication d’informations par le Centre canadien pour la cybersécurité

Certains partis politiques ont communiqué avec le Centre canadien pour la cybersécurité (le CCC). Ils ont estimé l’utilité de ces communications à des degrés variables. Au moins deux partis ont également consulté des experts externes en cybersécurité, l’un d’entre eux pour connaître les meilleures pratiques concernant une plateforme de médias sociaux spécifique. Un parti a déclaré qu’il bénéficierait de conseils et d’aide supplémentaires pour soutenir son infrastructure informatique actuelle contre les menaces d’ingérence étrangère et qu’il souhaiterait un financement à cet effet.

## 15.10 L’effet du projet de loi C-70

Avant l’adoption de la *Loi concernant la lutte contre l’ingérence étrangère* (déposée en tant que projet de loi C-70), le SCRS était restreint dans sa capacité de communiquer de l’information à l’extérieur du gouvernement fédéral. Grâce à ses nouveaux pouvoirs de divulgation, le SCRS pourrait être en mesure d’aborder différemment l’enjeu de fournir de l’information aux partis d’opposition ou aux parlementaires. Par exemple, un témoin du SCRS a expliqué que la nouvelle Loi permet au SCRS de fournir davantage de breffages classifiés à des entités comme les associations de circonscriptions électorales, ce que le SCRS a envisagé de faire étant donné qu’il perçoit les courses à l’investiture comme étant vulnérables à l’ingérence étrangère.

M. Mendicino, a expliqué que la *Loi concernant la lutte contre l’ingérence étrangère* vise à répondre aux limites du SCRS quant à la divulgation d’information classifiée lors des breffages préventifs de sécurité à l’intention des députés. Selon lui, les modifications permettront au SCRS de déclassifier autant d’information que possible et ainsi lui permettre de donner des

breffages plus complets, de communiquer du renseignement à l'extérieur du gouvernement et d'avoir une approche davantage tournée vers l'extérieur pour réduire la menace.

Cela dit, la *Loi concernant la lutte contre l'ingérence étrangère* ne change rien au besoin de protéger les sources de renseignement et les moyens de collecte, et il n'élimine pas non plus les difficultés et les risques que j'ai identifiés ci-dessus concernant la communication de l'information classifiée aux parlementaires et aux chefs des partis politiques. Ces difficultés existent toujours.

## 15.11 Conclusion

Comme le démontre ce chapitre, l'échange d'informations sur l'ingérence étrangère à l'extérieur du gouvernement est à la fois important et difficile. Même l'échange d'informations avec des acteurs tels que les parlementaires fédéraux peut présenter des difficultés pour le gouvernement. Cependant, quelle que soit la difficulté, l'échange d'informations avec les parlementaires est essentiel pour renforcer la résilience face à l'ingérence étrangère.

Les parlementaires ne sont toutefois pas les seuls acteurs extérieurs au gouvernement fédéral à avoir besoin d'accéder aux informations pour mieux se défendre contre la menace d'ingérence étrangère. Dans le chapitre suivant, j'aborde certaines des questions liées à l'échange d'informations avec d'autres acteurs extérieurs au gouvernement fédéral, dont les autres gouvernements et le public.

CHAPITRE 16

# La communication d’informations à l’extérieur du gouvernement fédéral

---

16.1	Introduction	99
16.2	Rapports avec d’autres gouvernements au Canada	99
16.3	Rapports avec le public	103
16.4	Conclusion	105

**Les informations peuvent être incomplètes :** des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.

## 16.1 Introduction

Les deux derniers chapitres de ce rapport se sont concentrés sur la manière dont l’information circule au sein du gouvernement fédéral, de même qu’avec les parlementaires et les partis politiques. Dans ce chapitre, j’examine la manière dont l’information est partagée avec des entités qui se trouvent complètement à l’extérieur de la sphère fédérale.

## 16.2 Rapports avec d’autres gouvernements au Canada

### L’importance de la communication intergouvernementale

L’ingérence étrangère ne vise pas seulement les institutions et les processus fédéraux. Les acteurs étrangers ciblent les institutions à tous les niveaux au Canada. Les gouvernements provinciaux, territoriaux, autochtones et municipaux sont des aspects fondamentaux de la société libre et démocratique dans laquelle nous vivons. En tant que société, il est important que nous nous efforcions de les défendre parallèlement aux processus démocratiques fédéraux. Cela requiert une collaboration entre les différents gouvernements. De hauts fonctionnaires fédéraux m’ont affirmé qu’il est important de partager des informations avec les autres ordres de gouvernement sur les menaces auxquelles ils sont confrontés.

Les réponses à l’ingérence étrangère, quel que soit l’ordre de gouvernement visé, peuvent aussi nécessiter des outils d’intervention dans des champs de compétence qui ne relèvent pas du gouvernement fédéral aux termes de la Constitution. L’éducation est un exemple important. On m’a dit que le développement de la littératie numérique était un élément clé de la lutte contre la mésinformation et la désinformation au Canada. Or, pour mettre en œuvre cet objectif, il faudrait probablement des initiatives en matière d’éducation publique qui ne relèvent pas du gouvernement fédéral et qui ne peuvent pas être mises en œuvre par ce dernier. Ce domaine est plutôt du ressort des gouvernements provinciaux et autochtones.

Cela ne veut pas dire que le gouvernement fédéral n’a aucun rôle à jouer, mais seulement que la réponse à l’ingérence étrangère doit reconnaître et respecter les limites juridiques et les champs de compétences imposés par la Constitution. Par exemple, le Service canadien du renseignement de sécurité (le « **SCRS** ») peut partager avec une municipalité ou une province des informations sur les dangers d’utiliser une technologie donnée et suggérer des mesures à prendre, mais c’est à la municipalité ou à la province qu’il incombe ensuite d’atténuer les risques. Pour cette raison, le gouvernement fédéral doit aider et soutenir les autres ordres de gouvernement dans l’exercice de leurs pouvoirs afin de renforcer la résilience collective du Canada.

Les gouvernements hors de la sphère fédérale sont donc des acteurs clés dans une réponse à l’ingérence étrangère qui implique l’ensemble de la société. Nous avons tous intérêt à renforcer la résilience et à veiller à ce que le Canada dispose d’une démocratie saine et d’élections libres et équitables, quel que soit l’ordre de gouvernement. Afin de lutter efficacement contre l’ingérence étrangère, une coopération et une collaboration entre les gouvernements d’un océan à l’autre seront nécessaires.

## Les défis du dialogue avec les autres gouvernements

Affirmer l’importance de la collaboration est une chose, mais je comprends que cette collaboration puisse parfois être difficile. Les relations intergouvernementales posent souvent des défis et ceux-ci peuvent se soulever lorsque vient le moment de coordonner la réponse à l’ingérence étrangère.

Les ressources, les capacités et les connaissances en matière de sécurité nationale varient d’un gouvernement à l’autre. Des témoins du gouvernement fédéral m’ont avisé qu’un facteur important pour eux lorsqu’ils dialoguent avec les provinces et les territoires est le niveau variable de leurs connaissances et de leurs capacités en ce qui concerne la sécurité nationale. Sur le plan opérationnel, cette situation complexifie une coordination efficace avec les provinces et les territoires. Il en va probablement de même avec les gouvernements autochtones et municipaux.

Divers gouvernements peuvent également être confrontés à des menaces différentes. Cela peut se traduire par des priorités qui varient d’un à l’autre et par le besoin d’adopter des approches distinctes lorsque le gouvernement fédéral travaille avec plusieurs ordres de gouvernement.

Le fait que les gouvernements possèdent tous leur fonctionnement propre crée également des défis sur le plan pratique. Les gouvernements fédéral, provinciaux, territoriaux, autochtones et municipaux sont tous structurés différemment. Sur le terrain, il peut être difficile pour les fonctionnaires fédéraux de déterminer les ministères, les bureaux ou leurs homologues avec lesquels ils pourraient collaborer.

Les problèmes entourant le partage d’informations classifiées, que j’ai abordés tout au long de ce rapport, constituent un autre défi pratique à une coopération intergouvernementale efficace.

Le 31 octobre 2023, le premier ministre du Yukon, Ranj Pillai, a écrit au premier ministre du Canada pour lui faire part de ses inquiétudes au sujet de l’absence de consultation sur les incidents de sécurité nationale et sur l’incapacité des agences de sécurité à partager des informations classifiées avec les fonctionnaires des gouvernements infranationaux. M. Pillai a soulevé les besoins en matière d’infrastructures physiques et numériques qui permettraient aux provinces et territoires d’avoir accès à des informations délicates. Le premier ministre du Canada a déclaré que la *Loi concernant la lutte contre l’ingérence étrangère* (le projet de loi C-70) – que j’aborde au chapitre 12, volume 3 – cherchait en partie à répondre à la préoccupation de M. Pillai quant au partage des informations.

Plusieurs témoins ont déclaré que le projet de loi C-70 a étendu la capacité du SCRS à communiquer des informations classifiées en dehors du gouvernement fédéral et ils s’attendent à ce que cela améliore la circulation des informations. Toutefois, le projet de loi C-70 ne réduit pas la nécessité pour les agences de sécurité de protéger leurs sources et leurs méthodes de collecte du renseignement lorsqu’elles partagent ainsi des informations classifiées en dehors du gouvernement.

Le gouvernement fédéral a également invité certains fonctionnaires provinciaux et territoriaux à obtenir une autorisation de sécurité, ce qui permettrait de bénéficier de points de contact pour les questions de sécurité nationale. Ce processus est en cours.

On m’a aussi expliqué que l’infrastructure et la capacité de traitement et de stockage des informations classifiées des provinces et des territoires constituaient un obstacle au partage du renseignement. Le gouvernement fédéral cherche actuellement à mettre en place des réseaux de partage d’informations avec les provinces et territoires. Il a aussi proposé de doter les provinces et territoires de systèmes de communication allant jusqu’au niveau « Secret ».

Dans l’intervalle, toutefois, les défis du partage d’informations classifiées demeurent. En outre, compte tenu du nombre considérable de gouvernements autochtones et de municipalités au Canada et de la diversité de leurs ressources et de leur capacité à gérer les informations classifiées, il m’apparaît que le partage d’informations continuera peut-être à poser des défis dans de nombreuses situations.

## Les travaux réalisés à ce jour

Malgré ces difficultés, j'ai entendu des témoignages selon lesquels le gouvernement fédéral s'efforçait de nouer un dialogue avec les provinces, les territoires, les gouvernements autochtones et les municipalités au sujet de l'ingérence étrangère.

Un certain nombre d'initiatives sont en cours au sein du Bureau du Conseil privé (le « **BCP** »). La conseillère à la sécurité nationale et au renseignement auprès du premier ministre travaille avec la communauté de la sécurité nationale et du renseignement pour élaborer des programmes et des breffages types à l'intention des provinces et des territoires, et concevoir des breffages et des documents adaptés à leurs besoins et aux menaces qui les concernent.

Le Secrétariat de la sécurité et du renseignement du BCP et Sécurité publique Canada codirigent une table sur la sécurité nationale au niveau des sous-ministres adjoints, qui rassemble les provinces et les territoires. Cette table a cessé de se réunir pendant la pandémie de COVID-19, mais a été relancée sous la forme d'un forum qui traite de toutes les questions de sécurité nationale, dont l'ingérence étrangère. Le BCP a également participé à plusieurs réunions bilatérales avec les provinces. L'objectif de ces réunions est de permettre au gouvernement de partager des informations avec les provinces et de donner à ces dernières la possibilité de faire part de leurs préoccupations. Cela vise à relever le défi que j'ai mentionné plus haut concernant les différences structurelles entre les gouvernements.

Le Secrétariat des institutions démocratiques du BCP entretient des contacts réguliers avec les fonctionnaires provinciaux et territoriaux. Il a transmis aux provinces et aux territoires son guide sur l'ingérence étrangère et son recueil de pratiques exemplaires en matière d'ingérence étrangère. En janvier 2024, il a publié sa *Trousse d'outils pour protéger la démocratie*, qu'il a également transmise aux provinces et territoires.

Le greffier du Conseil privé et le ministère du Patrimoine canadien (« **Patrimoine canadien** ») se sont efforcés de nouer un dialogue avec les provinces et les territoires afin de développer la littératie numérique. Patrimoine canadien a fait de même avec les gouvernements provinciaux sur des questions touchant l'intelligence artificielle.

Le coordonnateur national de la lutte contre l'ingérence étrangère, qui relève du ministère de la Sécurité publique et dont je parle au chapitre 11 (volume 3), a tenu un breffage sur l'ingérence étrangère à l'intention des députés provinciaux de la Colombie-Britannique avant les élections provinciales. Il a proposé d'organiser des breffages similaires pour toutes les provinces et tous les territoires.

## 16.3 Rapports avec le public

Pour l'essentiel, tous les organismes et ministères fédéraux qui ont témoigné ont souligné que sensibiliser le public représentait un élément clé d'une réponse à l'ingérence étrangère qui implique l'ensemble de la société. À titre d'exemple, j'ai entendu des témoignages selon lesquels la communauté de la sécurité nationale et du renseignement du Canada reconnaissait la nécessité de dialoguer avec les victimes de cyberincidents. Pour cela, elle a conçu des outils pour rejoindre le public, par exemple des publications, destinées à différents publics. Certains organismes, comme le SCRS et la Gendarmerie royale du Canada (la « **GRC** »), disposent également de services spécialisés à cet effet.

La plupart des témoins gouvernementaux ont affirmé qu'il ne serait pas productif d'avoir un seul point de contact au sein du gouvernement pour sensibiliser le public et interagir avec lui. Si la coordination est importante pour assurer la cohérence du message gouvernemental et éviter la « surdose de consultations », il est également essentiel que les gens aient des options, selon leur situation et leurs besoins, pour échanger avec le gouvernement. Trouver les meilleurs canaux pour atteindre les communautés est essentiel aux efforts de communication du gouvernement.

De plus, bien que le Canada fonde sa stratégie de dialogue avec le public sur le comportement des acteurs menaçants et non sur leurs cibles, le gouvernement tente d'adapter ses communications à la situation et aux besoins particuliers des communautés. D'après les témoins du gouvernement, il est donc important que chaque agence bâtisse sa propre relation avec la population. Il s'agit là, à mon avis, d'une bonne approche, mais qui ne doit pas occulter le besoin qu'a le gouvernement de développer rapidement une stratégie de communication globale et cohérente.

Les agences de sécurité et de renseignement ainsi que les organismes d'application de la loi tentent d'établir des liens avec le public, y compris avec les communautés issues des diasporas, en utilisant divers canaux :

- La GRC et le Centre canadien pour la cybersécurité (le « **CCC** ») du Centre de la sécurité des télécommunications ont récemment fait des efforts pour accroître leur présence dans les médias sociaux.
- Le SCRS et le CCC s'efforcent d'inclure de plus en plus d'informations spécifiques et détaillées sur l'ingérence étrangère dans leurs produits destinés au public.
- La GRC, le CCC et le SCRS se sont employés à traduire certains de leurs produits dans des langues autres que le français ou l'anglais.
- La GRC tente d'être plus présente lors d'événements communautaires locaux.

Les organismes mentionnés ci-dessus emploient également des processus de communication plus formels. Par exemple, Sécurité publique Canada et le

ministère de la Justice codirigent la Table ronde transculturelle sur la sécurité nationale. Ce forum regroupe des représentants communautaires qui informent le gouvernement des préoccupations de leurs communautés et qui sont consultés sur de potentielles initiatives politiques. Le gouvernement a également considéré les deux séries de consultations qu'il a menées sur le projet de loi C-70 comme un moyen d'échanger avec le secteur privé, les organisations communautaires et les communautés issues des diasporas.

Cependant, une grande partie de la communication des gouvernements s'effectue par le biais d'appels, de réunions et de messages informels. Certains témoins ont mentionné que le dialogue informel est parfois plus efficace pour bâtir la confiance et permet à un plus grand nombre de personnes d'exprimer leur opinion.

Tricia Geddes, qui était alors sous-ministre adjointe déléguée à la Sécurité publique<sup>29</sup>, a décrit les interactions continues et la communication au sujet de l'ingérence étrangère comme l'un des outils les plus efficaces que possède le gouvernement pour perturber les tentatives des États étrangers ciblant les communautés vulnérables. D'autres témoins se sont dit en accord et ont ajouté que ces interactions favorisent une meilleure compréhension par le public des outils à sa disposition pour se protéger et des ressources à la disposition du gouvernement pour contrer l'ingérence étrangère. Celles-ci encouragent également le public à signaler toute ingérence étrangère potentielle. J'ai entendu que des relations continues permettent le partage d'informations avec le public, partage qui peut accroître la résilience.

Les préoccupations ou les questions soulevées par le public peuvent alimenter la compréhension qu'a le gouvernement de la menace d'ingérence étrangère. Par exemple, le SCRS a indiqué que des aspects importants de sa compréhension de l'ingérence étrangère et les rapports qu'il a produits à ce sujet provenaient des témoignages de membres des communautés issues des diasporas. Le SCRS considère les relations avec ces personnes comme essentielles pour maintenir et soutenir son travail opérationnel. Affaires mondiales Canada a déclaré que les informations fournies par les particuliers peuvent éclairer l'élaboration de la politique étrangère. On m'a expliqué que la rétroaction du public était importante, car elle permet au gouvernement de modifier ses pratiques au besoin.

Les témoignages qui m'ont été présentés ont fréquemment rappelé l'importance de retrouver la confiance du public, surtout dans les relations avec les communautés issues des diasporas. Les témoins du SCRS ont reconnu que l'agence doit surmonter la méfiance des membres de ces communautés, qui ont pu être victimes dans le passé d'un traitement problématique par des organismes d'application de la loi ou par les agences de sécurité et de renseignement du Canada.

---

<sup>29</sup> Tricia Geddes est devenue sous-ministre de Sécurité publique Canada le 31 octobre 2024.

Les témoins du gouvernement ont déclaré que, dans une certaine mesure, certaines personnes au sein de communautés se méfient encore du gouvernement, mais estimaient que grâce à un long processus d’interactions et de réunions fréquentes, le manque de confiance est en train de se dissiper. Ils ont souligné que le soutien généralisé au projet de loi C-70 en était un indicateur.

On m’a également parlé de l’incidence de la *Loi concernant la lutte contre l’ingérence étrangère*. Les nouveaux pouvoirs de divulgation qu’elle accorde au SCRS pourraient permettre à ce dernier d’aborder différemment la façon dont il transmet des informations à des entités ou à des personnes à l’extérieur du gouvernement fédéral.

Cependant, même avec les modifications apportées à la *Loi sur le Service canadien du renseignement de sécurité*, le dialogue avec la population continuera à présenter des défis. J’ai d’ailleurs entendu des témoignages sur des travaux cherchant à faire en sorte que le gouvernement produise davantage d’informations non classifiées afin de faciliter cette démarche.

De hauts fonctionnaires du SCRS, autant anciens que toujours en poste, m’ont dit que l’agence avait par le passé pris l’habitude de donner de hauts niveaux de protection aux informations classifiées. Toutefois, les témoins du SCRS ont également parlé de l’évolution du SCRS vers une « politique de la lumière » pour être plus ouvert avec la population canadienne en matière d’ingérence étrangère. Selon un témoin, le SCRS comprend maintenant qu’il doit être en mesure de communiquer de l’information pour mieux protéger la population canadienne et renforcer sa confiance envers les agences de renseignement.

Il s’agit de bonnes intentions, mais un plan plus formel et plus structuré est nécessaire, car jusqu’à présent, la communication avec le public a été, selon moi, insuffisante. Les rapports annuels et autres documents publiés sur les sites Web du gouvernement ne suffisent pas, particulièrement si les sites ne sont pas eux-mêmes faciles à utiliser. Je reconnais que, dans un monde débordant d’informations, il n’est pas facile de retenir l’attention du public. Il faut trouver des solutions créatives. Je reviendrai sur ce sujet dans mes recommandations.

## 16.4 Conclusion

La communication en dehors de la sphère fédérale présente des défis uniques pour le gouvernement fédéral. Toutefois, d’autres ordres de gouvernement sont tout aussi vulnérables face à l’ingérence étrangère, et jouent un rôle crucial dans la lutte contre cette menace, compte tenu du partage des compétences prévu par la Constitution. De la même manière, la communication avec le public et sa mobilisation sont essentielles. Il s’agit de domaines dans lesquels le gouvernement devrait concentrer ses efforts à l’avenir.

## CHAPITRE 17

# La répression transnationale

17.1	Introduction	107
17.2	La répression transnationale et le mandat de la Commission	108
17.3	Les acteurs de la répression transnationale et leurs tactiques	108
17.4	La réponse du Canada à la répression transnationale	112
17.5	Des exemples d'activités de répression transnationale au Canada	114
17.6	Conclusion	120

*Les informations peuvent être incomplètes : des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.*

## 17.1 Introduction

Il n'existe actuellement aucune définition juridique de la répression transnationale au Canada. Le Service canadien du renseignement de sécurité (le « **SCRS** ») décrit la répression transnationale comme une activité d'un État étranger visant à surveiller, intimider et harceler les communautés issues des diasporas au Canada dans le but d'atteindre ses objectifs. Elle a aussi été décrite comme une pratique selon laquelle des puissances étrangères franchissent les frontières pour tenter d'intimider, de réduire au silence ou de causer préjudice à ceux qu'elles considèrent comme des détracteurs, généralement des dissidents, des réfugiés, des militants pour les droits de la personne ou des groupes minoritaires, et d'exercer un contrôle sur eux. La répression transnationale porte atteinte à la liberté d'un individu de s'engager dans des pratiques démocratiques légitimes et menace de miner la société démocratique et la souveraineté des États, dont celle du Canada.

J'ai entendu des témoins du gouvernement reconnaître la gravité de la menace que représente la répression transnationale pour les communautés issues des diasporas, le public canadien et l'ensemble de la société canadienne. Je suis d'accord avec eux. Il s'agit là d'une menace très importante qui semble devenir de plus en plus grande dans le contexte géopolitique actuel.

Les témoins de la Gendarmerie royale du Canada (la « **GRC** ») ont déclaré que la répression transnationale était l'un des types de menaces liées à l'ingérence étrangère les plus répandus au Canada. David Morrison, sous-ministre des Affaires étrangères actuel et ancien conseiller à la sécurité nationale et au renseignement auprès du premier ministre, estime que la véritable menace d'ingérence étrangère pour le Canada n'est pas le fait que des acteurs étrangers prennent pour cible des parlementaires afin d'accroître leur influence, ce qui a tellement attiré l'attention publique, mais qu'il s'agit plutôt de la répression transnationale. David Vigneault, ancien directeur du SCRS, a déclaré publiquement que la répression transnationale est l'un des plus grands défis stratégiques pour la souveraineté et la démocratie du Canada.

À mon avis, il serait difficile d'exagérer la gravité de la répression transnationale ou l'incidence qu'elle a sur les individus et notre tissu social.

## 17.2 La répression transnationale et le mandat de la Commission

Les activités de répression transnationales ne relèvent pas toutes de mon mandat, qui consiste à examiner l'ingérence étrangère dans les processus démocratiques canadiens. Pour cette raison, la Commission n'a pas mené d'enquête directe ou exhaustive sur la répression transnationale. Une telle enquête aurait effectivement outrepassé son mandat et ses ressources.

Toutefois, le mandat de la Commission me demande d'examiner et d'évaluer les mesures de soutien en place pour les membres des communautés issues des diasporas qui peuvent être vulnérables et victimes d'ingérence étrangère dans les processus démocratiques du Canada. Ce faisant, j'ai entendu des témoignages relatifs à la répression transnationale entraînant des répercussions sur les institutions démocratiques. De plus, compte tenu de l'importance du problème de la répression transnationale, de l'attention publique qu'il a suscitée et de la possibilité qu'il ait, dans certaines circonstances, une incidence sur notre démocratie, j'ai voulu mieux la comprendre. J'ai donc obtenu des informations quant à la répression transnationale qui n'avait pas de lien direct avec les institutions démocratiques.

Dans ce chapitre, je décris la preuve en lien avec la répression transnationale dont j'ai pris connaissance. Au chapitre 21 (volume 6), je résume aussi ce que j'ai entendu de la part de membres du public canadien au cours du processus de consultation publique de la Commission quant à leurs expériences de la répression transnationale et aux graves répercussions qu'elle a sur leur vie.

## 17.3 Les acteurs de la répression transnationale et leurs tactiques

On m'a dit qu'il est difficile d'évaluer l'ampleur de la répression transnationale au Canada. Les personnes ciblées sont souvent réticentes à faire part de leurs expériences. Bien que la GRC surveille les cas de répression transnationale, elle sait que ces cas sont probablement sous-déclarés. Les personnes peuvent craindre des représailles contre elles ou leurs proches à l'étranger si elles dénoncent la situation. Elles peuvent croire que les agences de sécurité ne seront pas en mesure d'enquêter ou de porter des accusations à l'endroit de personnes qui se livrent à des activités signalées réalisées à partir de l'étranger (p. ex., le harcèlement en ligne) ni à l'endroit du personnel des missions étrangères protégé par des immunités (p. ex., les diplomates). Plusieurs personnes ciblées sont issues de

communautés qui, pour des raisons culturelles et historiques, peuvent se méfier des organismes d'application de la loi et des agences de sécurité.

Les représentants du SCRS classent les États étrangers qui entreprennent des activités de répression transnationale au Canada dans différentes catégories en fonction de leurs objectifs, de leurs intentions et de leurs méthodes. Certains peuvent avoir intérêt à s'ingérer dans les processus démocratiques canadiens, alors que d'autres ne l'ont pas.

Des États comme l'Iran, entre autres, se concentrent sur la répression des dissidents et des ressortissants étrangers vivant au Canada. Ces pays ont montré peu d'intérêt à s'ingérer dans les processus démocratiques canadiens. Leurs activités de répression transnationale peuvent inclure la collecte d'informations, le harcèlement numérique, les menaces physiques et la violence. Le Centre canadien pour la cybersécurité estime que les auteurs de cybermenaces parrainés par l'Iran et l'Arabie saoudite ont presque certainement surveillé les populations de la diaspora et les militants au moyen de cyberoutils, et il juge très probable que ces acteurs ciblent des personnes au Canada.

La République populaire de Chine (la « **RPC** ») et l'Inde se livrent également à des activités répressives à l'encontre des communautés, des dissidents politiques et des défenseurs des droits de la personne, mais elles démontrent également un intérêt à s'ingérer dans les processus démocratiques canadiens.

Je fournis ci-dessous de plus amples informations sur la répression transnationale que certains de ces États exercent. L'inventaire des pays n'est pas exhaustif et ne doit pas être interprété comme indiquant qu'aucun autre pays ne se livre à de la répression transnationale au Canada.

## L'Iran

L'Iran n'est pas, et n'a jamais été historiquement, un acteur important de menace d'ingérence étrangère dans les élections fédérales canadiennes. Cependant, l'Iran est considéré comme une menace très importante de répression transnationale en raison de l'intensité de ses activités, principalement menées à l'aide de cyberoutils.

Selon les rapports de renseignement, il est vraisemblable que dans le cadre de ses efforts visant à prévenir les critiques du régime, des représentants de l'Iran surveillent, influencent, harcèlent et intimident la communauté issue de la diaspora iranienne au Canada, et recueillent des informations à son sujet. Par exemple, j'ai entendu que l'Iran a tenté de dissuader les proches des victimes du vol PS752 au Canada de le critiquer. Cela avait pris la forme de menaces en ligne et par voie numérique, de communications de la part de représentants du gouvernement iranien, d'éventuelles cyberintrusions pour accéder à un réseau ou à un appareil, ainsi que la coercition et l'intimidation de membres de la famille toujours en Iran.

L'Iran s'appuie également sur des groupes criminels pour mener à bien un grand nombre des activités qu'il mène en dehors du pays contre les dissidents iraniens.

## La République populaire de Chine

La RPC harcèle, intimide et cherche à punir des personnes dans le monde entier, dans le but de forcer le retour des « fugitifs » en RPC. Elle utilise un large éventail de moyens techniques pour mener à bien ses activités de répression transnationale. Elle collecte du renseignement de sources humaines, effectue de la surveillance en ligne, commet des cyberintrusions, contrôle la mobilité et se livre à de la coercition par procuration. Elle a également recours au harcèlement et aux menaces de violence, aux rapatriements forcés et à la violence physique. Lorsque les autorités de la RPC ne disposent pas de moyens directs pour mener à bien leurs activités de répression transnationale, Internet devient leur outil privilégié. La RPC utilise efficacement les technologies existantes et les nouvelles technologies, notamment l'intelligence artificielle. Elle également a recours à la stratégie consistant à utiliser les membres de la famille qui vivent en RPC comme moyen de pression contre la personne qui se trouve au Canada.

La RPC fait appel à un large éventail d'acteurs pour ses activités d'ingérence étrangère. Le Département du travail du front uni (le « **DTFU** »), un département du Parti communiste chinois, tente de contrôler et d'influencer la diaspora chinoise.

La preuve démontre que les activités de répression transnationale de la RPC, qui comprennent le harcèlement et d'autres menaces, visent plus souvent des personnes affiliées à des groupes que la RPC considère comme particulièrement menaçants et qu'elle appelle collectivement les « cinq poisons » : les adeptes de Falun Gong, les Ouïghours, les Tibétains, les partisans de l'indépendance de Taïwan et les défenseurs de la démocratie en Chine continentale et à Hong Kong.

Plus que tout autre pays, la RPC sait dissimuler sa répression transnationale. Pour mener à bien ces activités, la RPC utilise, entre autres, ses missions diplomatiques, des étudiants de la RPC, des organisations communautaires et des particuliers affiliés au DTFU ou au ministère de la Sécurité de l'État de la RPC.

La RPC utilise parfois des entités gouvernementales infranationales, tant à des fins légitimes qu'illégitimes, ce qui complique la tâche des agences de sécurité et de renseignement canadiennes lorsqu'il s'agit de détecter ses activités de répression transnationale.

## L'Inde

Les activités de répression transnationale de l'Inde au Canada ciblent principalement la diaspora sikhe, qui compte environ 800 000 membres.

Depuis la tragédie d'Air India en 1985, l'Inde exerce des pressions sur le Canada pour qu'il adopte une position plus ferme à l'égard des sikhs canadiens qui appuient l'établissement du « Khalistan », que le gouvernement canadien définit comme une patrie distincte pour les sikhs du sous-continent indien. Selon le SCRS, l'Inde a des raisons légitimes de s'inquiéter de la menace pour la sécurité que représente l'extrémisme khalistanais au Canada. Certains extrémistes se sont livrés à des activités menaçantes visant l'Inde depuis le Canada, notamment en coordonnant et en finançant des activités terroristes en Inde. Toutefois, selon le SCRS, la grande majorité des partisans du Khalistan sont pacifiques.

Bien que le Canada ait toujours coopéré avec l'Inde pour traiter les cas de terrorisme réel ou de menace de terrorisme basés sur une preuve crédible, cette question continue de susciter des tensions importantes dans les relations entre le Canada et l'Inde. En outre, l'Inde et le Canada ont des points de vue opposés quant aux manifestations pacifiques qui ont lieu au Canada en faveur du Khalistan et sur ce qui constitue la liberté d'expression protégée. Cette situation a aggravé les tensions.

Dans ce contexte, la répression transnationale à laquelle se livre l'Inde vise à promouvoir un discours pro-Inde et anti-Khalistan au Canada.

La répression transnationale à laquelle se livre l'Inde comprend la collecte d'informations, la surveillance des personnes d'intérêt et l'affaiblissement du soutien aux politiques canadiennes liées à des questions comme l'extrémisme pakistanais et khalistanais. L'Inde s'adonne également à des activités d'ingérence étrangère qui visent à contrer les activités des communautés issues des diasporas qu'elle considère comme contraires à ses intérêts nationaux, comme la promotion légale et publique de questions telles que l'indépendance du Khalistan. Les informations recueillies par l'Inde, directement ou par le biais de mandataires, sont utilisées pour cibler les membres de la communauté sud-asiatique.

La déclaration faite par la GRC en octobre 2024 concernant des activités criminelles violentes au Canada ayant des liens avec des agents du gouvernement indien est conforme à la preuve classifiée sur les activités de plus en plus agressives et violentes menées par l'Inde à laquelle j'ai eu accès. De plus, l'Inde aspire à mettre en place un cyberprogramme modernisé. La communauté de la sécurité nationale et du renseignement estime que l'Inde est un acteur émergent de la cybermenace.

## 17.4 La réponse du Canada à la répression transnationale

Même si cela n'était pas l'objet de l'enquête de la Commission, j'ai entendu des témoignages portant sur les tentatives du gouvernement de répondre à la répression transnationale. Ces efforts englobent nécessairement la répression transnationale qui ne relève pas de mon mandat, mais également celle pouvant avoir une incidence directe ou indirecte sur nos institutions démocratiques. C'est dans cette optique que j'aborde brièvement ci-dessous, la réponse du gouvernement.

Sécurité publique Canada collabore avec d'autres ministères et organismes gouvernementaux pour élaborer des conseils stratégiques sur la répression transnationale.

Le coordonnateur national de la lutte contre l'ingérence étrangère (le « **CNLIE** ») a expliqué que son mandat comprend la réponse à la répression transnationale. Il m'a dit qu'il soumettait un plan d'action en matière de répression transnationale au sous-ministre de la Sécurité publique pour examen. Il a mis en place un groupe de travail interministériel sur la répression transnationale, qui réunit plusieurs ministères, et non seulement des organismes d'application de la loi ou des agences de sécurité et de renseignement. Selon lui, il s'agit là d'un élément essentiel pour lutter contre la répression transnationale compte tenu de la complexité de l'enjeu. Le CNLIE a notamment expliqué qu'Immigration, Réfugiés et Citoyenneté Canada et l'Agence des services frontaliers du Canada peuvent participer aux efforts visant à dépister les personnes qui pourraient avoir des liens avec le Département du travail du front uni (DTFU) avant d'entrer au Canada.

En 2022, Sécurité publique Canada a rétabli la « Table ronde transculturelle ». Celle-ci, créée après le 11 septembre 2001, a réuni différentes communautés pour discuter de radicalisation, puis a cessé de fonctionner à un certain moment. Shawn Tupper, ancien sous-ministre de la Sécurité publique, considère qu'elle permet d'entendre les points de vue des différentes communautés et de recevoir des conseils sur la façon dont Sécurité publique Canada peut améliorer son travail.

Dans le cadre de sa mobilisation auprès des groupes issus des diasporas, le SCRS a mis en place une ligne téléphonique d'urgence permettant de signaler de manière anonyme les cas d'ingérence étrangère. Le SCRS dispose aussi de protocoles lui permettant de réagir rapidement s'il apprend qu'une menace pèse sur un individu ou une communauté. Selon le SCRS, il peut être difficile d'évaluer les conséquences de la répression transnationale sur les communautés issues des diasporas et, en particulier, de déterminer si la répression transnationale a un effet sur la participation des membres des communautés aux processus démocratiques.

Bien que le Centre de la sécurité des télécommunications (le « **CST** ») n'ait pas de mandat domestique, certaines de ses cyberactivités ont des répercussions sur la répression transnationale. Par exemple, le CST a mené des cyberactivités conçues pour cibler les activités de répression transnationale auxquelles se livrent des entités étrangères ayant des répercussions au Canada.

Affaires mondiales Canada (« **AMC** ») a fait des efforts pour s'attaquer à la répression transnationale. L'un des quatre groupes de travail du Mécanisme de réponse rapide (le « **MRR du Canada** ») mis sur pied en 2023 est consacré à la répression transnationale. En juillet 2023, il a commencé à travailler à l'élaboration d'une définition de la répression transnationale. AMC a également organisé à Ottawa un forum sur les droits de la personne axé sur la répression transnationale exercée par la RPC. En avril 2023, AMC a organisé une activité publique sur la répression transnationale à l'Université métropolitaine de Toronto. Il a aussi fréquemment soulevé l'enjeu de la répression transnationale dans ses engagements diplomatiques avec certains pays, notamment la RPC.

En 2024, l'Initiative de citoyenneté numérique de Patrimoine canadien a financé des projets visant à comprendre la répression transnationale à laquelle se livre la RPC au Canada. L'un de ceux-ci cherchait à déterminer comment les campagnes de répression transnationale et la désinformation étrangère provenant de la RPC ont une incidence sur l'inclusion sociale au Canada. Les outils élaborés dans le cadre de ce projet ont été déployés dans différentes langues partout au Canada. Un autre projet, intitulé « *Strengthening Community Resilience to Foreign Interference* » (renforcer la résilience des communautés face à l'ingérence étrangère), visait à mieux comprendre l'ingérence étrangère de la RPC, y compris le fait qu'elle cible les Canadiennes et les Canadiens d'origine chinoise.

Pour protéger la capacité des membres des communautés issues des diasporas à participer aux élections, Élections Canada a publié des guides à l'intention des électeurs dans 51 langues et dialogue avec ces communautés au moyen de divers mécanismes. Ces initiatives visent à fournir de l'information aux personnes qui ne connaissent peut-être pas le processus électoral canadien et des renseignements sur l'intégrité électorale, comme le secret du vote et les différentes manières de voter.

Le gouvernement discute également avec ses alliés des réponses globales à apporter à la répression transnationale. Par exemple, lors du Sommet du G7 de juin 2022, les dirigeants ont publié la Déclaration de 2022 sur les démocraties résilientes, par laquelle ils se sont engagés à renforcer la résilience contre la répression transnationale qui vise à miner la confiance envers le gouvernement, la société et les médias.

## 17.5 Des exemples d'activités de répression transnationale au Canada

Comme je l'ai indiqué plus haut, des témoins ont donné plusieurs exemples notables de répression transnationale menée au Canada qui, même s'ils ne sont pas nécessairement liés directement aux institutions démocratiques, fournissent des informations utiles sur le type d'activités clandestines et menaçantes auxquelles se livrent certains États étrangers au Canada. Ces témoignages étaient importants en eux-mêmes, mais aussi pour aider à contextualiser d'autres éléments de preuve portant sur l'ingérence étrangère.

Dans cette section, j'aborde deux exemples de répression transnationale qui m'ont été donnés au cours des audiences publiques.

### Les postes de police étrangers de la RPC

En septembre 2022, l'organisation non gouvernementale espagnole Safeguard Defenders a émis un rapport public alléguant que la RPC avait créé plus de 50 postes de police à l'étranger dans 29 pays, dont le Canada. Le rapport révèle que la RPC utilise les postes de police étrangers pour harceler, intimider et punir des individus à travers le monde dans le but de rapatrier des « fugitifs » en RPC.

AMC, Sécurité publique Canada, la GRC et le SCRS ont discuté de ce rapport. Des enquêtes ultérieures ont confirmé l'existence de postes de police étrangers au Canada. Le SCRS a communiqué des renseignements sur ceux-ci à la GRC. En octobre 2022, le cabinet du premier ministre a été informé de la question. Celle-ci a fait l'objet d'une discussion lors d'une réunion à l'échelon des sous-ministres.

Le sous-ministre adjoint responsable de la région indopacifique à AMC a expliqué que la RPC est très douée pour s'engager dans des activités relevant de la « zone grise ». Ces activités peuvent avoir un double objectif, à la fois légitime et illégitime.

Par exemple, les rapports des agences de renseignement indiquent que les postes de police étrangers ont assumé un certain nombre de fonctions qui ne sont pas directement liées à la répression transnationale, notamment en fournissant des services administratifs gouvernementaux comme le renouvellement des permis de conduire. Ces services ont pu être utiles aux membres de la communauté pendant la pandémie de COVID-19, lorsque les restrictions de voyage ont limité leur capacité à se rendre en RPC.

Cela dit, ces postes de police étrangers ont aussi été utilisés pour se livrer à de la répression transnationale. Les représentants infranationaux de la RPC semblent avoir dirigé ces postes de police étrangers pour tirer parti des

populations de la diaspora afin de mettre en œuvre les stratégies du DTFU, recueillir du renseignement et faciliter la répression transnationale, peut-être à l'insu ou sans l'approbation des autorités nationales de la RPC.

Les postes de police étrangers ont donc illustré comment les organismes communautaires pouvaient être utilisés comme outils efficaces pour permettre à la RPC de se livrer à de la répression transnationale sous prétexte de fournir des services utiles.

Le sous-ministre adjoint pour la région indopacifique à AMC a cependant expliqué que, du point de vue du droit international, la RPC a violé ses obligations en vertu de la *Convention de Vienne sur les relations consulaires* en opérant des postes de police étrangers au Canada, même s'ils n'avaient pas été impliqués dans la répression transnationale. Les postes exerçaient leurs activités sans l'accord du Canada, ce qui n'est pas permis. Ainsi, à son avis, la RPC devait être tenue responsable de ces postes.

Les postes de police étrangers ont posé des défis à la capacité du gouvernement d'utiliser les outils traditionnels pour intervenir. Certaines activités des postes de police étrangers étaient dirigées par des citoyens canadiens. Expulser du Canada ceux qui étaient responsables n'était donc pas envisageable, contrairement à ce qui aurait été le cas pour des représentants d'États étrangers.

La GRC a choisi de réagir en ayant recours à des tactiques de perturbation. Elle a déployé des agents en uniforme dans les postes de police étrangers pour faire connaître sa présence et échanger avec la communauté locale, directement et en publiant des documents. La GRC m'a confirmé que cette tactique de perturbation avait contribué à la fermeture des postes de police étrangers, bien qu'aucune accusation n'ait été portée. Shawn Tupper, qui était alors sous-ministre de la Sécurité publique, a déclaré qu'il s'agissait d'un exemple de la façon dont des activités perturbatrices peuvent parfois être aussi efficaces que des poursuites judiciaires.

La diplomatie a aussi joué un rôle important dans la réponse du Canada. Il y a eu de multiples interactions de haut niveau sur l'ingérence étrangère avec l'ambassade de la RPC à Ottawa entre octobre 2022 et avril 2023. À chacune de ces occasions, les représentants d'AMC ont fait part à leurs homologues de la RPC des préoccupations du Canada concernant les postes de police étrangers chinois.

Le 7 octobre 2022, AMC a demandé à l'ambassadeur de la RPC des renseignements détaillés sur les postes de police étrangers et l'a sommé de mettre fin à toute activité interdite par la *Convention de Vienne sur les relations consulaires*. Le 28 octobre, AMC a transmis une note diplomatique à la RPC insistant sur la fermeture des postes de police étrangers. Le 30 novembre 2022, AMC a reçu un avis officiel de l'ambassade de la RPC affirmant que ce qu'elle appelle les « centres de services chinois à l'étranger » n'étaient plus en activité. Il semble toutefois que cela n'était pas vrai.

Tout au long de l'année 2023, l'équipe du MRR du Canada a analysé les services fournis par des postes de la RPC nouvellement identifiés en s'appuyant sur le travail réalisé par Safeguard Defenders. Sur la base de ces recherches, le 24 février 2023, AMC a exigé à nouveau que la RPC mette un terme aux activités de tous les postes situés au Canada.

Tout au long de l'automne 2022 et jusqu'au début de l'année 2023, AMC a été en contact avec des pays aux visions similaires afin d'échanger sur la façon dont ces pays planifiaient répondre à la question des postes de police étrangers chinois. En outre, des discussions de haut niveau ont eu lieu avec certains dirigeants et ministres des affaires étrangères lors du Sommet de l'Asie de l'Est, du G20 et des réunions du forum de la Coopération économique de la zone Asie-Pacifique (l'APEC), afin de sensibiliser la communauté internationale à l'ampleur de l'ingérence étrangère de la RPC.

Durant les audiences publiques, j'ai entendu un large éventail de points de vue sur les actions de la GRC. Un membre de la communauté qui a participé à un panel de consultation de la Commission a qualifié la réponse de la GRC d'irresponsable et de préjudiciable aux institutions communautaires essentielles.

À l'inverse, un participant aux travaux de la Commission a laissé entendre aux témoins de la GRC que la réponse aux postes de police étrangers était trop « diplomatique » et qu'elle se distinguait donc de la façon dont la GRC réagit face à d'autres organisations criminelles. Les témoins de la GRC n'étaient pas d'accord avec cette caractérisation de leur intervention. Ils ont déclaré avoir adopté des approches similaires dans d'autres enquêtes, reconnaissant aussi que dans ce cas, il était particulièrement important d'établir un lien de confiance avec les membres de la communauté chinoise au Canada, qui étaient les victimes d'activités criminelles faisant l'objet de l'enquête.

Étant donné que cette affaire dépasse le cadre du mandat de la Commission et compte tenu des enquêtes en cours, je ne juge pas opportun de formuler des conclusions particulières.

## L'assassinat de Hardeep Singh Nijjar

Hardeep Singh Nijjar a été assassiné le 18 juin 2023 à Surrey, en Colombie-Britannique.

### Un lien entre le gouvernement indien et la mort de M. Nijjar

Des rumeurs ont immédiatement circulé selon lesquelles la mort de M. Nijjar serait liée au gouvernement de l'Inde, mais ce n'est pas ce que les agences de renseignement et de sécurité du Canada ont d'abord pensé. L'évaluation initiale était qu'il s'agissait d'un assassinat commis par un gang ou lié à la criminalité, ce dont le premier ministre a été informé.

Toutefois, les fonctionnaires canadiens ont commencé à entendre un certain nombre de députés canadiens d'origine sud-asiatique et d'autres membres de la communauté sud-asiatique affirmer avec insistance que l'assassinat était lié au gouvernement de l'Inde. Un certain nombre d'articles de presse ont également allégué que le gouvernement indien était impliqué et qu'il s'agissait peut-être de représailles pour l'assassinat de Ripudaman Singh Malik un an plus tôt. M. Malik avait été inculpé pour avoir contribué au financement de l'attentat à la bombe contre Air India, mais avait été acquitté en 2005.

À la lumière de ce qu'elles entendaient, les agences de renseignement ont continué à enquêter sur les circonstances de l'assassinat.

Au cours de l'été, lorsque le renseignement a révélé l'implication du gouvernement indien dans l'assassinat, le directeur du SCRS, David Vigneault (maintenant retraité), a informé la conseillère à la sécurité nationale et au renseignement auprès du premier ministre, Jody Thomas. Dans l'heure qui a suivi ce breffage, elle a informé le greffier du Conseil privé, John Hannaford. Le premier ministre a ensuite été informé rapidement de l'évaluation actualisée.

### **La réponse du gouvernement**

Le gouvernement souhaitait que l'Inde reconnaisse son implication dans l'assassinat, mais il devait également adopter une approche pragmatique pour résoudre le problème.

Le premier ministre a témoigné que l'approche du gouvernement a d'abord été de dialoguer avec le gouvernement de l'Inde et de communiquer l'idée qu'il était nécessaire pour les deux pays de collaborer tout en veillant à ce qu'il y ait reddition de comptes. Le Canada a également fait appel à ses alliés pour garantir une réponse collective et cohérente.

M<sup>me</sup> Thomas avait déjà prévu rencontrer son homologue indien, Ajit Doval, en août 2023. Elle et d'autres fonctionnaires du Bureau du conseil privé ont rencontré M. Doval, ainsi que les dirigeants de l'agence de renseignement et du bureau de police interne de l'Inde et des représentants de leur ministère des Affaires étrangères. Il s'agissait d'une réunion officielle : M<sup>me</sup> Thomas disposait d'un script indiquant ce qu'elle pouvait dire au sujet de l'enquête. Elle croit que M. Doval et ses collègues ont parfaitement compris que le Canada savait qu'il s'agissait d'un assassinat extrajudiciaire et qu'il dénonçait l'Inde pour son rôle dans l'assassinat de M. Nijjar.

Lorsque la ministre Mélanie Joly a pris connaissance du renseignement en août 2023, elle a commencé à faire part des préoccupations du Canada à son homologue de l'Inde, avec trois objectifs principaux : faire la lumière sur la nature de l'intervention de l'Inde, protéger la sécurité des Canadiennes et des Canadiens et protéger la souveraineté canadienne.

En septembre 2023, M. Vigneault, M<sup>me</sup> Thomas et M. Morrison se sont rendus en Inde pour le Sommet du G20, dont l'Inde était l'hôte. Le Canada avait initialement prévu profiter de ce sommet pour améliorer ses relations bilatérales avec l'Inde. L'assassinat de M. Nijjar a fait échouer ce projet. Au lieu de cela, juste avant le Sommet, ils ont rencontré leurs homologues en vue d'amener l'Inde à coopérer à l'enquête.

M<sup>me</sup> Thomas a déclaré que lors de sa deuxième rencontre avec M. Doval, ils avaient tous deux des scripts. Elle voulait communiquer que le Canada savait que l'Inde avait été impliquée dans l'assassinat tout en protégeant l'intégrité de l'enquête de la GRC alors en cours.

M. Morrison a dit à son homologue qu'il était très probable que la vérité finisse par éclater en raison de l'enquête canadienne, la publication d'un acte d'accusation aux États-Unis ou une fuite dans les médias.

M. Vigneault a lu son script mot pour mot. Son objectif était de situer cet événement dans le contexte plus large de cas précédents où le SCRS avait indiqué que le Canada était au courant des activités d'ingérence étrangère de l'Inde et qu'il les considérait comme problématiques. L'Inde n'a pas reconnu avoir été impliquée dans l'assassinat.

Le premier ministre Trudeau a décrit le Sommet du G20 comme un « moment important », où le gouvernement a travaillé en coulisse pour tenter d'obtenir la coopération de l'Inde. Ces efforts ont abouti à une conversation entre le premier ministre et Narendra Modi, le premier ministre de l'Inde, après la dernière séance du Sommet du G20. Le premier ministre a informé M. Modi que le Canada était au courant de l'implication de l'Inde et que cette information serait probablement rendue publique. M. Modi a répondu que le Canada hébergeait des gens que l'Inde voulait voir arrêtés, et il a demandé au Canada de partager le renseignement qu'il avait sur l'assassinat.

### **Les reportages médiatiques sur l'assassinat de M. Nijjar**

Peu après le G20, le gouvernement canadien a reçu des informations qui l'ont amené à penser que l'implication de l'Inde serait bientôt divulguée dans les médias. Le gouvernement a décidé qu'il devait informer la population canadienne qu'il était au courant des allégations concernant l'implication de l'Inde et qu'il enquêtait sur ces allégations dans l'intérêt de la sécurité publique. Le Canada a consulté ses alliés avant de faire cette déclaration.

Le 18 septembre 2023, le Globe and Mail a publié un article affirmant que les responsables canadiens détenaient de l'information à propos de la participation potentielle de l'Inde à la mort de M. Nijjar. À la suite de la publication de cet article, le premier ministre Trudeau a annoncé à la Chambre des communes que les agences de sécurité canadiennes menaient activement une enquête sur des allégations crédibles concernant un lien potentiel entre des agents du gouvernement indien et l'assassinat de M. Nijjar.

## La déclaration d'un diplomate indien *persona non grata*

Parallèlement, le Canada a déclaré un diplomate indien *persona non grata*.

L'Inde a réagi en déclarant un fonctionnaire canadien *persona non grata* et a également levé l'immunité diplomatique de 41 Canadiennes et Canadiens en Inde, les expulsant de fait. Des témoins ont qualifié cette réaction d'« extrême ». En raison de cette levée d'immunités diplomatiques, le Canada a fermé ses trois consulats en Inde.

Le MRR du Canada a également détecté une campagne de désinformation ciblant le premier ministre Trudeau, le haut-commissariat du Canada en Inde, les agences de sécurité nationale et du renseignement du Canada, la diaspora sikhe du Canada et les croyances politiques de M. Nijjar. Plusieurs médias alignés avec le premier ministre de l'Inde ont amplifié cette campagne. Les publications affirmaient que le premier ministre et les institutions canadiennes étaient des « complices du terrorisme » et des « traîtres contre Bharat (Inde) »<sup>30</sup>.

Le premier ministre a déclaré qu'il s'agissait d'une situation où il y avait des indications claires que l'Inde avait violé la souveraineté du Canada, mais que lorsqu'il avait été confronté à ce sujet, la réponse du gouvernement indien avait été de « doubler la mise » et d'attaquer encore plus le Canada.

## Réponse continue du gouvernement

AMC a indiqué que le Canada poursuivait ses efforts pour que les personnes responsables de l'assassinat de M. Nijjar répondent de leurs actes. Une enquête de la GRC est en cours et quatre personnes ont été arrêtées en mai 2024.

La question de l'ingérence étrangère et de la répression transnationale de l'Inde a évolué de manière assez spectaculaire au cours des audiences publiques de la Commission.

Le 14 octobre 2024, au milieu des audiences, la GRC a rendu publiques ses conclusions concernant l'implication d'agents du gouvernement indien dans des activités criminelles graves au Canada.

Simultanément, AMC a annoncé que le Canada avait expulsé six diplomates et responsables consulaires indiens à la suite d'une campagne entreprise contre des citoyens canadiens par des agents liés au gouvernement de l'Inde. Ces six personnes ont été identifiées comme des personnes d'intérêt dans l'assassinat de M. Nijjar.

Le premier ministre a déclaré que la décision de faire cette annonce était fondée sur des considérations de sécurité publique, l'objectif étant de

---

<sup>30</sup> Mécanisme de réponse rapide du Canada, *Manipulation d'information et ingérence étrangères potentielles à la suite de la déclaration du premier ministre sur l'assassinat de Hardeep Singh Nijjar*, p. 1, CAN025923.

perturber la chaîne d'activités criminelles liées à l'Inde, ciblant principalement la communauté sikhe au Canada, et la collecte secrète d'information par les diplomates indiens au sujet de Canadiennes et de Canadiens opposés au gouvernement de M. Modi.

### **Le défi de l'attribution**

Les événements décrits ci-dessus illustrent bien à quel point il peut être difficile de décider de la nécessité, du moment et de la manière d'attribuer publiquement des activités d'ingérence étrangère à un État particulier. Beaucoup d'éléments entrent en jeu et les conséquences peuvent être graves.

## 17.6 Conclusion

Comme je l'ai indiqué plus haut, le mandat de la Commission ne me demandait pas de mener une étude approfondie de la répression transnationale au Canada. Par conséquent, le travail effectué par la Commission à cet égard ne fait probablement qu'effleurer la surface de ce phénomène.

Ce que les travaux de la Commission m'ont permis de constater, cependant, c'est la gravité du problème que constitue la répression transnationale, la nocivité de ses effets sur des personnes au Canada et l'importance pour le gouvernement d'y répondre de manière significative.

Toute réponse efficace à l'ingérence étrangère doit tenir compte de la répression transnationale à laquelle se livrent certains États au Canada.

À mon avis, le gouvernement doit d'ailleurs s'intéresser d'encore plus près à la répression transnationale et aux conséquences graves qu'elle peut avoir sur certaines Canadiennes et certains Canadiens. Il s'agit d'un enjeu complexe.

## CHAPITRE 18

# La motion de la Chambre des communes sur le rapport du CPSNR

18.1	Introduction	122
18.2	La motion de la Chambre des communes	124
18.3	L'enquête de la Commission	126
18.4	Observations sur le renseignement	129
18.5	Discussion sur les affirmations identifiées dans le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)	132
18.6	Le renseignement et le défi de l'équité procédurale	138
18.7	La réponse du gouvernement	141
18.8	Conclusions sur le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)	143

**Les informations peuvent être incomplètes :** des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.

## 18.1 Introduction

Le 3 juin 2024, le Comité des parlementaires sur la sécurité nationale et le renseignement (le « **CPSNR** ») a publié une version publique caviardée de son *Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada* (le « **rapport du CPSNR** »). Les répercussions de ce rapport sur le débat public concernant l'ingérence étrangère ont été immédiates puisqu'il contenait des affirmations selon lesquelles certains élus aidaient des États étrangers « sciemment » ou « semi-sciemment »<sup>31</sup>. Ces affirmations ont suscité de vives inquiétudes dans les médias, au sein du public et dans les couloirs du Parlement lui-même.

La Chambre des communes m'a demandé d'enquêter sur les affirmations formulées dans le rapport du CPSNR. Cette tâche s'est avérée particulièrement difficile.

Je tiens tout d'abord à souligner une évidence. Le rapport du CPSNR est l'aboutissement d'un travail considérable et très important. Il s'agit d'une synthèse impressionnante et détaillée d'une vaste quantité d'informations. Ce rapport a apporté une contribution considérable et précieuse à la sensibilisation du public au sujet de l'ingérence étrangère. Mes remarques dans ce chapitre ne doivent en aucun cas être interprétées comme une remise en cause de tout ce qui précède.

Dans le cadre de l'enquête demandée par la Chambre des communes, la Commission a examiné la version classifiée du rapport du CPSNR ainsi que le renseignement que le CPSNR a pris en compte pour rédiger son rapport. La Commission a ensuite entrepris la tâche de produire un résumé pouvant être divulgué publiquement des affirmations contenues dans le rapport du CPSNR selon lesquelles des parlementaires aidaient « semi-sciemment » ou « sciemment » des États étrangers. Ce résumé a été déposé en preuve lors des audiences publiques de la Commission.

La Commission a également examiné un grand nombre d'informations supplémentaires dont le CPSNR ne disposait pas, notamment le

<sup>31</sup> Dans la version anglaise de son Rapport, le CPSNR emploie les termes *witting* et *semi-witting* ou leurs dérivés pour qualifier les activités de ces parlementaires. Dans la version française de son rapport, le CPSNR utilise différents termes pour traduire ces notions. Pour ma part, dans ce chapitre, j'utiliserai les termes suivants, selon le contexte, pour référer à ces notions : « sciemment », « volontairement » ou « en connaissance de cause », puis « semi-sciemment » ou « semi-volontairement ».

renseignement brut et les rapports opérationnels sous-jacents aux documents sur lesquels le CPSNR s'est appuyé. La Commission a obtenu d'autres informations écrites du gouvernement et a interrogé à huis clos de hauts fonctionnaires du Service canadien du renseignement de sécurité (le « **SCRS** ») et du Bureau du Conseil privé (le « **BCP** »).

Ce volet de l'enquête de la Commission a été révélateur. Ce que j'ai appris a été à la fois surprenant et instructif. Ce que j'ai observé de plus important au cours de l'enquête sur le rapport du CPSNR concerne la nature du renseignement : ce qu'il est et ce qu'il n'est pas, comment il devrait être utilisé et comment il ne devrait pas l'être.

Le renseignement peut évidemment être extrêmement précieux afin d'informer le gouvernement et lui permettre d'élaborer des politiques et de répondre aux menaces. Mais il existe des limites inhérentes quant à ce qu'il peut faire et à la façon dont il peut être communiqué. Les fragilités du renseignement font en sorte qu'il est dangereux de s'y fier sans réserve. Cela vaut en particulier pour le renseignement pouvant suggérer des inconduites de la part d'individus, comme la participation de parlementaires à des activités d'ingérence étrangère. Le renseignement ne doit jamais être traité ou rapporté comme s'il s'agissait d'un fait incontestable. Et le renseignement à lui seul ne doit pas être utilisé pour porter un jugement sur des personnes qui n'ont pas l'occasion de se défendre.

Le fait que le rapport du CPSNR, même la version classifiée, ne nomme pas les parlementaires auxquels il fait référence témoigne d'une compréhension et d'une prise en compte de ces préoccupations.

Cependant, le rapport du CPSNR formule néanmoins, en termes forts et sans équivoque, des affirmations contre certains parlementaires. Ces affirmations ont eu l'effet (peut-être de façon non voulue) de semer une grande consternation dans l'opinion publique, jetant un voile de suspicion sur tous les parlementaires (en particulier ceux issus de la diversité) et ont contribué à éroder la confiance des Canadiennes et des Canadiens dans leurs institutions démocratiques. Cela peut s'expliquer en partie par le fait que peu de gens connaissent les limites du renseignement, c'est-à-dire ce qu'il est et ce qu'il n'est pas, et comment il doit ou ne doit pas être utilisé.

L'enquête de la Commission m'a amenée à conclure que la consternation suscitée par le rapport du CPSNR, quoique compréhensible, est, à certains égards importants, injustifiée. La situation n'est peut-être pas aussi tranchée, et certainement pas aussi extrême, que les craintes suscitées par le rapport du CPSNR pourraient laisser entendre.

À mon avis, certaines conclusions du rapport du CPSNR concernant la participation « volontaire » de certains parlementaires à des activités d'ingérence étrangère sont plus définitives que ce que le renseignement sous-jacent permet de soutenir. Elles contiennent parfois des inexactitudes, soit dans la manière dont le renseignement est décrit, soit en raison d'inexactitudes dans le renseignement lui-même.

En termes clairs, cela ne signifie pas que les comportements rapportés ne sont pas préoccupants. Il y a des préoccupations légitimes par rapport à des parlementaires ayant possiblement des relations problématiques avec des représentants étrangers, démontrant un mauvais jugement, agissant avec naïveté, et peut-être, possédant une conduite douteuse sur le plan éthique. Mais je n'ai pas vu de preuve indiquant que des parlementaires conspirent avec des États étrangers contre le Canada. Si certains comportements peuvent être préoccupants, je n'ai pas vu de preuve indiquant la présence de « traîtres » au sein du Parlement.

Fondamentalement, ce que je retiens de cet aspect de mon enquête est qu'il faut être très prudent lorsqu'on utilise du renseignement pour tirer des conclusions sur des personnes, et encore plus lorsqu'on en fait état publiquement.

## 18.2 La motion de la Chambre des communes

Le 6 mars 2023, le premier ministre a demandé au CPSNR d'évaluer l'état de l'ingérence étrangère dans le cadre des élections générales de 2019 et de 2021. Le CPSNR a décidé de mener une étude plus large sur l'ingérence étrangère dans les institutions et les processus démocratiques fédéraux, englobant à la fois les parlementaires et le processus parlementaire.

Le 22 mars 2024, le CPSNR a produit son rapport classifié et l'a présenté au premier ministre. Le 3 juin 2024, il a publié une version caviardée du rapport pouvant être divulguée publiquement.

La version publique contient des affirmations qui ont généré des préoccupations importantes au sein du public. Par exemple, il contient une affirmation voulant que « certains représentants élus [aient] commencé sciemment à aider des acteurs étatiques étrangers peu de temps après leur élection », et une autre voulant que le CPSNR ait « vu des renseignements inquiétants selon lesquels certains parlementaires sont, aux dires des services de renseignement, des *participants* mi-consentants ou volontaires aux efforts d'ingérence des États étrangers dans la politique du pays »<sup>32</sup>. Cette dernière affirmation est suivie de cinq cas de figure illustrant une telle participation.

---

<sup>32</sup> Comité des parlementaires sur la sécurité nationale et le renseignement, *Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada*, para. 55, 164, COM0000362.

Ces affirmations ont suscité un tollé, qui s'est notamment traduit par des accusations voulant qu'il y ait des « traîtres » au sein du Parlement et par des demandes adressées au gouvernement pour qu'il nomme les élus qui avaient « sciemment » commencé à aider des États étrangers et auxquels le rapport du CPSNR faisait référence.

Dans ce contexte, le Bloc Québécois a déposé une motion à la Chambre des communes (la « **motion de la Chambre** »). Cette motion a été adoptée le 11 juin 2024. Elle demandait l'élargissement de mon mandat pour que la Commission puisse enquêter sur certaines affirmations contenues dans le rapport du CPSNR. La motion se lisait ainsi :

---

Que cette Chambre :

- (a) prenne acte du Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada du Comité des parlementaires sur la sécurité nationale et le renseignement;
  - (b) constate avec inquiétude que certains élus pourraient travailler volontairement ou involontairement aux intérêts de puissances étrangères;
  - (c) demande que le mandat de la commission sur l'ingérence étrangère (Commission Hogue) soit élargi pour lui permettre d'enquêter sur les institutions démocratiques fédérales du Canada, incluant les parlementaires de la Chambre des communes élus lors des 43<sup>e</sup> et 44<sup>e</sup> législatures ainsi que les parlementaires siégeant au Sénat<sup>33</sup>.
- 

Le 17 juin 2024, la Commission a pris acte de la motion de la Chambre et a indiqué qu'elle mènerait l'enquête demandée. Toutefois, aucune modification du mandat de la Commission n'a été nécessaire. La Commission a mené l'enquête dans le cadre de son mandat existant.

---

<sup>33</sup> Canada, Chambre des communes, *Journaux*, 44<sup>e</sup> législature, 1<sup>re</sup> session, No. 329 (11 juin 2024), pp. 4150-4152.

## 18.3 L'enquête de la Commission

### Le mandat de la Commission

Il est important de bien comprendre le mandat de la Commission en ce qui concerne le rapport du CPSNR.

Lors des audiences publiques de la Commission, dans les médias et au Parlement, plusieurs ont suggéré qu'il fallait, dans l'intérêt public, nommer les parlementaires auxquels réfère le rapport du CPSNR. Je tiens à expliquer ici pourquoi cela ne servirait pas l'intérêt public et pourquoi je ne divulgue pas ces noms.

D'emblée, je veux dissiper l'idée que le rapport classifié du CPSNR comportait une liste de parlementaires soupçonnés de travailler dans l'intérêt d'un État étranger. Ce n'est pas le cas. Le rapport du CPSNR ne nomme pas de parlementaires.

Le rapport classifié du CPSNR comportait plusieurs passages décrivant la conduite ou les activités de parlementaires non nommés. Ces passages comportent des notes en bas de page mentionnant les produits de renseignement sur lesquels le CPSNR s'était appuyé pour formuler ces affirmations. Identifier les personnes auxquelles le CPSNR fait allusion a donc été un exercice de « rétro-ingénierie », non seulement pour la Commission, mais aussi pour le SCRS lorsqu'il a examiné le rapport du CPSNR.

Comme je l'ai expliqué au chapitre 3 (volume 2), le mandat de la Commission n'est pas de tenter de démasquer et d'identifier des personnes ou des organisations qui agissent comme agents présumés de l'ingérence étrangère. Le mandat consiste à examiner et à évaluer la capacité du Canada à détecter, à prévenir et à contrer l'ingérence étrangère dans ses institutions démocratiques, notamment les processus électoraux. Cela implique d'examiner le renseignement dont dispose le gouvernement sur de potentielles activités étrangères menées par divers acteurs étatiques hostiles, notamment dans le cadre de leurs interactions avec les élus, et d'évaluer la façon dont le gouvernement y répond. Il ne s'agit pas de juger de la culpabilité de quelque élu que ce soit.

En fait, juger de la culpabilité d'un élu, ou de toute autre personne, contreviendrait aux obligations légales de la Commission et aux exigences d'équité procédurale. L'article 13 de la *Loi sur les enquêtes* interdit expressément à la Commission de rédiger un rapport défavorable concernant une personne (c'est-à-dire un constat qui jetterait le discrédit sur cette personne ou serait nuisible à sa réputation) à moins qu'elle ait été informée de ce qui lui est reproché et ait eu la possibilité de se faire entendre à ce sujet. Si la Commission avait enquêté sur des parlementaires en particulier dans la perspective de déclarer dans son rapport qu'ils ont sciemment

participé à des actes d'ingérence étrangère, elle serait légalement tenue de leur donner un préavis, l'accès à la preuve retenue contre eux et la possibilité d'y répondre. Cela n'a jamais été envisagé par mon mandat.

De plus, la procédure prévue à l'article 13 serait impossible à respecter lorsque l'information s'appuie sur du renseignement hautement classifié. Le simple fait de mentionner que le rapport du CPSNR fait référence à la conduite d'un parlementaire en particulier constituerait une information classifiée. Cette divulgation, sans parler des détails des affirmations elles-mêmes, pourrait révéler les capacités d'enquête du SCRS à des adversaires et mettre des sources en danger. Cela irait à l'encontre de l'obligation de la Commission de ne pas divulguer des informations qui pourraient être préjudiciables aux intérêts cruciaux, à la défense nationale ou à la sécurité nationale du Canada, ou de ses alliés. Cela pourrait même constituer une infraction criminelle en vertu de la *Loi sur l'ingérence étrangère et la protection de l'information*.

De plus, la Commission est tenue, aux termes de son mandat, de veiller à ce que ses travaux ne compromettent aucune enquête ou procédure criminelle en cours. La Commission, en menant son enquête à la suite de la motion de la Chambre, a respecté cette obligation, tout comme le compte rendu que j'en fais ici.

## Le processus de la Commission

Avant de passer à mes conclusions, il est important de comprendre comment la Commission a mené son enquête sur les affirmations contenues dans le rapport du CPSNR.

En premier lieu, la Commission a examiné attentivement les versions classifiée et non classifiée du rapport du CPSNR pour y repérer les affirmations relevant de la motion de la Chambre, c'est-à-dire celles concernant les parlementaires fédéraux qui pourraient « travailler volontairement ou involontairement aux intérêts de puissances étrangères ». La Commission n'a pas enquêté sur d'autres affirmations contenues dans le rapport du CPSNR, telles que celles concernant des politiciens non fédéraux. Bien que le rapport du CPSNR comporte une discussion à ce sujet, parmi d'autres sujets importants, la motion de la Chambre ne demandait pas à la Commission de les examiner.

La Commission s'est efforcée de repérer les affirmations selon lesquelles des parlementaires fédéraux, actuels ou anciens, auraient agi « volontairement » (en connaissance de cause) ou « semi-volontairement » (en connaissance de cause partielle ou par aveuglement volontaire) dans l'intérêt d'États étrangers. J'utilise l'expression « les affirmations identifiées » pour faire référence à ces affirmations.

Chacune des affirmations identifiées dans le rapport du CPSNR renvoie à une note en bas de page. En juillet 2024, la Commission a demandé au gouvernement d'identifier tous les documents mentionnés dans ces notes en bas de page, ainsi que tous les autres documents qui ont été présentés à la Commission et qui étaient pertinents pour l'examen des affirmations identifiées. Elle a également demandé et obtenu les rapports de renseignement sous-jacents, c'est-à-dire ceux auxquels les documents mentionnés dans chaque note en bas de page font eux-mêmes référence ou sur lesquels ils s'appuient. La Commission a aussi requis, et obtenu, toutes les informations et tout le renseignement pertinents qui ne lui avaient pas encore été remis. Elle a demandé que le renseignement sous-jacent, y compris les rapports opérationnels, lui soit remis. Elle avait en effet besoin de voir les informations sous une forme aussi « brute » et détaillée que possible pour pouvoir évaluer adéquatement les affirmations identifiées dans le rapport du CPSNR.

Ce processus a permis à la Commission d'examiner tout ce que le CPSNR a consulté en préparant le rapport du CPSNR, et même plus. Comme je l'explique ci-dessous, l'examen minutieux du renseignement a permis à la Commission d'identifier des divergences entre ce qu'indique le renseignement et ce qu'affirme le rapport du CPSNR. Dans certains cas, les informations décrites dans le renseignement étaient tout simplement erronées, ou des erreurs ont été commises dans leur évaluation.

Après un premier examen, la Commission a demandé au gouvernement qu'il lui fournisse, par écrit, des informations supplémentaires sur chaque affirmation identifiée. Ces informations portent notamment sur la manière dont le renseignement a été diffusé tant à l'intérieur qu'à l'extérieur du SCRS, et sur les mesures prises en réponse. La Commission a également demandé au gouvernement d'indiquer et de produire, s'il ne l'avait pas déjà fait, le renseignement à l'appui de certains aspects précis de chaque affirmation identifiée. De plus, la Commission a demandé au gouvernement de répondre à des questions plus précises à propos de certaines affirmations et du renseignement qui s'y rapporte.

La Commission a ensuite interrogé à huis clos de hauts fonctionnaires du SCRS et du Bureau du Conseil privé (BCP) sur les informations et le renseignement liés aux affirmations identifiées, ainsi que sur les enquêtes qui avaient généré ce renseignement. Avant ses audiences publiques en septembre et octobre 2024, la Commission a produit des résumés contenant toutes les informations obtenues lors de ces interrogatoires que les considérations de sécurité nationale permettaient de divulguer publiquement. Les informations hautement confidentielles ont fait de cette tâche un énorme défi, et je suis heureuse que la Commission l'ait relevé. Cela a permis à la Commission et aux parties d'interroger de nouveau de hauts fonctionnaires du SCRS et du BCP à ce sujet lors des audiences publiques de la Commission en octobre.

## 18.4 Observations sur le renseignement

### La nature du renseignement

Le renseignement est un outil important qui permet au Canada d'élaborer ses réponses aux menaces à la sécurité nationale. Le renseignement peut contribuer à l'élaboration de politiques, à déterminer quelles réponses diplomatiques donner et à orienter les enquêtes. Il peut donner aux personnes et aux groupes concernés une connaissance situationnelle, et les moyens de renforcer la résistance aux menaces.

L'enquête de la Commission, y compris son enquête sur les affirmations du rapport du CPSNR, rappelle toutefois que le renseignement a des limites. Les conclusions que l'on peut en tirer sont limitées, par exemple, par le contenu de ce qui a été collecté et par la manière dont cette collecte a été effectuée. Aussi précieux que soit le renseignement, il présente des faiblesses inhérentes. Ces faiblesses font en sorte qu'il est dangereux de s'y fier sans réserve, en particulier lorsqu'il s'agit de tirer des conclusions sur des personnes. Le renseignement ne devrait jamais être traité ou rapporté comme s'il constituait un fait avéré.

### La perte d'exactitude et de nuance lorsque le renseignement est résumé

Dans son examen du rapport du CPSNR, la Commission a eu l'avantage notable de pouvoir retracer la manière dont le renseignement était rapporté à travers plusieurs produits de renseignement. La Commission a pu voir comment les informations étaient présentées dans les rapports opérationnels et comment elles évoluaient au fur et à mesure qu'elles migraient vers des rapports de renseignement, des évaluations plus précises, des examens externes (comme le rapport du CPSNR classifié) et finalement vers des documents publics épurés (comme le rapport du CPSNR non classifié). Cet exercice a permis à la Commission de mieux comprendre les défis très concrets qui doivent être relevés pour pouvoir garantir l'exactitude des informations à mesure qu'elles franchissent ces étapes, en passant du domaine classifié au domaine public.

Au niveau opérationnel, les informations sont recueillies pour construire et renforcer la compréhension qu'a le gouvernement des activités d'un acteur menaçant ou pour déterminer les prochaines étapes d'une enquête. Au fur et à mesure que le renseignement brut est utilisé pour développer des produits de renseignement plus raffinés, un contexte plus grand peut se dégager et une image plus complète peut émerger. Toutefois, l'évolution peut aussi se

faire dans l'autre sens, en supprimant la subtilité, la nuance et la précision. C'est la conséquence inévitable de la synthèse de l'information.

Comme je l'ai appris, ce problème empire de façon exponentielle lorsque les informations sont soumises à un examen de sécurité nationale afin qu'elles puissent être rendues publiques. Un témoin du SCRS a déclaré que ce processus supprimait inévitablement des détails, entraînait une perte de contexte et menait à l'abstraction. Par exemple, je suis bien consciente qu'en raison des préoccupations de sécurité, je peux seulement discuter ici des affirmations contenues dans le rapport du CPSNR en termes généraux et abstraits, sans révéler les spécificités et les détails dont dispose la Commission. C'est d'ailleurs le cas pour de nombreux sujets abordés dans ce rapport. Mais cela pose un problème particulier dans le cas présent, car il limite la mesure dans laquelle je peux expliquer ce que j'ai constaté et augmente considérablement le risque qu'un lecteur ne soit pas en mesure de comprendre, ou qu'il interprète erronément, ce que la preuve a réellement révélé.

Cela ne signifie pas pour autant que les rapports publics n'ont aucune valeur. Au contraire, ces rapports peuvent contribuer grandement à la compréhension qu'a le public de l'ingérence étrangère.

Mais nous ne pouvons ignorer le fait qu'en passant de l'espace classifié à l'espace non classifié, des détails, du contexte et des nuances peuvent être perdus. Le produit final est inévitablement incomplet et omet nécessairement des informations pertinentes. Il y a un danger très réel qu'il puisse induire en erreur. C'est une préoccupation que j'ai eue tout au long des travaux de la Commission et que celle-ci s'est efforcée d'éviter. Je ne peux qu'espérer, sans toutefois pouvoir le garantir, que nous y sommes parvenus.

## Les difficultés à évaluer le « caractère volontaire » des actes des parlementaires

Il est d'une importance primordiale pour l'interprétation des rapports de renseignement ayant trait à l'ingérence étrangère et aux parlementaires de comprendre que les parlementaires font rarement l'objet d'enquêtes du SCRS en lien avec l'ingérence étrangère. Le SCRS recueille généralement des informations sur leur implication potentielle d'une manière accessoire lorsqu'il mène des enquêtes sur les acteurs menaçants étrangers. Ce point peut sembler technique, mais il a des répercussions importantes. J'ai également appris qu'il est souvent oublié dans le discours portant sur l'implication potentielle de parlementaires dans des activités d'ingérence étrangère.

Le fait que les parlementaires fassent rarement l'objet d'enquêtes en lien avec l'ingérence étrangère est important pour au moins deux raisons.

Premièrement, cela signifie qu'il y aura des lacunes dans ce que le SCRS sait de l'implication potentielle d'un parlementaire dans des activités d'ingérence étrangère. Comme les parlementaires ne font généralement pas l'objet ou ne sont pas au centre d'une enquête, le SCRS ne dispose que d'informations limitées à leur sujet. Pour illustrer ce que cela signifie en pratique, j'utiliserai un exemple qui n'a rien à voir avec l'ingérence étrangère.

Imaginons une enquête policière sur une organisation criminelle présumée. La police dispose d'un large éventail de techniques pour cibler l'organisation. Elle peut recourir à de l'écoute électronique, à des agents d'infiltration, à des informateurs, à la surveillance publique et à l'observation des médias sociaux. Ces techniques peuvent révéler que les membres de l'organisation criminelle misent sur le fait qu'un fonctionnaire donné est susceptible d'être corrompu.

Il s'agit là d'un renseignement utile sur l'organisation faisant l'objet de l'enquête. Il éclaire la police sur la nature et les intentions de cette organisation. Celle-ci semble avoir un intérêt à commettre des crimes et plus particulièrement semble cibler un fonctionnaire.

Mais qu'est-ce que cela révèle sur le fonctionnaire? Voilà qui est beaucoup plus difficile à déterminer. Cela signifie peut-être que le fonctionnaire est ouvert à la corruption. Ou peut-être pas. Il se pourrait tout aussi bien que les criminels se trompent et que le fonctionnaire soit irréprochable. Comme la police ne cible pas le fonctionnaire, elle est moins susceptible d'avoir des informations permettant de faire la lumière sur ses motivations, ses objectifs, ses intentions ou ses actions. La police en sait beaucoup sur l'organisation criminelle, mais elle en sait très peu sur le fonctionnaire.

En ce qui concerne le renseignement en lien avec l'ingérence étrangère, les cibles et les méthodes peuvent être différentes, mais le principe fondamental est le même. Les parlementaires ne sont généralement pas au centre des enquêtes menées par les agences de renseignement, de sorte que le renseignement disponible comportera des lacunes à propos des actes et des motivations des parlementaires.

La deuxième conséquence découlant du fait que les parlementaires font rarement l'objet d'enquêtes en lien avec l'ingérence étrangère est liée à la première. Lorsque le SCRS obtient des informations selon lesquelles un parlementaire pourrait être impliqué dans des activités d'ingérence étrangère, il n'évalue pas nécessairement si le parlementaire agit en connaissance de cause. Ce n'est pas l'objectif de son enquête. L'objectif est plutôt de comprendre les activités de l'acteur menaçant étranger. Il s'agit là d'une réserve importante à garder à l'esprit lorsqu'on examine les affirmations contenues dans le rapport du CPSNR. Dans la plupart des cas examinés, le SCRS n'avait pas évalué si le parlementaire en question avait « volontairement » participé à l'ingérence étrangère. Les conclusions sur le « caractère volontaire » étaient de manière générale celles du CPSNR, et non du SCRS.

## 18.5 Discussion sur les affirmations identifiées dans le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)

En gardant à l'esprit les observations précédentes sur la nature du renseignement, j'examine le rapport du CPSNR lui-même.

### Le « caractère volontaire » des actes des parlementaires

Comme je l'indique ci-dessus, le SCRS n'évalue pas toujours si un parlementaire a agi en connaissance de cause. Voici deux conclusions sur le « caractère volontaire » des actes d'un parlementaire où le rapport du CPSNR va plus loin que le SCRS.

Dans une affirmation, le rapport du CPSNR réfère à ce qu'il qualifie d'« un exemple classique d'ingérence étrangère où un État étranger a soutenu un politicien volontaire<sup>34</sup> ». Le CPSNR s'appuie sur un document de breffage pour soutenir cette affirmation. Or, ce document de breffage ne fait pas référence à l'incident comme constituant un « exemple classique d'ingérence étrangère ». Un autre document lié à cette affirmation, mais non cité dans les notes en bas de page du rapport du CPSNR, réfère bien à cet incident comme constituant un « exemple classique d'ingérence étrangère » sans toutefois décrire le député concerné comme étant un « politicien volontaire ».

Dans une réponse écrite transmise à la Commission, le SCRS indique que le degré de connaissance qu'avait le député des détails, et le fait qu'ils constituaient de l'ingérence étrangère, étaient des éléments manquants du renseignement. Le SCRS a déterminé que le politicien était conscient de l'aide apportée par un État étranger et l'avait acceptée, mais n'a pas déterminé qu'il participait volontairement à de l'ingérence étrangère. Cette nuance, et l'élément manquant reconnu par le SCRS, sont importants.

Dans un autre passage, le rapport du CPSNR évoque ce qu'il décrit comme des exemples « de députés qui se sont employés à influencer leurs collègues pour le compte de l'Inde et qui ont proactivement fourni des renseignements confidentiels à des représentants indiens »<sup>35</sup>. En discutant d'un de ces

---

<sup>34</sup> Comité des parlementaires sur la sécurité nationale et le renseignement, *Rapport spécial sur l'ingérence étrangère dans les processus et institutions démocratiques du Canada*, para. 56, COM0000362.

<sup>35</sup> Comité des parlementaires sur la sécurité nationale et le renseignement, *Rapport spécial sur l'ingérence étrangère dans les processus et institutions démocratiques du Canada*, para. 55, COM0000362.

exemples, le SCRS a déclaré à la Commission qu’il n’avait pas réellement évalué si le député en question avait agi en connaissance de cause. Les témoins du SCRS ont insisté que le SCRS n’avait pas nécessairement évalué la conduite des parlementaires ou leur caractère volontaire, puisqu’il évalue plutôt les informations portant sur les États étrangers. Des informations sur les parlementaires ont été recueillies de manière accessoire et non parce que les parlementaires faisaient l’objet d’une enquête visant à déterminer s’ils représentaient une menace.

À mon avis, le rapport du CPSNR est allé trop loin en affirmant que des parlementaires ont agi en connaissance de cause ou par complicité.

Je comprends que le CPSNR est un comité de parlementaires, lesquels ont vu ces situations à travers leur regard de parlementaires, essentiellement en portant un jugement sur la conduite de collègues ayant, selon eux, franchi la ligne. Cependant, à mon avis, ces affirmations vont au-delà de ce que le renseignement disponible permet d’affirmer. Mais je dois également reconnaître que je n’ai pas examiné les informations sous le même angle que le CPSNR. Je me suis concentrée uniquement sur ce que le renseignement révélait.

## Les erreurs relatives au renseignement lui-même

Il est toujours important de reconnaître le risque que le renseignement soit simplement erroné. C’est pourquoi la Commission a entendu et répété à maintes reprises que ce n’est pas parce qu’une information figure dans le renseignement qu’elle représente un fait avéré. Les informations provenant de sources humaines ne sont pas toujours fiables. Il s’agit souvent de ouï-dire, au mieux. Le risque d’erreur humaine est considérable. De plus, les sources peuvent avoir des raisons de fabriquer des éléments ou être incitées à dire ce qu’elles pensent que les services de renseignement veulent entendre. Même les sources techniques, comme l’interception de communications privées, sont susceptibles de donner lieu à des erreurs en raison d’une mauvaise interprétation, d’une traduction inexacte, d’un manque de contexte et d’autres facteurs. Les professionnels du renseignement sont bien sûr formés pour évaluer la fiabilité de ces informations, mais procéder à cette évaluation reste plus facile à dire qu’à faire.

Un exemple clair de renseignement inexact a été mis en lumière lors de l’enquête de la Commission sur une affirmation identifiée dans le rapport du CPSNR. Le CPSNR a signalé qu’un élu avait fourni de manière proactive des informations confidentielles à des fonctionnaires indiens à un moment

donné<sup>36</sup>. Il s'agit d'une affirmation extrêmement grave, d'autant plus que les informations confidentielles en question étaient importantes.

Toutefois, en examinant cette affirmation, la Commission a découvert que les informations en question avaient déjà été rendues publiques par le gouvernement au moment où l'élu les avait prétendument fournies. En d'autres mots, si l'élu a effectivement fourni les informations aux fonctionnaires indiens, ces informations n'étaient nullement confidentielles au moment des faits. Elles avaient au contraire déjà été communiquées au public.

En termes clairs, cette erreur n'en était pas une que le CPSNR pouvait éviter. Le document du SCRS sur lequel le CPSNR s'est appuyé contenait la même erreur. Dans son rapport annuel classifié 2022-2023 transmis au ministre de la Sécurité publique, sur lequel le CPSNR s'est appuyé pour formuler cette affirmation, le SCRS décrit cet incident et indique que les informations en question étaient confidentielles. Au cours des audiences à huis clos de la Commission et de communications de suivi, le SCRS a finalement convenu qu'il semblait que les informations en question n'étaient pas confidentielles au moment où elles auraient été communiquées, et que le SCRS n'avait aucune autre indication voulant que l'élu ait partagé des informations confidentielles.

Un autre exemple de renseignement inexact – qui est sans rapport avec le volet de l'enquête portant sur le rapport du CPSNR – a fait surface pendant les travaux de la Commission. Comme je l'ai décrit au chapitre 10 (volume 3), la Commission a demandé au gouvernement de dresser la liste de tous les cas majeurs d'ingérence étrangère soupçonnée ciblant les processus démocratiques du Canada de 2018 à aujourd'hui et de les décrire. Comme je l'ai expliqué dans ce chapitre, la liste initiale comprenait sept cas présumés. Le septième cas a toutefois été éventuellement supprimé lorsque le SCRS a repéré des informations incontestables et accessibles au public qui réfutaient l'affirmation centrale provenant de ce renseignement. Je souligne d'ailleurs que les informations réfutées provenaient de sources considérées comme étant fiables. Je relève cet exemple afin de souligner le fait que le renseignement peut parfois être tout simplement erroné.

## Le renseignement est une mosaïque et une cible mouvante

Le renseignement est comme une mosaïque, un puzzle ou parfois même une tour Jenga. Il se compose de pièces individuelles qui sont des instantanés, des moments dans le temps – une conversation partielle ici, un rapport de source là. Ce n'est que lorsque ces éléments sont assemblés qu'une image

---

<sup>36</sup> Comité des parlementaires sur la sécurité nationale et le renseignement, *Rapport spécial sur l'ingérence étrangère dans les processus et institutions démocratiques du Canada*, para. 55, COM0000362.

juste, précise et cohérente peut être obtenue. Un élément de renseignement peut suggérer une inférence ou une conclusion, mais combiné à des informations supplémentaires, l'inférence ou la conclusion qui peut être tirée peut changer considérablement. S'appuyer sur un seul élément de renseignement sans apprécier plus largement le contexte dans lequel il s'inscrit risque de laisser le lecteur avec une compréhension déformée, voire trompeuse, d'une situation. La valeur ajoutée du processus d'évaluation du renseignement pour les décideurs provient en grande partie de la mise en contexte qui est ultimement fournie au lecteur. Comme l'a déclaré l'ancien directeur du SCRS, M. Vigneault, il est important de comprendre le renseignement dans son contexte.

Le fait que le renseignement évolue est tout aussi important. Il est dynamique et non statique. Le renseignement est recueilli à un moment précis. La manière dont ce renseignement est compris à un moment donné dépend de ce qui est connu au moment où il est examiné. Au fur et à mesure que de nouvelles informations apparaissent, la manière dont le renseignement est compris peut changer radicalement. Les évaluations qui sont faites peuvent devenir plus définitives, ou beaucoup moins. Des changements peuvent se produire au fil des ans, mais aussi du jour au lendemain. Un témoin du SCRS m'a dit qu'une personne peut sembler compromise un jour, mais que, le lendemain, le SCRS peut découvrir des informations qui modifient son évaluation.

Des témoins du SCRS m'ont indiqué que, si le SCRS évalue les activités d'un député, cette évaluation se fait sur une « échelle mobile », car le SCRS continue de recueillir accessoirement des informations quant à leurs activités. Il peut être difficile d'en prendre conscience lorsqu'on rapporte du renseignement à un moment précis. Mais cette appréciation est cruciale pour bien comprendre les conclusions qui peuvent, ou non, être tirées équitablement.

Deux exemples décrits dans ce chapitre montrent comment de nouvelles informations peuvent modifier fondamentalement la compréhension qu'on peut avoir de renseignement obtenu antérieurement.

Comme j'ai expliqué plus haut, le « septième cas » d'ingérence étrangère présumée identifié par le gouvernement se fondait sur du renseignement provenant de sources considérées comme fiables. Pourtant, dans ce cas, des informations facilement accessibles dans le domaine public ont conduit à une réévaluation et à son retrait de la liste.

Le SCRS a expliqué qu'il n'avait pas vérifié le renseignement concernant le « septième cas », car le député ne faisait pas l'objet de l'enquête. Puisque les parlementaires ne font que très rarement l'objet d'une enquête, je note que la plupart des informations recueillies à leur sujet sont également susceptibles de ne pas être vérifiées.

De même, il y a le cas du parlementaire qui, selon le SCRS, aurait fourni des informations « confidentielles » à l'Inde. Cette conclusion a dû être réévaluée

lorsque la Commission a souligné que les informations en question avaient déjà été rendues publiques à l'époque, et qu'elles n'étaient donc pas confidentielles. Le SCRS a tiré des inférences d'informations qu'il a reçues et n'a pas consulté des informations provenant de sources ouvertes facilement accessibles avant de conclure que le parlementaire avait transmis des informations confidentielles.

## Des erreurs dans la description du renseignement

Dans certains cas, il y a des erreurs dans la manière dont le rapport du CPSNR décrit ce que dit réellement le renseignement.

Par exemple, le rapport du CPSNR décrit deux situations où il est allégué qu'un même député aurait aidé un État étranger en particulier<sup>37</sup>. En décrivant la deuxième situation, le rapport classifié du CPSNR indique qu'il s'agit du même député que dans la première situation. Ainsi, le CPSNR a conclu qu'un seul et même député s'est livré aux activités décrites dans les deux situations.

Pourtant, d'après les notes en bas de page du rapport du CPSNR, et d'après d'autres éléments de renseignement dont dispose la Commission, ces deux affirmations ne semblent pas concerner le même député. Les rapports de renseignement relatifs à la deuxième situation font référence à un tout autre député. Cela est notable, puisqu'une personne raisonnable serait probablement plus portée à croire qu'un député a fait preuve d'une mauvaise conduite si le CPSNR mentionne deux situations distinctes où il aurait peut-être aidé un État étranger.

Dans un autre exemple, le rapport classifié du CPSNR indique qu'un État étranger a compromis un député. Le rapport utilise un langage particulier pour décrire la compromission. La note en bas de page accompagnant le texte renvoie à un produit de renseignement. Ce produit de renseignement utilise effectivement les termes particuliers contenus au rapport du CPSNR, mais il réfère à un État étranger différent de celui que le CPSNR identifie dans son rapport. Autrement dit, le CPSNR identifie le mauvais pays.

De plus, il y a un problème plus fondamental dans la façon dont le CPSNR rapporte le renseignement concernant ce député. Le rapport du CPSNR indique que le langage particulier mentionné ci-dessus représente l'évaluation qu'a faite le SCRS du député – c'est-à-dire que c'est le SCRS qui aurait déterminé que le député était compromis. Or, ce n'était pas le cas. Plutôt, dans un produit de renseignement que le CPSNR a examiné, le SCRS a rapporté les propos employés par un tiers, et non par le SCRS. « Quelqu'un a

---

<sup>37</sup> Comité des parlementaires sur la sécurité nationale et le renseignement, *Rapport spécial sur l'ingérence étrangère dans les processus et institutions démocratiques du Canada*, para. 55, COM0000362.

dit au SCRS que le député était compromis » est une affirmation très différente par rapport à « Le SCRS a évalué que le député était compromis ».

Dans un exemple additionnel, le rapport du CPSNR décrit les interactions entre un parlementaire et une personne décrite comme un « agent de renseignement non déclaré » affilié à un État étranger. Cette notion d'agent de renseignement « non déclaré » mérite une brève explication. Un agent de renseignement déclaré au Canada est une personne occupant un poste diplomatique légitime pour le compte d'un gouvernement étranger, au su du gouvernement canadien. Un agent de renseignement non déclaré est au contraire un espion.

Lorsque la Commission a examiné le renseignement cité par le CPSNR, elle a appris que la personne qualifiée d'agent de renseignement non déclaré (c'est-à-dire, un espion) est en fait un agent de renseignement *déclaré*, c'est-à-dire un représentant étranger légitime. Si le statut d'agent de renseignement n'était pas connu de tous (ce qui est normal), le SCRS a reconnu qu'il est probable que le parlementaire le savait. Ainsi, le rapport du CPSNR affirmait que le parlementaire a parlé à un espion étranger, alors qu'en réalité, le parlementaire s'était entretenu avec un représentant étranger légitime. Il y a là une différence.

Un autre exemple concerne ce que le rapport du CPSNR réfère à une situation qu'il qualifie de particulièrement inquiétante « où un ancien député entretenait une relation avec un agent de renseignement étranger ». Le rapport ajoute que, « d'après le SCRS, le député a cherché à organiser une réunion dans un État étranger avec un représentant haut placé du renseignement et a aussi proactivement fourni à l'agent de renseignement des informations reçues à titre confidentiel ». Quoique cela n'apparaisse pas dans le rapport public du CPSNR, le rapport classifié du CPSNR décrit aussi l'information en question comme étant « privilégiée ». À première vue, fournir des informations confidentielles et privilégiées à un agent de renseignement étranger semble en effet un geste particulièrement inquiétant.

Cependant, lorsque la Commission a enquêté sur cette affirmation, elle a découvert qu'il n'existait aucune indication voulant que les informations en question étaient dans les faits confidentielles ou privilégiées. Le SCRS a au contraire confirmé que ces informations n'étaient en fait ni classifiées ni privilégiées au sens juridique du terme. De plus, le SCRS ne savait pas si le député avait même été invité à garder l'information confidentielle. Voilà qui brosse un tableau assez différent de celui qui se dégage du rapport du CPSNR.

Les témoins du SCRS ont affirmé qu'ils considéraient que l'information était sensible, et que la décision du député de communiquer cette information à un représentant d'un État étranger constituait un signal d'alarme. Toutefois, le SCRS a déclaré à la Commission que le rapport du CPSNR avait utilisé des termes plus forts que ceux qu'il aurait lui-même employés pour décrire la situation.

Quant à l'affirmation selon laquelle le député a cherché à organiser une rencontre dans un autre pays avec un haut fonctionnaire du renseignement, la Commission n'a pas été en mesure d'enquêter sur cet élément en raison du trop peu d'informations disponibles à ce sujet. La Commission a demandé au SCRS de lui fournir toute information supplémentaire relative à cette affaire. Aucune n'a été fournie. Puisque la Commission a reçu tous les rapports fournis au CPSNR, je comprends que la conclusion dans le rapport du CPSNR était vraisemblablement fondée sur les mêmes informations limitées. C'est là une considération importante étant donné la gravité de l'affirmation.

La Commission a également identifié des informations plus récentes détenues par le SCRS qui ont fourni un contexte supplémentaire et important sur la relation entre le député et l'agent de renseignement, et sur les raisons pour lesquelles ils ont pu être en contact. Le CPSNR ne disposait pas de ces informations. Je les mentionne uniquement parce qu'elles sont, à mon avis, pertinentes pour comprendre adéquatement les affirmations concernant ce député.

## 18.6 Le renseignement et le défi de l'équité procédurale

Comme je l'ai mentionné ci-dessus, la conclusion principale que je tire de mon enquête sur les affirmations contenues dans le rapport du CPSNR est qu'il existe des limites inhérentes à ce que le renseignement peut faire et comment il devrait être utilisé.

Le renseignement est évidemment utile pour répondre aux menaces à la sécurité nationale, et il est d'une importance capitale pour l'élaboration des stratégies gouvernementales. Même si les agences de sécurité nationale et de renseignement ne disposent pas de toutes les informations nécessaires pour dresser un tableau complet d'une menace particulière, ils peuvent avoir assez d'informations pour informer utilement le gouvernement. Le gouvernement peut alors agir pour gérer les risques. Des éléments de renseignement peuvent permettre à un ministère de mettre en contexte d'autres informations qu'il détient ou de poser des questions différentes sur des informations qu'il reçoit d'autres sources. Les agences gouvernementales emploient des experts qui savent évaluer les informations tout en tenant compte de leurs limites.

Mais cela ne signifie pas que du renseignement peut être utilisé à toutes les fins. Le renseignement doit plutôt être utilisé de manière responsable, en tenant compte de ses limites, en particulier lorsqu'il s'agit de l'utiliser d'une façon qui aura des répercussions directes et importantes sur une personne.

Je reviens sur une observation que j'ai formulée au début de ce chapitre voulant qu'il aurait été inapproprié de me prononcer sur la culpabilité ou l'innocence de certains parlementaires. Pour des raisons que j'estime valables, qui sont liées à la sécurité nationale et à l'équité procédurale, je ne pouvais divulguer les noms de ceux auxquels le rapport du CPSNR semble référer. Je ne pouvais pas m'entretenir avec eux et leur donner l'occasion de comprendre les reproches qui leur étaient adressés. Je ne pouvais pas obtenir d'eux des informations susceptibles de confirmer ou d'infirmier d'autres éléments de renseignement que je pourrais avoir vus. Je ne pouvais pas leur donner la possibilité raisonnable de se faire entendre. En bref, il m'était impossible de mettre en œuvre une procédure équitable.

Pour cette raison, il serait fondamentalement injuste que je me prononce sur la question de savoir si un parlementaire particulier a pu commettre une faute en collaborant avec un État étranger.

Il s'agit là d'une préoccupation plus large quant à l'équité de traitement. Chaque fois que le gouvernement agit sur la base d'informations classifiées, il y a un risque que ses actions aient une incidence sur les droits ou les intérêts d'individus. Certaines incidences peuvent être mineures ou diffuses. D'autres peuvent être profondes et directes. Ces conséquences, et le fait que les individus peuvent n'avoir que peu, voire aucune possibilité de se défendre, doivent être pris en compte lorsque l'on décide d'agir sur la base du renseignement.

Par exemple, le premier ministre peut tout à fait prendre des décisions sur le choix des personnes à nommer au Cabinet en s'appuyant sur le genre de renseignement utilisé aux fins du rapport du CPSNR. Personne n'a un droit à occuper un poste ministériel. Je ne dis pas cela pour minimiser l'impact qu'une telle décision pourrait avoir sur la carrière ou les aspirations d'un individu. Cependant, en raison des intérêts en jeu des deux côtés, une telle décision serait défendable.

Cela dit, j'ai entendu des témoignages portant sur des cas de figure où les agences de renseignement ont fourni au premier ministre du renseignement sur des députés qui était susceptible d'affecter leur carrière, et où ce renseignement s'est révélé complètement erroné. La cheffe de cabinet du premier ministre a décrit une situation où une agence de renseignement avait identifié une menace liée à un député. Les fonctionnaires du cabinet du premier ministre lui ont posé des questions sur le renseignement qu'elle détenait. Après qu'il lui eut été demandé d'effectuer des vérifications supplémentaires, le SCRS s'est rendu compte qu'il s'agissait de la mauvaise personne et il a complètement modifié son évaluation.

Des exemples comme ceux-ci montrent pourquoi il serait injuste de s'appuyer sur du renseignement non vérifié pour qualifier publiquement un parlementaire de traître. Cela aurait une incidence profonde sur ce parlementaire, qui ne peut être justifiée à la lumière des faiblesses du renseignement et de l'incapacité à donner à cette personne une occasion raisonnable de se défendre.

La réticence du CPSNR à nommer des députés, même dans le rapport classifié du CPSNR, témoigne de l'attention louable accordée à cette question d'équité procédurale. Mais le rapport du CPSNR emploie des termes qui peuvent avoir été interprétés comme des conclusions définitives selon lesquelles de nombreux députés ont volontairement collaboré avec des États étrangers à l'encontre des intérêts du Canada. L'accent y est mis sur les députés, comme si c'étaient eux, et non les États étrangers, qui sont les acteurs menaçants. Il est rédigé comme si le renseignement constituait des faits avérés. Et il ne mentionne pas que le CPSNR n'a bénéficié d'aucune information provenant des parlementaires en question. L'effet global qui en résulte est de laisser croire (peut-être de façon non voulue) que certains parlementaires sont effectivement des « traîtres » envers notre pays. À mon avis, cela va beaucoup plus loin que ce que le renseignement suggère.

Cet aspect de l'enquête de la Commission m'a fait réfléchir au défi auquel sont confrontés des organismes comme le CPSNR, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (l'« **OSSNR** »), le Rapporteur spécial indépendant sur l'ingérence étrangère (le « **RSI** ») et, bien sûr, cette Commission. On leur demande d'examiner la conduite d'individus, d'enquêter et de rendre compte de leurs conclusions. Aucun de ces organismes n'est conçu pour agir comme un tribunal chargé de se prononcer sur la culpabilité ou l'innocence, la responsabilité ou l'absence de responsabilité d'un individu. Certes, ils peuvent – et doivent – se prononcer sur la conduite des institutions publiques. Mais porter un jugement sur des individus est très différent. Le renseignement ne peut pas, à lui seul, fonder une telle conclusion. Les commissions d'enquête qui n'ont pas à traiter de renseignement sont mieux équipées pour examiner la conduite d'individus particuliers. Pouvant offrir une plus grande équité procédurale, elles sont mieux placées pour tirer des conclusions sur la conduite des individus (mais pas sur leur responsabilité). L'entrée en scène du renseignement change la donne. Le renseignement est complexe, nuancé et presque toujours incomplet.

Le renseignement est également secret par nature. Des organismes comme l'OSSNR, le CPSNR, le RSI ou cette Commission peuvent travailler à promouvoir l'ouverture et la transparence. Mais ils ne peuvent pas divulguer complètement le renseignement dont ils disposent ni garantir une procédure équitable à ceux dont la conduite a été remise en question. Ils peuvent interroger et sonder la conduite des agences de renseignement, leurs évaluations et leurs conclusions. Mais ils ne peuvent prétendre porter un jugement sur ces personnes alors que l'équité exige de leur offrir le droit de se défendre.

Les organes de surveillance sont des acteurs extrêmement importants et précieux dans l'architecture de la sécurité nationale du Canada. Chacun d'entre eux apporte un ensemble distinct de compétences, de pouvoirs et d'aptitudes à l'objectif commun et d'une importance vitale qu'est celui d'assurer la responsabilité et la transparence. J'espère que les travaux de cette Commission contribueront aux efforts considérables qu'ils déploient.

Lorsque nous menons une enquête ou rédigeons un rapport, nous devons être conscients de nos forces, mais aussi de nos faiblesses. Il faut prendre au sérieux les limites de ce que nous pouvons accomplir. Il faut aussi ne pas tenter de faire plus que ce que nous permettent nos compétences et capacités institutionnelles.

## 18.7 La réponse du gouvernement

Au cours de mon enquête, j'ai entendu des témoignages portant sur la réponse du gouvernement au renseignement à l'origine des affirmations identifiées. Je suis limitée dans ce que je peux dire sur les mesures précises que le gouvernement a prises en réponse aux affirmations individuelles. Toutefois, la preuve indique que, le cas échéant, certaines mesures ont été prises pour réduire la menace d'activités d'ingérence étrangère. Par exemple, j'ai entendu des témoignages voulant que le Pakistan aurait tenté de soutenir l'élection d'un candidat qu'il préférait. De l'information à ce sujet aurait été transmise à Élections Canada et au Bureau du commissaire aux élections fédérales puisque le renseignement aurait pu indiquer une contravention potentielle à la *Loi électorale du Canada* et qu'il pouvait leur fournir du contexte leur permettant d'améliorer leur compréhension des méthodes de certains États. J'ai aussi été informée d'une mesure de réduction de la menace (une « **MRM** ») particulière que le SCRS a utilisée pour répondre à certains éléments de renseignement liés aux affirmations identifiées ainsi que de ses résultats. Bien entendu, l'efficacité de ces mesures est difficile à évaluer.

Cela dit, on peut et doit toujours en faire plus. En particulier, cette partie de mon enquête a mis en évidence la nécessité d'une communication continue et accrue avec les parlementaires au sujet de l'ingérence étrangère. Le renseignement ne doit pas être surestimé et doit être lu en gardant à l'esprit d'importantes mises en garde. Il n'en reste pas moins qu'il suggère que certains élus ont entretenu des relations ou ont eu des interactions avec des représentants étrangers qui ont pu dépasser les limites de la diplomatie normale. Le renseignement indique également que certains élus ont pu savoir qu'ils avaient le soutien de représentants étrangers ou d'intermédiaires, bien que la mesure dans laquelle ils étaient conscients du lien que ce soutien pouvait avoir avec l'ingérence étrangère n'était pas nécessairement claire.

En termes clairs, cela ne signifie aucunement que ces élus sont des « traîtres ». Mais cela suggère, au minimum, que certains élus peuvent ne pas avoir su où se trouve la frontière entre l'ingérence étrangère et les activités diplomatiques acceptables. En effet, j'ai entendu des témoignages au sujet d'une MRM prise par le SCRS qui a clairement révélé un manque de sensibilisation à l'ingérence étrangère parmi les politiciens canadiens, et qui

a également indiqué que certains élus ne savent peut-être pas que les représentants étrangers ne devraient pas entreprendre certaines activités.

Des témoins du SCRS m'ont également indiqué que certains élus sont au fait de ce qu'est l'ingérence étrangère, mais ne savent pas toujours où tracer la ligne. De plus, une évaluation du renseignement réalisée en novembre 2021 indique que « l'un des plus grands défis pour les députés semble être de bien identifier l'ingérence étrangère et de savoir quoi faire lorsqu'ils pensent être ciblés », car de nombreuses interactions entre les députés et les représentants étrangers se situent dans la « zone grise » comprise entre l'influence étrangère, qui est légitime, et l'ingérence étrangère, qui est illégitime<sup>38</sup>. Cette méconnaissance peut rendre les députés susceptibles d'être exploités par des États étrangers.

Les élus ne sont pas les seuls à être confrontés au défi de repérer ce qui est et ce qui n'est pas de l'ingérence étrangère. Comme je l'explique au chapitre 10 (volume 3), différents ministères et organismes gouvernementaux parviennent parfois à des conclusions différentes sur la question de savoir si un ensemble de faits constitue de l'ingérence étrangère, et si c'est le cas, sur la gravité de cette ingérence.

Compte tenu de ce défi – qui touche même les fonctionnaires qui sont bien informés sur l'ingérence étrangère – nous ne pouvons pas nous attendre à ce que les élus soient en mesure de tracer facilement la frontière entre l'ingérence étrangère et l'influence étrangère sans davantage d'indications. Comme je l'explique plus en détail au [chapitre 15](#), l'un des moyens dont dispose le gouvernement pour contrer l'ingérence étrangère consiste à éduquer les parlementaires. Mon enquête sur les affirmations identifiées dans le rapport du CPSNR a montré l'importance de cet échange. Par exemple, offrir aux parlementaires une formation supplémentaire sur la distinction entre l'ingérence étrangère et une activité diplomatique acceptable pourrait aider à combler un certain manque en matière de connaissances et favoriser la résilience des parlementaires s'ils sont la cible d'activités d'ingérence étrangère. Je reviendrai sur ce point dans mes recommandations.

---

<sup>38</sup> Service canadien du renseignement de sécurité, La mobilisation du SCRS auprès des élus sur l'ingérence étrangère : Une initiative d'importance nationale, CAB 2021-22/89 (3 novembre 2021), p. 5, CAN003712\_R01.

## 18.8 Conclusions sur le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)

Le rapport du CPSNR a apporté une contribution importante à la compréhension qu'a le public de l'ingérence étrangère. Il identifie des sujets de préoccupation légitimes. Cependant, le discours public des derniers mois, ainsi que les témoignages et les observations des Participants aux travaux de la Commission, suggère que ces affirmations ont contribué à éroder la confiance du public envers les élus et envers les institutions démocratiques du Canada de manière plus générale. Cette situation est à la fois regrettable et injustifiée.

### L'ampleur du problème

En termes clairs, le fait que j'aie identifié certaines préoccupations relatives à des affirmations de participation volontaire à de l'ingérence étrangère dans le rapport du CPSNR ne signifie pas que la conduite des personnes en question était irréprochable. Certaines informations contenues dans le renseignement peuvent susciter des inquiétudes ou justifier la tenue d'une enquête plus approfondie. J'ai entendu des témoins du SCRS dire qu'ils pensaient qu'il y a et qu'il y avait eu des relations préoccupantes entre des élus et des États étrangers. Comme l'a expliqué la Conseillère à la sécurité nationale et au renseignement auprès du premier ministre, Nathalie Drouin, même si la conduite d'un député n'équivaut pas à une trahison, cela ne veut pas dire qu'il ne faut pas examiner ce comportement ou le redresser.

Comme je l'indique ci-dessus, le fait que des parlementaires méconnaissent l'ingérence étrangère, ne soient pas certains où la ligne est tracée ou fassent preuve d'un mauvais jugement ou d'une mauvaise éthique, sont des problèmes qui méritent notre attention.

Cependant, il ne faut pas exagérer l'inquiétude que devraient susciter les anciens élus et les élus actuels. Bien que certains comportements puissent être source d'inquiétude, je n'ai vu aucune preuve qu'il y a des « traîtres » au sein du Parlement. L'ancien directeur du SCRS, M. Vigneault, a témoigné qu'il y a eu très peu de cas dans l'histoire du SCRS où un député a été soupçonné de représenter une menace pour la sécurité nationale du Canada à titre personnel et en raison de ses liens avec un acteur menaçant. Vanessa Lloyd, sous-directrice des Opérations du SCRS, a souligné que le nombre d'individus qui comprennent ce qu'est l'ingérence étrangère et qui profitent volontairement de telles relations avec des États étrangers est très faible. Un

tel « degré de conscience » est très rare. Sur la base de ce que j’ai vu, rien ne suggère que je devrais être en désaccord avec ce constat.

Le rapport du CPSNR a eu raison de soulever des préoccupations sur l’ingérence étrangère visant les parlementaires. Il s’agit assurément d’un vrai problème. Mais, d’après le renseignement que j’ai examiné et la preuve que j’ai entendue, le problème est peut-être moins répandu et moins dramatique que le discours public auquel a donné lieu le rapport du CPSNR ne le laisse entendre.

## L’incidence du rapport du CPSNR

Les discussions publiques sérieuses portant sur les enjeux de sécurité nationale au Canada ont été minimales dans le passé. Comme je l’ai dit, le CPSNR a grandement contribué à rehausser le profil de ces enjeux et à les faire progresser. Je suis d’accord avec le greffier du Conseil privé, John Hannaford, pour dire que d’avoir un groupe comme le CPSNR qui se pencher sur des questions comme l’ingérence étrangère fait partie d’un important processus continu de renforcement de la résilience collective face à la menace. Le CPSNR a fourni aux Canadiennes et aux Canadiens une quantité importante d’informations sur l’ingérence étrangère. Je note d’ailleurs que la plupart des informations contenues dans le rapport du CPSNR n’étaient pas liées à des affirmations concernant des parlementaires en particulier.

Malheureusement, les commentaires sur les parlementaires ont attiré l’attention du public, avec des conséquences troublantes. Cela est particulièrement vrai pour les députés qui sont membres de certaines communautés issues des diasporas. Par exemple, la députée Jenny Kwan – elle-même victime présumée d’ingérence étrangère – a témoigné que le rapport avait jeté un voile de suspicion sur les parlementaires. Elle a raconté qu’en passant devant la Chambre des communes, alors qu’elle se rendait à une réunion de comité, elle a été confrontée à des manifestants qui qualifiaient les parlementaires, dont elle, de « traîtres ». Comme l’a expliqué M<sup>me</sup> Kwan, le problème de ce voile de suspicion, au-delà des ramifications personnelles, est que l’intégrité du Parlement lui-même est remise en question. Et affaiblir les institutions démocratiques et les élus est exactement ce que veulent les acteurs menaçants.

# Conclusions quant à la capacité du gouvernement à détecter, prévenir et contrer l'ingérence étrangère

Le décret créant la Commission m'enjoignait d'abord d'examiner et d'évaluer l'ingérence de la Chine, de la Russie et d'autres acteurs étatiques ou non étatiques étrangers, ainsi que toute répercussion potentielle de cette ingérence, afin de confirmer l'intégrité et les répercussions, le cas échéant, sur les 43<sup>e</sup> et 44<sup>e</sup> élections générales (les élections de 2019 et de 2021) à l'échelle nationale et à celle des circonscriptions.

Cet examen a été réalisé essentiellement lors de la première phase des travaux de la Commission. Ces travaux m'ont permis de conclure dans mon rapport initial que les élections générales de 2019 et de 2021 ont sans aucun doute fait l'objet d'ingérence étrangère. J'ai cependant conclu que cette ingérence n'a pas porté atteinte à l'intégrité du système électoral lui-même et n'a pas eu d'incidence sur l'identité du parti qui a pris le pouvoir. Alors qu'il était difficile de déterminer avec certitude si cette ingérence a eu ou non une incidence sur le résultat des élections au niveau des circonscriptions, j'ai reconnu la possibilité qu'elle ait affecté certains résultats, mais dans un nombre très limité de circonscriptions.

Les travaux de la Commission réalisés depuis le dépôt du rapport initial ne m'ont pas conduit à modifier ces conclusions. Or, ils ne m'ont pas non plus permis de modifier ma conclusion voulant que l'ingérence étrangère ait eu une incidence sur l'écosystème électoral dans son ensemble et ait ébranlé la confiance du public envers la démocratie canadienne. Au contraire, mes travaux depuis le dépôt du rapport initial n'ont fait que renforcer cette conclusion.

Le décret m'ordonnait aussi d'examiner et d'évaluer la façon dont l'information à destination de décideurs de haut rang, notamment d'élus, et entre le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (le « Groupe de travail ») et le panel du Protocole public en cas d'incident électoral critique, a circulé pendant les périodes électorales ayant mené aux 43<sup>e</sup> et 44<sup>e</sup> élections générales et au cours des semaines qui ont suivi, ainsi que les mesures prises en réaction à cette information. Ce que j'ai fait.

La preuve présentée devant moi n'a pas révélé de problème particulier quant à la façon dont l'information a circulé à ces occasions. Hormis un rapport qui n'aurait pas été acheminé au Groupe de travail en temps opportun, la façon dont les informations ont circulé a été adéquate.

Le décret me demandait aussi d'examiner et d'évaluer la capacité des ministères, organismes, structures institutionnelles et processus de gouvernance fédéraux à permettre au gouvernement du Canada de détecter, de prévenir et de contrer toute forme d'ingérence étrangère visant directement ou indirectement les processus démocratiques du Canada, notamment en ce qui a trait à :

- La création, l'échange, l'évaluation et la diffusion du renseignement et la formulation de conseils à l'intention de décideurs de haut rang, notamment d'élus.
- Les mesures de soutien et de protection en place pour les membres d'une diaspora qui peuvent être particulièrement vulnérables et devenir les premières victimes de cette ingérence, dans les processus démocratiques canadiens.
- Les mécanismes qui étaient en place pour protéger l'intégrité des 43<sup>e</sup> et 44<sup>e</sup> élections générales contre l'ingérence étrangère, comparativement à ceux qui étaient en place pour protéger celle des élections fédérales antérieures récentes que j'aurais jugé pertinentes.

Je retiens de mon examen que certains des processus par lesquels le renseignement devait être communiqué en haut lieu ont connu des ratés. Des informations qui auraient dû se rendre à des ministres et même au premier ministre ne se sont pas rendues. La preuve ne m'a pas permis d'identifier précisément les raisons expliquant pourquoi cela s'est produit dans chacun des cas. La preuve a cependant permis de mettre en lumière que les systèmes alors en place n'étaient pas très robustes. Ces systèmes ne permettaient pas de savoir qui avait reçu un rapport donné, si ceux et celles l'ayant reçu en avaient pris connaissance et si une action quelconque s'en était suivie.

Dans certains cas, l'impression qui se dégage de la preuve est que les divers intervenants estimaient avoir satisfait à leurs obligations dès lors qu'ils avaient communiqué l'information, sans par ailleurs s'assurer qu'elle avait bien été reçue et comprise.

Je n'ai par ailleurs aucune preuve me permettant de conclure à de la mauvaise foi de la part de quiconque. Les déficiences observées semblent avoir été des déficiences systémiques dont les conséquences ont été accentuées par divers facteurs extérieurs, dont la pandémie de COVID-19 qui a rendu nécessaire une réorganisation importante du travail. Manifestement, cette réorganisation du travail dans l'appareil gouvernemental a été sous-optimale à plusieurs égards.

Heureusement, le système de transmission du renseignement a depuis été entièrement repensé. Je n'ai pas été en mesure de mettre ce nouveau système à l'épreuve pour en vérifier l'efficacité et la résistance, mais la preuve donne à penser qu'il est beaucoup plus adéquat que celui qui était en place auparavant. À mon avis, le gouvernement devra être très vigilant et en mesurer régulièrement l'efficacité.

Évidemment, lorsqu'une information n'a pas été transmise à la personne qui aurait été en mesure d'agir, je n'ai pas pu évaluer le caractère adéquat de quelque réponse gouvernementale. En effet, si une information ne se rend pas à un décideur, elle ne peut pas donner lieu à une action.

J'ai néanmoins pu examiner et évaluer plusieurs mesures prises en réponse à de l'information qui a été reçue en lien avec l'ingérence étrangère. J'en retiens que l'importance accordée à de telles informations a considérablement varié au fil des années, ce qui suggère que le gouvernement a mis un certain temps à prendre la pleine mesure de la menace que pose l'ingérence étrangère dans les processus et les institutions démocratiques canadiens.

L'appareil gouvernemental réagit beaucoup plus rapidement depuis quelques années, quoiqu'il lui reste encore du chemin à parcourir. Les gouvernements, vu leur taille, ne sont généralement pas reconnus pour leur vitesse de réaction. J'en conviens. Toutefois, l'ingérence étrangère est un phénomène qui évolue rapidement et qui s'accroît. Il faut donc que le gouvernement trouve des façons de faire qui lui permettront de réagir plus vite. La réorganisation structurelle du système de gouvernance de la sécurité nationale à laquelle le gouvernement a procédé, qui a permis de réduire d'environ une douzaine à cinq le nombre de comités directement impliqués dans la lutte à l'ingérence étrangère, est un pas dans la bonne direction. Il demeure néanmoins important d'éviter les discussions et les consultations perpétuelles qui ne mènent à aucune action. L'appareil gouvernemental doit faciliter l'action, et non la paralyser. Parmi les diverses mesures mises en place par le gouvernement, la création du poste de coordonnateur national de la lutte contre l'ingérence étrangère devrait, je l'espère, y contribuer grandement.

Dans le cadre de mon évaluation de la capacité du gouvernement de détecter, prévenir et contrer l'ingérence étrangère visant les processus démocratiques, mon mandat me demandait d'examiner les mécanismes qui étaient en place pour protéger l'intégrité des 43e et 44e élections générales contre l'ingérence étrangère, comparativement à ceux qui étaient en place pour protéger celle des élections fédérales antérieures. Je mentionne qu'il

m'a été difficile de mener cet examen comparatif. Hormis certains mécanismes destinés à protéger l'infrastructure électorale, il n'existait en effet à peu près aucune mesure spécifique visant à protéger les processus électoraux contre l'ingérence étrangère avant 2017.

Je retiens en effet de la preuve que c'est à la lumière des allégations d'ingérence étrangère dans les élections américaines de 2016, le référendum sur la sortie du Royaume-Uni de l'Union européenne de 2016 et les élections françaises de 2017, que le Canada a commencé à s'intéresser à l'ingérence étrangère dans les processus démocratiques de façon plus prononcée.

Le gouvernement en place a d'ailleurs réagi assez rapidement puisque le premier ministre a confié à la ministre des Institutions démocratiques de l'époque la responsabilité de diriger les efforts du gouvernement pour défendre le processus électoral canadien contre les cybermenaces dès 2017.

En 2018, les pays du G7, réunis dans Charlevoix, ont convenu de mettre sur pied le Mécanisme de réponse rapide du G7 afin de renforcer la coordination et mieux déceler les menaces pesant sur les démocraties. Le Canada héberge son secrétariat.

En 2019, le Plan pour protéger la démocratie canadienne a été annoncé et mis en place. Cette initiative marque à mon avis un tournant important puisqu'elle reconnaît le risque que nos élections puissent être l'objet d'ingérence étrangère et s'y attaque spécifiquement. Ce plan n'était pas parfait, mais il a été régulièrement évalué et amélioré depuis. Il continue d'ailleurs de l'être et est toujours utilisé pour protéger nos processus et institutions démocratiques contre l'ingérence étrangère.

L'examen que j'ai fait des moyens dont dispose le gouvernement, en portant un regard particulier sur ceux dont dispose la communauté du renseignement, me permet aussi de conclure que le Canada possède les moyens nécessaires pour détecter, prévenir et contrer l'ingérence étrangère. Certains de ces moyens peuvent être améliorés, certes, mais ils existent.

Cela ne signifie toutefois pas que la lutte contre l'ingérence étrangère est gagnée. En fait cette lutte sera probablement sans fin puisque les États qui tentent de s'ingérer dans les démocraties, dont la nôtre, sont des acteurs sophistiqués qui raffinent aussi leurs méthodes.

Je retiens aussi de la preuve que cette menace a évolué et montre maintenant son sombre visage par l'intermédiaire de campagnes de désinformation dans les médias et sur les réseaux sociaux. Cette nouvelle tendance est très inquiétante puisqu'il est très difficile de contrer la désinformation, et les tentatives pour réglementer les médias sociaux afin qu'eux-mêmes la limitent se sont révélées infructueuses jusqu'à maintenant. Le Canada doit réfléchir à cette menace et trouver des moyens d'y faire face. Cela nécessitera probablement une très grande concertation entre les démocraties du monde entier.

En somme, la lutte contre l'ingérence étrangère doit se faire sans relâche et avec détermination. La confiance envers notre démocratie en dépend.

Dans ce rapport final, je formule certaines recommandations qui, je l'espère, devraient aussi contribuer à améliorer la posture canadienne face à cette menace.

Finalement, j'aimerais rappeler ce que j'ai déjà mentionné à plusieurs endroits dans ce rapport final : la répression transnationale est un fléau qui dépasse le cadre du mandat de la Commission. Il s'agit toutefois là d'une forme d'ingérence étrangère à laquelle le gouvernement doit rapidement s'attaquer. Il s'y intéresse déjà depuis un moment, mais il doit intensifier ses efforts.

## ANNEXE A

# Glossaire

Terme	Sigle ou abréviation	Définition
Affaires mondiales Canada (Global Affairs Canada)	AMC (GAC)	Ministère fédéral qui gère les relations diplomatiques, fait la promotion du commerce international et fournit de l'aide consulaire. Il dirige également les efforts internationaux en matière de développement, d'aide humanitaire et d'appui à la paix et à la sécurité, et contribue à la sécurité nationale et au développement du droit international.
Agent des relations avec les clients (Client Relations Officer)	ARC (CRO)	Fonctionnaire des services de renseignement chargé de transmettre des produits de renseignement pertinents aux responsables et au personnel du gouvernement qui disposent d'une autorisation de sécurité.
Avocats de la Commission (Commission Counsel)		Avocats qui travaillent pour la Commissaire au sein de la Commission sur l'ingérence étrangère.
« Besoin de savoir » ("Need to know")		Terme décrivant une condition devant être satisfaite pour accéder à de l'information classifiée. Même si une personne dispose de l'autorisation de sécurité nécessaire pour accéder à une information, elle ne peut y accéder que si cela est nécessaire dans l'exercice de ses fonctions officielles.
Breffage préventif de sécurité (Protective Security Briefing)	BPS (PSB)	Type de breffage non classifié fourni par le Service canadien du renseignement de sécurité (SCRS) pour sensibiliser un individu à une menace. Également appelé « breffage sur la sécurité défensive ».
Breffage sur la sécurité défensive (Defensive briefing)		Voir « Breffage préventif de sécurité ».

Terme	Sigle ou abréviation	Définition
Bureau du commissaire aux élections fédérales (Office of the Commissioner of Canada Elections)	<b>BCEF</b> <b>(OCCE)</b>	Organisation dirigée par le commissaire aux élections fédérales (CEF) au sein du Bureau du directeur général des élections (DGE).  Dans le cadre de ses responsabilités en matière de conformité et d'application de la <i>Loi électorale du Canada</i> , le BCEF agit indépendamment du DGE.
Bureau du Conseil privé (Privy Council Office)	<b>BCP</b> <b>(PCO)</b>	Ministère dont le rôle principal est la coordination de l'administration gouvernementale. Souvent qualifié de ministère du premier ministre.  Fournit des conseils non partisans au premier ministre, au Cabinet et aux comités du Cabinet sur des questions qui revêtent une importance nationale et internationale.  Appuie le processus décisionnel du Cabinet et veille à la mise en œuvre du programme politique et législatif du gouvernement par tous les ministères et organismes du gouvernement fédéral.
Bureau du directeur général des élections (Office of the Chief Electoral Officer)	<b>DGE</b> <b>(OCEO)</b>	Agence indépendante composée d'Élections Canada et du Bureau du commissaire aux élections fédérales (BCEF).
Cabinet		Organe décisionnel politique présidé par le premier ministre.  Composé des ministres nommés par la gouverneure générale sur recommandation du premier ministre.  Par convention, ces ministres (membres du Cabinet) sont généralement des députés. Ils dirigent les ministères du gouvernement.
Cabinet du premier ministre (Prime Minister's Office)	<b>CPM</b> <b>(PMO)</b>	Soutient le premier ministre dans l'exercice de ses responsabilités à titre de chef du gouvernement, de chef de parti politique et de député.  Le cabinet du premier ministre est composé de personnel politique et non de fonctionnaires de carrière.

Terme	Sigle ou abréviation	Définition
Camouflage de pourriels (Spamouflage)		Tactique qui utilise des réseaux de nouveaux comptes de médias sociaux ou des comptes piratés pour publier et amplifier des messages de propagande à travers de multiples plateformes.
Centre canadien pour la cybersécurité (Canadian Centre for Cyber Security)	CCC (CCCS)	Fait partie du Centre de la sécurité des télécommunications (CST). Il s'agit de la source unifiée de conseils, d'avis, de services et de soutien spécialisés en matière de cybersécurité pour les Canadiennes et les Canadiens.
Centre de la sécurité des télécommunications (Communications Security Establishment)	CST CSE)	Organisme du gouvernement fédéral qui fournit au gouvernement du renseignement électromagnétique étranger, et est responsable de la cybersécurité et de la protection de l'information. Le Centre canadien pour la cybersécurité fait partie du CST.
Comités interministériels (Inter-departmental Committees)		Comités composés de hauts fonctionnaires issus de divers ministères et organismes afin d'assurer une action coordonnée. Existent généralement au niveau des sous-ministres, des sous-ministres adjoints et des directeurs généraux.
Comité des parlementaires sur la sécurité nationale et le renseignement (National Security and Intelligence Committee of Parliamentarians)	CPSNR (NSICOP)	Comité statutaire composé de députés et de sénateurs et régi par la <i>Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement</i> . Examine les opérations de renseignement du gouvernement, notamment les cadres législatif, réglementaire, stratégique, administratif et financier de la sécurité nationale et du renseignement. Examine aussi les activités des ministères liées à la sécurité nationale ou au renseignement (à moins qu'une activité ne soit une opération en cours et que le ministre compétent ne détermine que l'examen serait préjudiciable à la sécurité nationale). Enquête également sur toute question liée à la sécurité nationale ou au renseignement dont il est saisi par un ministre.

Terme	Sigle ou abréviation	Définition
Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (Standing Committee on Access to Information, Privacy and Ethics)	<b>ETHI</b>	Composé de députés. Étudie des questions qui touchent : <ul style="list-style-type: none"> <li>le Commissariat à l'information du Canada</li> <li>le Commissariat à la protection de la vie privée du Canada</li> <li>le Commissariat au lobbying du Canada.</li> </ul> Étudie aussi certaines questions relatives au Commissariat aux conflits d'intérêts et à l'éthique.
Comité permanent de la procédure et des affaires de la Chambre (Standing Committee on Procedure and House Affairs)	<b>PROC</b>	Composé de députés. Étudie les questions suivantes et en fait rapport : <ul style="list-style-type: none"> <li>règles et pratiques de la Chambre des communes et de ses comités</li> <li>questions électorales</li> <li>questions de privilège</li> <li>conflits d'intérêts des députés.</li> </ul>
Comités de coordination de la sécurité des élections (Elections Security Coordinating Committees)	<b>CCSE</b> <b>(ESCCs)</b>	Comités de hauts fonctionnaires du gouvernement et d'Élections Canada créés pendant les élections fédérales (au niveau des sous-ministres, des sous-ministres adjoints ou des directeurs généraux). Coprésidés par le Bureau du Conseil privé et Élections Canada. Assurent une approche coordonnée et une compréhension commune entre la communauté de la sécurité nationale et du renseignement, Élections Canada et le commissaire aux élections fédérales.
Commissaire aux élections fédérales (Commissioner of Canada Elections)	<b>CEF</b> <b>(CCE)</b>	Veille au respect de la <i>Loi électorale du Canada</i> et de la <i>Loi référendaire</i> . Nommé par le directeur général des élections, après consultation auprès du directeur des poursuites pénales.
Commission sur l'ingérence étrangère (Foreign Interference Commission)	<b>Commission</b>	Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Terme	Sigle ou abréviation	Définition
Communauté de la sécurité et du renseignement (Security and Intelligence Community)	(S&I Community)	Ministères et agences du gouvernement du Canada qui travaillent à la sécurité nationale et à la collecte du renseignement : AMC, BCP, CST, GRC, MDN, SCRS et Sécurité Publique Canada.
Confidentialité à des fins de sécurité nationale (National security confidentiality)	CSN (NSC)	Vise à restreindre l'accès à certaines informations du gouvernement ainsi qu'à empêcher leur divulgation afin de protéger les intérêts de la sécurité nationale.
Conseil privé du Roi pour le Canada (King's Privy Council for Canada)		Groupe de personnes nommées par la gouverneure générale pour conseiller le Roi : membres du Cabinet, anciens ministres, juge en chef du Canada, anciens juges en chef, anciens présidents de la Chambre des communes, anciens présidents du Sénat, anciens gouverneurs généraux et autres personnes éminentes.
Conseil de la radiodiffusion et des télécommunications canadiennes (Canadian Radio-television and Telecommunications Commission)	CRTC	Organisme public chargé de réglementer et de superviser la radiodiffusion et les télécommunications au Canada.  Le CRTC exerce ses activités indépendamment du gouvernement fédéral et met en œuvre les lois et règlements adoptés par le Parlement.
Conseil de la sécurité nationale (National Security Council)	CSN (NSC)	Comité du Cabinet créé en 2023 et présidé par le premier ministre pour prendre des décisions stratégiques sur les intérêts du Canada en matière de sécurité publique, de sécurité nationale, de politique étrangère et de renseignement.
Conseiller à la sécurité nationale et au renseignement auprès du premier ministre (National Security and Intelligence Advisor to the Prime Minister)	CSNR (NSIA)	Haut fonctionnaire qui donne des conseils stratégiques et opérationnels au premier ministre et au Cabinet en matière de sécurité nationale afin d'assurer la coordination de la réponse du gouvernement aux menaces.  Reçoit de l'information de ses secrétariats et de la communauté de la sécurité et du renseignement.  A maintenant le statut de sous-greffier au sein du Bureau du Conseil privé et relève du greffier du Conseil privé et secrétaire du Cabinet.

Terme	Sigle ou abréviation	Définition
Coordonnateur national de la lutte contre l'ingérence étrangère (National Counter Foreign Interference Coordinator)	<b>CNLIE</b>  <b>(NCFIC)</b>	Poste créé en 2023 pour coordonner la réponse sur le plan des politiques du gouvernement du Canada en matière d'ingérence étrangère.  Cela inclut le travail qui vise à améliorer la transparence de la réponse gouvernementale par le biais d'un dialogue public avec tous les Canadiens et Canadiennes, y compris les groupes des diasporas, les universités, les organisations non gouvernementales et d'autres partenaires nationaux et internationaux.
Décret (Order in council)	<b>(OIC)</b>	Instrument juridique faisant état d'une décision prise par la gouverneure en conseil en vertu d'un pouvoir prévu par une loi (ou, à l'occasion, de la prérogative royale).  Toujours préparé sur recommandation du ministre responsable et n'entre en vigueur qu'une fois approuvé par la gouverneure générale.
Désinformation (Disinformation)		Informations fausses ou inexactes propagées délibérément dans le but de tromper ou d'induire en erreur.  Voir aussi « Méinformation ».
Directeur général des élections (Chief Electoral Officer)	<b>DGE</b>  <b>(CEO)</b>	Chef d'Élections Canada.  Chargé de la conduite des élections et de la conformité aux règles électorales.  Relève directement du Parlement, et non du gouvernement.
Élections Canada (Elections Canada)		Entité responsable de l'administration des élections fédérales. Dirigée par le directeur général des élections (DGE).  Fonctionne indépendamment du gouvernement.
Gendarmerie royale du Canada (Royal Canadian Mounted Police)	<b>GRC</b>  <b>(RCMP)</b>	Service de police national du Canada.  Préviens la criminalité et mène des enquêtes, assure le maintien de l'ordre, fait respecter les lois, contribue à la sécurité nationale, assure la sécurité des représentants de l'État désignés, des dignitaires étrangers et du corps diplomatique, et fournit un soutien opérationnel à d'autres services de police et organismes d'application de la loi au Canada et à l'étranger.

Terme	Sigle ou abréviation	Définition
Gouverneure en conseil (Governor in Council)	<b>GEC</b> (GIC)	Gouverneure générale agissant sur l'avis du Conseil privé du Roi pour le Canada.  Par convention, la gouverneure générale n'exerce ses pouvoirs que sur l'avis des membres du Conseil privé du Roi, qui comprend les membres du Cabinet (voir la définition de « Conseil privé du Roi pour le Canada »).  En pratique, la notion de gouverneure en conseil fait référence au Cabinet et à la Gouverneure générale.  Les décisions de la gouverneure en conseil sont souvent rendues officiellement par des décrets.
Greffier du Conseil privé et secrétaire du Cabinet (Clerk of the Privy Council and Secretary to the Cabinet)	<b>Greffier</b> (Clerk)	Haut fonctionnaire du Bureau du Conseil privé qui exerce aussi les fonctions de secrétaire du Cabinet et de sous-ministre auprès du premier ministre.
Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (Security and Intelligence Threats to Elections Task Force)	<b>Groupe de travail</b>  (SITE TF)	Groupe de travail gouvernemental composé de représentants des entités suivantes : <ul style="list-style-type: none"> <li>• Service canadien du renseignement de sécurité (SCRS)</li> <li>• Centre de la sécurité des télécommunications (CST)</li> <li>• Affaires mondiales Canada (AMC)</li> <li>• Gendarmerie royale du Canada (GRC).</li> </ul> Créé pour protéger les élections fédérales canadiennes contre l'ingérence étrangère.
Groupe des cinq (Five Eyes)		Alliance de renseignement composée de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis.  Ces pays sont parties à l'accord multilatéral UK-USA, un traité de coopération commune en matière de renseignement d'origine électromagnétique.
Huis clos ( <i>In camera</i> )		Terme juridique signifiant « en privé ».  Par exemple, les audiences à huis clos sont des audiences qui se déroulent sans la présence du public ou des médias.
Hypertrucage (Deepfake)		Images, séquences vidéo ou audio synthétiques qui sont altérées ou générées numériquement à l'aide d'outils d'intelligence artificielle.

Terme	Sigle ou abréviation	Définition
Information classifiée (Classified information)		Information que le gouvernement déclare comme pouvant raisonnablement porter préjudice à l'intérêt national si elle est divulguée. Répartie en trois catégories selon les niveaux suivants : <ul style="list-style-type: none"> <li>• Confidentiel (préjudice limité ou modéré)</li> <li>• Secret (préjudice grave)</li> <li>• Très secret (préjudice extrêmement grave).</li> </ul>
Information cloisonnée (Compartmented information)		Information classifiée soumise à un système de contrôle supplémentaire (un cadre administratif) qui établit des normes pour l'accès, le marquage, le traitement et le contrôle de l'information.
Information protégée (Protected information)		Information dont la divulgation publique pourrait raisonnablement, selon le gouvernement, causer un préjudice à un intérêt autre que national. Elle comprend trois catégories : <ul style="list-style-type: none"> <li>• Protégé A (préjudice limité ou modéré)</li> <li>• Protégé B (préjudice grave)</li> <li>• Protégé C (préjudice extrêmement grave).</li> </ul>
Ingérence étrangère (Foreign Interference)	IE (FI)	Aux fins de la Commission, on entend par ingérence étrangère toute activité clandestine, trompeuse ou menaçante à laquelle se livrent un État étranger ou ceux qui agissent en son nom et qui s'avère préjudiciable aux intérêts du Canada.
Initiative de citoyenneté numérique (Digital Citizen Initiative)	ICN (DCI)	Programme du ministère du Patrimoine canadien officiellement établi en 2020 pour lutter contre la désinformation en ligne, soutenir la démocratie et promouvoir un écosystème d'information sain par le biais d'initiatives de recherche et de partenariats.

Terme	Sigle ou abréviation	Définition
Intelligence artificielle / Intelligence artificielle générative (Artificial Intelligence/Generative Artificial Intelligence)	IA / IA générative  (AI / GenAI)	Technologie de l'information qui effectue des tâches dont la réalisation nécessiterait normalement la puissance du cerveau humain.  L'IA générative est un type d'IA qui produit diverses formes de contenu telles que du texte, de la voix ou de l'audio, du code, des vidéos et des images. Elle apprend à partir du contenu existant et utilise les modèles et les structures pour générer du nouveau contenu, sur la base d'informations fournies par les utilisateurs.
Intervenant (Intervener)		Entité ayant la « qualité pour agir » (voir la définition) à titre d'intervenant auprès de la Commission sur l'ingérence étrangère, avec des droits de participation limités.  Un intervenant est aussi un participant.  A le droit de recevoir les avis d'audiences publiques de la Commission et d'y assister à titre de participant, de présenter des observations et de recevoir des pièces provenant des audiences publiques. Peut avoir d'autres droits s'ils sont expressément accordés par la Commissaire.
Mandat (Terms of Reference)	(ToR)	Mandat de la Commission sur l'ingérence étrangère énoncé dans le Décret C.P. n° 2023-0882 (ce décret a créé la Commission sur l'ingérence étrangère et a nommé la Commissaire).
Mécanisme de réponse rapide du G7 (G7 Rapid Response Mechanism)	MRR du G7  (G7 RRM)	Mécanisme du G7 (Canada, France, Allemagne, Italie, Japon, Royaume-Uni et États-Unis) visant à déceler les menaces étrangères contre les démocraties, et à y répondre.  Le MRR du G7 est coordonné par le Secrétariat du MRR du G7, qui fait partie d'Affaires mondiales Canada.
Mémoire au Cabinet (Memorandum to Cabinet)	MC	Document écrit qui présente une initiative législative ou de politique, et qui est utilisé pour obtenir l'approbation du Cabinet.
Mésinformation (Misinformation)		Informations fausses ou inexactes (sans intention d'induire en erreur).  Voir aussi « Désinformation ».

Terme	Sigle ou abréviation	Définition
Ministère de la Défense nationale (Department of National Defence)	<b>MDN</b>  (DND)	Ministère fédéral de qui relèvent les Forces armées canadiennes, qu'il soutient.
Mesure de réduction de la menace (Threat reduction measure)	<b>MRM</b>  (TRM)	Mesure opérationnelle prise par le Service canadien du renseignement de sécurité (SCRS) pour réduire les menaces à la sécurité du Canada, en vertu de l'article 12.1 de la <i>Loi sur le SCRS</i> , lequel exige que la mesure soit raisonnable et proportionnelle à la gravité de la menace.
Observatoire de l'écosystème médiatique (Media Ecosystem Observatory)	<b>(MEO)</b>	Organisation résultant d'une collaboration interdisciplinaire entre l'Université McGill et l'Université de Toronto qui étudie la santé de l'écosystème des médias.  Il s'agit de l'organe de coordination du « Réseau canadien de recherche sur les médias numériques » (voir la définition).
Office de surveillance des activités en matière de sécurité nationale et de renseignement (National Security and Intelligence Review Agency)	<b>OSSNR</b>  (NSIRA)	Organisme de surveillance statutaire externe créé par la <i>Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement</i> et qui relève du Parlement.  Examine les activités du gouvernement en matière de sécurité nationale et de renseignement et mène des enquêtes pour s'assurer qu'elles sont légales, raisonnables et nécessaires.  Examine également les plaintes du public concernant les principales agences et activités de sécurité nationale.
Panel des cinq (Panel of Five or Panel)		Voir « Protocole public en cas d'incident électoral majeur ».
Participant		Individu ou entité ayant la « qualité pour agir » (voir la définition) auprès de la Commission sur l'ingérence étrangère, soit en tant que partie, soit en tant qu'intervenant.

Terme	Sigle ou abréviation	Définition
Partie (Party)		Individu ou entité ayant la « qualité pour agir » (voir la définition) auprès de la Commission sur l'ingérence étrangère et disposant de tous les droits de participation, notamment le droit de consulter les documents avant les audiences et d'interroger les témoins.  Une partie est également un participant.
Patrimoine canadien (Canadian Heritage)		Ministère fédéral chargé de promouvoir l'identité et les valeurs canadiennes, le développement culturel et le patrimoine.
<i>Persona non grata</i>	PNG	Terme latin signifiant « personne indésirable ». En diplomatie, il fait référence à la pratique d'un État hôte qui demande à un diplomate étranger de quitter son territoire.  Lorsqu'un État hôte déclare un diplomate « <i>persona non grata</i> », cela revient à l'expulser du pays.
Pouvoir exécutif (Executive branch)		L'un des trois pouvoirs du régime gouvernemental canadien. Les deux autres sont le pouvoir législatif et le pouvoir judiciaire. Chacun a des pouvoirs et des responsabilités différents, définis dans la Constitution.  Le pouvoir exécutif met en œuvre les lois et les politiques.  Le premier ministre et le Cabinet constituent le pouvoir exécutif du gouvernement.
Pouvoir judiciaire (Judicial branch)		L'un des trois pouvoirs du régime gouvernemental canadien. Les deux autres sont le pouvoir législatif et le pouvoir exécutif. Chacun a des pouvoirs et des responsabilités différents définis dans la Constitution.  Le pouvoir judiciaire interprète et applique le droit.  Le pouvoir judiciaire est constitué des tribunaux canadiens et il est indépendant du gouvernement.

Terme	Sigle ou abréviation	Définition
Pouvoir législatif (Legislative branch)		L'un des trois pouvoirs du régime gouvernemental canadien. Les deux autres sont le pouvoir exécutif et le pouvoir judiciaire. Chacun a des pouvoirs et des responsabilités différents définis dans la Constitution.  Le pouvoir législatif crée les lois.  Le Parlement (Sénat et Chambre des communes) constitue le pouvoir législatif du gouvernement fédéral.
<b>Privilèges</b>		
— Privilège du secret professionnel de l'avocat (Solicitor-client privilege)		Protège les communications (y compris les documents) entre un avocat et son client, produites pour une consultation ou un avis juridique, et destinées à demeurer confidentielles.  Ce privilège appartient au client qui est la seule personne à pouvoir y renoncer.
— Privilège en vertu de l'article 38 de la <i>Loi sur la preuve au Canada</i> (Section 38 of the <i>Canada Evidence Act</i> privilege)		Protège les informations qui, si elles sont divulguées, sont susceptibles de porter préjudice aux relations internationales, à la défense nationale ou à la sécurité nationale. La protection de cette dernière s'appelle aussi « privilège de la sécurité nationale ».  L'information protégée par l'article 38 ne peut être divulguée que si un tribunal l'ordonne ou si le procureur général du Canada y consent.
— Privilège parlementaire (Parliamentary privilege)		Ensemble des droits et immunités nécessaires pour que la Chambre des communes, le Sénat et leurs membres puissent exercer leurs fonctions. Par exemple : la liberté de parole à la Chambre et aux comités de la Chambre et le droit de ne pas être forcé à comparaître comme témoin devant un tribunal.  Également, pouvoir de la Chambre et du Sénat de se protéger et de protéger les députés ou sénateurs et leurs procédures, de toute ingérence indue afin qu'ils puissent s'acquitter efficacement de leurs principales fonctions.

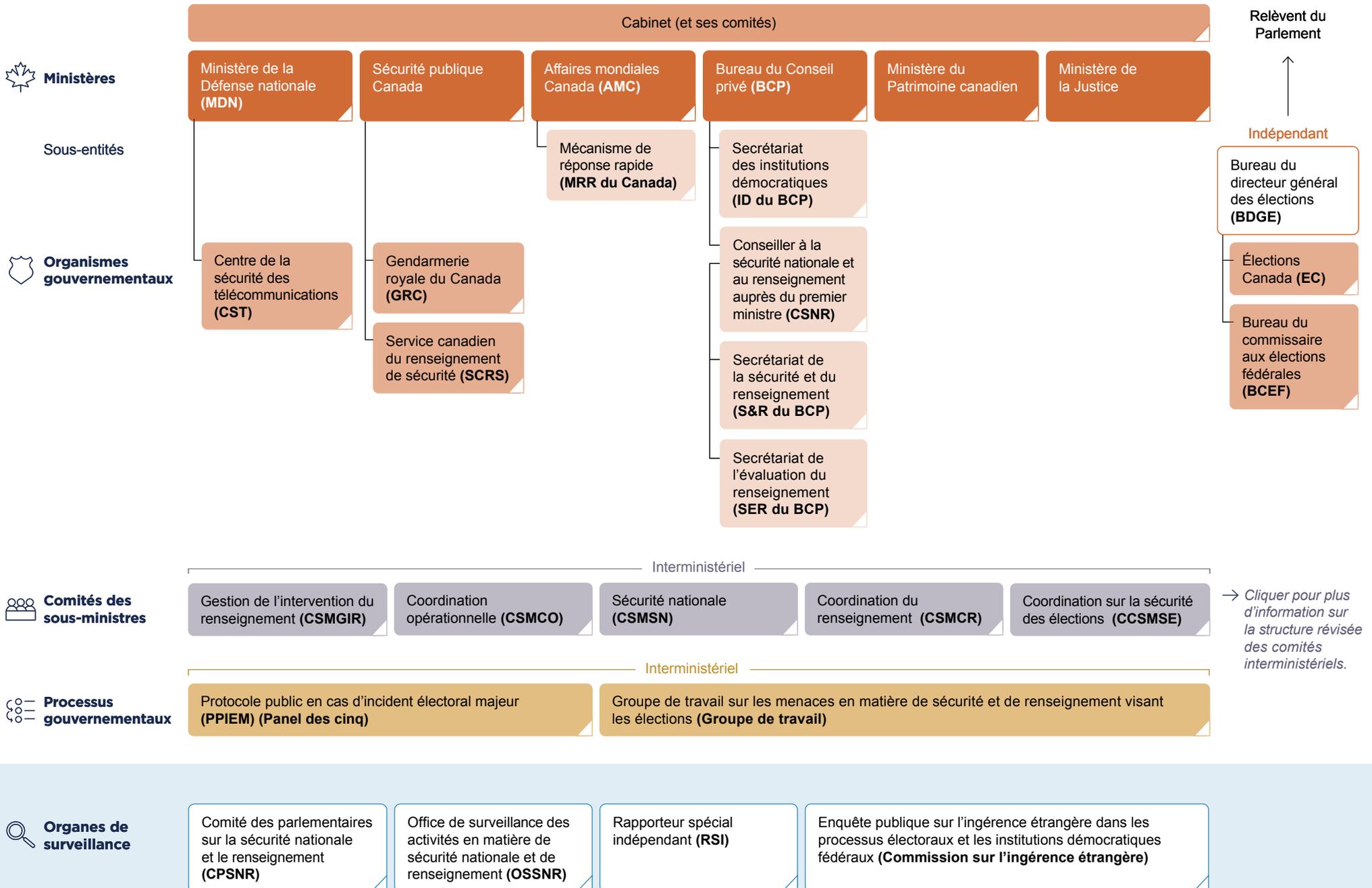
Terme	Sigle ou abréviation	Définition
<p>— Privilège relatif au litige (Litigation privilege)</p>		<p>Protège les communications (y compris les documents) entre un avocat et ses clients ou une tierce partie, produites principalement en préparation d'un litige existant ou anticipé.</p>
<p>— Privilège relatif aux renseignements confidentiels du Cabinet (Cabinet confidences privilege)</p>		<p>Protège la confidentialité des échanges ayant lieu au sein du Cabinet.</p> <p>La protection des renseignements confidentiels du Cabinet est une règle de common law et une règle édictée à l'article 39 de la <i>Loi sur la preuve au Canada</i> et reconnue par la <i>Loi sur l'accès à l'information</i>.</p> <p>S'applique à toute personne qui participe aux réunions du Cabinet, même si elle n'est pas ministre.</p>
<p>— Protection des renseignements d'intérêt public (article 37 de la <i>Loi sur la preuve au Canada</i>) (Public interest privilege, section 37 of the Canada Evidence Act)</p>		<p>Protège l'information pour des raisons d'intérêt public déterminées. Tout intérêt public suffisamment important peut justifier de ne pas divulguer une information.</p> <p>Peut par exemple servir à protéger l'identité d'informateurs confidentiels, des informations sur des enquêtes criminelles en cours, des informations sur des techniques d'enquête sensibles, et des informations qui, si elles étaient divulguées, mettraient en danger la sécurité des titulaires d'une charge publique ou du public.</p> <p>Aussi appelée « immunité relative aux renseignements d'intérêt public ».</p>
<p>Procureur général du Canada (Attorney General of Canada)</p>	<p><a href="#">PGC</a> <a href="#">(AGC)</a></p>	<ul style="list-style-type: none"> <li>• Dirige des poursuites au nom du gouvernement du Canada.</li> <li>• Ne représente pas les ministères ou les organismes individuellement, mais leur offre des conseils juridiques et des services législatifs.</li> <li>• Agit dans l'intérêt du public, notamment en faisant respecter la Constitution, le principe de la primauté du droit et l'indépendance des tribunaux.</li> </ul>

Terme	Sigle ou abréviation	Définition
Protocole public en cas d'incident électoral majeur (Critical Election Incident Public Protocol)	PPIEM (CEIPP)	Protocole appliqué pendant les élections fédérales par un groupe de cinq hauts fonctionnaires (Panel des cinq) : <ul style="list-style-type: none"> <li>• le greffier du Conseil privé</li> <li>• le conseiller à la sécurité nationale et au renseignement auprès du premier ministre</li> <li>• le sous-ministre de la Justice et sous-procureur général du Canada</li> <li>• le sous-ministre de la Sécurité publique</li> <li>• le sous-ministre des Affaires étrangères.</li> </ul> Destiné à protéger les élections fédérales contre les ingérences, y compris l'ingérence étrangère.
Qualité pour agir (Standing)		Possibilité de participer directement à des procédures (par exemple en cour ou devant des tribunaux administratifs) en bénéficiant de certains droits.  Les <i>Règles de pratique et de procédure</i> de la Commission sur l'ingérence étrangère déterminent qui peut avoir la qualité pour agir comme partie ou comme intervenant (collectivement appelés les « participants ») dans les procédures de la Commission.
Répression transnationale (Transnational repression)	RTN (TNR)	Aux fins de la Commission, la répression transnationale se produit lorsque des pays font usage de mesures au-delà de leurs frontières pour intimider, réduire au silence, contraindre, harceler ou blesser des individus, en particulier des membres des communautés issues des diasporas au Canada.
Réseau canadien de recherche sur les médias numériques (Canadian Digital Media Research Network)	RCRMN (CDMRN)	Communauté de recherche au Canada visant à renforcer la résilience de l'information et à protéger la démocratie canadienne.  Le réseau est coordonné par l'Observatoire des écosystèmes médiatiques (voir la définition).
Sanction royale (Royal assent)		Octroyée lorsque la gouverneure générale approuve un projet de loi adopté par le Parlement, ce qui en fait une loi fédérale.

Terme	Sigle ou abréviation	Définition
Secrétariat de l'évaluation du renseignement (Intelligence Assessment Secretariat)	<b>SER du BCP</b>  (PCO-IAS)	Unité du Bureau du Conseil privé chargée de l'analyse et de l'évaluation stratégique du renseignement collecté par les agences de sécurité et de renseignement.  Fournit des analyses et des évaluations au premier ministre, au Cabinet, au greffier du Conseil privé et secrétaire du Cabinet et aux hauts fonctionnaires du gouvernement.
Secrétariat de la sécurité et du renseignement du Bureau du Conseil privé (Security and Intelligence Secretariat of the Privy Council Office)	<b>S et R du BCP</b>  (PCO-S&I)	Secrétariat du Bureau du Conseil privé qui offre des conseils stratégiques et de l'aide au conseiller à la sécurité nationale et au renseignement auprès du premier ministre afin qu'il l'informe, ainsi que le Cabinet, sur les principales questions de sécurité nationale.  Joue un rôle de coordination lorsque le Cabinet est saisi de questions de sécurité nationale ou de renseignement.  Collabore avec Sécurité publique Canada et d'autres ministères pour organiser et appuyer les réunions régulières de la haute gouvernance consacrées aux menaces d'ingérence étrangère et aux mesures à prendre.
Secrétariat des institutions démocratiques du Bureau du Conseil privé (Democratic Institutions Secretariat of the Privy Council Office)	<b>ID du BCP</b>  (PCO-DI)	Secrétariat du Bureau du Conseil privé qui fournit un soutien et des conseils en matière de politiques au premier ministre et au ministre des Institutions démocratiques sur les enjeux qui ont des répercussions sur les institutions démocratiques canadiennes.
Sécurité publique Canada (Public Safety Canada)	<b>SITE TF</b> (Groupe de travail)	Ministère fédéral responsable de la gestion de la sécurité publique, de la sécurité nationale et des urgences.
Sergent d'armes (Sergeant-at-Arms)	(SAA)	Exerce plusieurs fonctions protocolaires à la Chambre des communes et est responsable, à titre de directeur de la sécurité institutionnelle, de la sécurité de la Chambre et de ses membres à l'extérieur de la Colline du Parlement.

Terme	Sigle ou abréviation	Définition
Service canadien du renseignement de sécurité (Canadian Security Intelligence Service)	SCRS (CSIS)	Organisme du gouvernement fédéral régi par la <i>Loi sur le Service canadien du renseignement de sécurité</i> . <ul style="list-style-type: none"><li>• Enquête sur les activités qui pourraient constituer une menace pour la sécurité du Canada et en fait rapport au gouvernement.</li><li>• Peut prendre des mesures visant à réduire les menaces pour la sécurité du Canada.</li><li>• Peut aussi prêter assistance à certains ministres pour collecter du renseignement étranger au Canada.</li></ul>
Sources ouvertes (Open source)	PROC	Information accessible au public.

# Les principales entités fédérales chargées de répondre à l'ingérence étrangère





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