

**ENQUÊTE PUBLIQUE SUR L'INGÉRENCE ÉTRANGÈRE DANS LES PROCESSUS
ÉLECTORAUX ET LES INSTITUTIONS DÉMOCRATIQUES FÉDÉRAUX**

**REPRÉSENTATIONS ÉCRITES NON CLASSIFIÉES DU
GOUVERNEMENT DU CANADA
(PARTIE C DES AUDIENCES)**

5 novembre, 2024

LE PROCUREUR GÉNÉRAL DU CANADA

Ministère de la Justice du Canada
Section du contentieux des affaires civiles
50, rue O'Connor, bureau 500
Ottawa (Ontario) K1A 0H8
Télécopieur: (613) 954-1920

Gregory Tzemenakis
Avocat général principal
Barney Brucker
Avocat général principal p.i.

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

Avocats pour le gouvernement du Canada

Table des matières

A.	Aperçu.....	1
B.	L'ingérence étrangère au Canada.....	2
C.	La réponse du Canada à l'ingérence étrangère.....	5
1.	Renforcer le système électoral du Canada.....	7
a)	<i>Le Groupe d'experts/Le Protocole public en cas d'incident électoral majeur.....</i>	<i>7</i>
b)	<i>Le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections.....</i>	<i>9</i>
2.	Collaboration avec les parlementaires, les partis politiques et les autres gouvernements	10
a)	<i>Le Canada a rendu le système politique plus résilient.....</i>	<i>10</i>
b)	<i>Partenariats du Canada avec les autres ordres de gouvernement.....</i>	<i>15</i>
c)	<i>La coordination du Canada avec ses partenaires internationaux.....</i>	<i>16</i>
3.	Le Canada bâtit la résilience du public à l'IE.....	18
a)	<i>La collaboration avec les communautés culturelles.....</i>	<i>19</i>
b)	<i>Collaborer avec des organisations de la société civile afin de bâtir la résilience.....</i>	<i>20</i>
4.	La communauté de la sécurité nationale du Canada a la capacité de détecter, prévenir, et contrer l'IE.....	23
a)	<i>SCRS – Outils de renseignement.....</i>	<i>24</i>
b)	<i>CST – Renseignement électromagnétique étranger et outils de cyberdéfense.....</i>	<i>25</i>
c)	<i>AMC – Outils diplomatiques.....</i>	<i>26</i>
d)	<i>GRC – Outils d'application de la loi.....</i>	<i>30</i>
e)	<i>Sécurité publique – Outils réglementaires.....</i>	<i>31</i>
5.	La réponse du gouvernement aux menaces d'IE est coordonnée.....	31
a)	<i>Le Conseil de la sécurité nationale (CSN).....</i>	<i>31</i>
b)	<i>La coordination entre sous-ministres.....</i>	<i>32</i>
c)	<i>Le coordonnateur national de la lutte contre l'ingérence étrangère.....</i>	<i>33</i>
d)	<i>La dissémination du renseignement.....</i>	<i>33</i>
D.	La réponse du Canada à des cas et allégations spécifiques.....	36
1.	Les processus des partis politiques relèvent des partis politiques.....	36
2.	Les débats au sein de la fonction publique relativement à l'IE constituent une force, non une faiblesse.....	37
3.	Les postes de police étrangers.....	37
4.	Le document sur le ciblage et le rapport spécial n'ont pas été fournis au premier ministre.....	38
5.	Mandats du SCRS et délai d'approbation de l'un d'entre eux.....	39

6.	Le Mémoire au Cabinet sur les Activités hostiles parrainées par des acteurs étatiques (AHAE) et le projet de loi C-70.....	41
E.	Les Canadiens peuvent et doivent avoir confiance	41
1.	Confiance dans les 43^e et 44^e élections générales.....	41
2.	Confiance dans les processus démocratiques	42
<i>a)</i>	<i>Reportages médiatiques sur l'IE en fin 2022 et début 2023.....</i>	<i>42</i>
3.	Confiance dans les parlementaires	43
F.	Conclusion	44

A. Aperçu

1. Depuis près d'une décennie, le gouvernement du Canada travaille résolument à travers de nombreux domaines pour renforcer la capacité du Canada à détecter, prévenir et contrer l'ingérence étrangère (IÉ). Le Canada a mieux équipé son système électoral et politique, est un chef de file sur la scène internationale en matière d'IÉ, a renforcé davantage la communauté de la sécurité nationale et du renseignement et a accru la résilience du public face à cette menace.
2. Contrairement au portrait erroné qu'ont dressé certaines informations trompeuses rendues publiques illégalement, la preuve entendue par cette Commission démontre que les Canadiens peuvent et doivent avoir confiance dans leurs institutions démocratiques, y compris dans leurs élections, leur gouvernement et les parlementaires qui les représentent. Malgré les activités d'IÉ néfastes et inacceptables, ces institutions demeurent fondamentalement sûres.
3. La longue et vaste série de mesures énergiques prises par le gouvernement ne signifie pas que le problème de l'IÉ est résolu. L'IÉ est menée dans un contexte géopolitique évolutif, par des États qui modifieront leurs tactiques pour tenter de contourner les défenses du Canada. Les acteurs malveillants qui mènent des activités d'IÉ exploitent les libertés garanties au Canada en profitant de l'ouverture de l'Internet pour propager la désinformation et en victimisant certaines communautés à travers les liens qu'elles entretiennent avec leurs pays d'origine. Les acteurs d'IÉ prennent avantage des droits d'expression et de participation qui sont fondamentaux pour notre démocratie.
4. Pour ces raisons, l'IÉ est, par sa nature même, un problème complexe, difficile et évolutif. Il faut répondre à cette menace par des actions ciblées de manière urgente. Le travail du gouvernement doit se poursuivre et se poursuivra. En plus de contribuer directement à une meilleure compréhension de l'IÉ par le public, les recommandations de la Commission influenceront les travaux futurs du Canada. Le Canada remercie la Commission pour son étude approfondie.

B. L'ingérence étrangère au Canada

5. Pour détecter, prévenir et contrer l'IE, il est primordial de comprendre cette menace complexe et évolutive. Rencontrées par toutes les démocraties, les activités d'IE peuvent prendre plusieurs formes, cibler de nombreuses parties de la société et utiliser des méthodes variées. Le Canada continue à développer sa compréhension sophistiquée de l'IE, des acteurs étatiques hostiles, de leurs tactiques et objectifs, ainsi que des différents vecteurs et méthodes pouvant être utilisés.

6. L'IE n'est pas un nouveau phénomène. Les États ont longtemps cherché à influencer les politiques des uns et des autres, et ceci relève de la diplomatie régie par la *Convention de Vienne sur les relations diplomatiques* et de la *Convention de Vienne sur les relations consulaires*¹. L'influence étrangère devient ingérence lorsqu'elle est trompeuse, clandestine ou comporte des menaces contre autrui². Il est parfois difficile de déterminer si une activité spécifique relève de l'influence étrangère ou de l'IE³. L'IE est particulièrement pernicieuse lorsqu'elle tente de miner la démocratie, les valeurs ou les objectifs du Canada. De plus, les acteurs malveillants peuvent tenter de dissimuler leurs activités d'ingérence.

7. Au Canada, la République populaire de Chine (RPC) et l'Inde représentent actuellement les menaces d'IE les plus importantes. Le Canada fait aussi face à des tentatives d'IE électorale de la part de la Russie et du Pakistan. D'autres pays, tel qu'illustré par le cas de l'Iran, ne ciblent pas directement les institutions démocratiques canadiennes, mais entreprennent néanmoins d'autres formes d'IE, comme la répression transnationale⁴.

8. Comme la Commission l'a souligné dans son rapport initial, les activités d'IE ne concernent pas que les processus électoraux ou les institutions démocratiques⁵ – ces derniers faisant partie du mandat de cette Commission. Bien que le Canada lutte contre l'ensemble des

¹ Affaires mondiales Canada, Transcription de l'audience publique, [volume 10](#), pp 9-17.

² Affaires mondiales Canada, Transcription de l'audience publique, [volume 10](#), p 18.

³ Affaires mondiales Canada, Transcription de l'audience publique, [volume 10](#), pp 18-20.

⁴ Résumés des pays, [CAN.SUM.000030](#), (†**Version française du document n'est pas disponible sur le site de la Commission**); Résumé de l'interrogatoire à *huis clos* : Représentant #1 du SCRS, Représentant #2 du SCRS, Ryan Macdonald, Robin Wettlaufer, Greg O'Hayon [WIT0000139](#), p 7-12.†

⁵ Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux (le « [Rapport initial](#) »), p 96.

activités d'IE, ces représentations ne portent que sur celles qui relèvent du mandat de la Commission.

9. Parmi les activités visant les processus électoraux ou les institutions démocratiques qui ont été identifiées dans les rapports de renseignement, on retrouve:

- a. des efforts de soutien illicite à des candidats électoraux considérés comme favorables ou vulnérables à l'influence d'un pays étranger et de ses intérêts⁶;
- b. la réduction au silence de candidats électoraux ou d'élus considérés comme antithétiques aux intérêts d'un pays étranger⁷;
- c. la répression de la participation de candidats aux événements communautaires et électoraux⁸;
- d. des menaces implicites ou explicites, ou support aux membres issus des communautés culturelles du Canada⁹; et
- e. la manipulation de l'information sous toutes ses formes, y compris des campagnes de désinformation sur les plateformes en ligne utilisées par les communautés culturelles¹⁰.

10. L'IE visant les institutions démocratiques se manifeste sous deux formes distinctes: l'IE entre personnes et la manipulation de l'information. L'IE entre personnes comprend des tentatives visant à influencer, intimider, manipuler, interférer, corrompre ou discréditer certains

⁶ Don Valley-Nord, [CAN.SUM.000001.FR](#); Représentants de la République populaire de Chine – Activité d'ingérence étrangère visant l'élection générale de 2019 dans le Grand Vancouver, [CAN.SUM.000003.FR](#); République populaire de Chine — Auteurs de menaces, contact avec des candidats et du personnel, et financement d'auteurs de menaces, [CAN.SUM.000010.FR](#); Activités d'ingérence étrangère du gouvernement de l'Inde dans l'élection générale de 2021, [CAN.SUM.000012.FR](#).

⁷ Représentants de la République populaire de Chine – Activités d'ingérence étrangère visant l'élection générale de 2019 dans le Grand Vancouver, [CAN.SUM.000003.FR](#); Michael Chong, [CAN.SUM.000017.†](#); Opérations par courriel de la RPC contre les parlementaires, [CAN.SUM.000027.†](#); Cas soupçonnés d'ingérence étrangère, CAN.SUM.000031* Document n'est pas disponible sur le site de la Commission.

⁸ Représentants de la République populaire de Chine – Activités d'ingérence étrangère visant l'élection générale de 2019 dans le Grand Vancouver, [CAN.SUM.000003.FR](#).

⁹ Postes de police de la République populaire de Chine, [CAN.SUM.000015.†](#)

¹⁰ Ciblage des parlementaires, [CAN.SUM.000018](#), para 8.†

individus afin de promouvoir les intérêts d'un pays étranger. Ces relations s'entretiennent souvent sur une période prolongée¹¹.

11. La manipulation de l'information en ligne est une menace réelle et actuelle pour les démocraties à travers le monde. Ce phénomène continuera d'être un sujet de préoccupation et de priorité des efforts en cours visant à contrer l'IÉ. La désinformation et la propagande¹² ne sont pas des nouveaux enjeux confrontés par les démocraties. Cependant, l'avènement de l'Internet et des réseaux sociaux a permis à certains acteurs malveillants de développer de nouvelles tactiques d'ingérence et d'atteindre une plus grande portée. L'intelligence artificielle et la sophistication croissante des acteurs malveillants en ligne rendent la désinformation plus difficile à détecter¹³; les mécanismes permissifs de surveillance et de modération mis en place par les médias sociaux privés font en sorte qu'il est plus difficile de la prévenir¹⁴; et la présence de groupes de plus en plus séparés sur les réseaux sociaux la rend plus difficile à contrer¹⁵. De plus, l'accélération du déclin des médias traditionnels a amplifié ces problèmes¹⁶.

12. Outre ce qui précède, les tactiques de répression transnationale sont déployées par certains États pour harceler, intimider et contraindre des individus à se comporter d'une certaine manière¹⁷. L'étendue de la répression transnationale est plus large que celle de l'IÉ ciblant les institutions démocratiques. La Commission a entendu des témoignages courageux de la part des représentants de plusieurs communautés sur cette menace¹⁸. La répression transnationale est inacceptable au Canada et est largement condamnée par des pays partageant les mêmes valeurs. Le Canada s'engage à lutter contre cette grave menace et à travailler avec les communautés culturelles pour renforcer la résilience face à celle-ci¹⁹.

¹¹ Résumé d'interrogatoire à *huis clos*: une subdivision de la Direction du directeur adjoint des exigences (DAE) du SCRS, [WIT0000043.FR](#), para 10.

¹² Bureau du Conseil privé, Transcription de l'audience publique, [volume 29](#), p 54.

¹³ L'Observatoire de l'écosystème des médias, transcription de l'audience publique, [volume 22](#), pp 41-42.

¹⁴ Ministre St-Onge, Transcription de l'audience publique, [volume 33](#), pp 115-116; L'Observatoire de l'écosystème des médias, transcription de l'audience publique, [volume 22](#), pp 43-44.

¹⁵ L'Observatoire de l'écosystème des médias, transcription de l'audience publique, [volume 22](#), pp 30-32.

¹⁶ L'Observatoire de l'écosystème des médias, transcription de l'audience publique, [volume 22](#), pp 8-10.

¹⁷ [Rapport initial](#), pp 101 et 172.

¹⁸ Comités de consultation, Transcription de l'audience publique, [volume 26](#).

¹⁹ Gendarmerie royale du Canada, Transcription de l'audience publique, [volume 27](#), pp 20-21.

C. La réponse du Canada à l'ingérence étrangère

13. Au cours de la dernière décennie, le Canada a agi proactivement et efficacement pour contrer la menace évolutive de l'IE. En effet, le Canada a développé des outils novateurs pour répondre aux types d'activités d'IE observées au Canada et ailleurs. Grâce à ces efforts continus, le Canada a une capacité technologique et humaine plus sophistiquée pour détecter, prévenir et contrer l'IE.

14. Le Canada doit continuer d'agir de manière coordonnée à l'échelle du gouvernement et avec les autres acteurs de la société. Cela comprend, entre autres, la participation d'élus et de leur personnel, des partis politiques, des communautés culturelles, d'organisations de la société civile, des institutions académiques, et des organisations internationales multilatérales. Comme l'ont souligné certains experts lors des audiences sur le volet de consultations relatif aux politiques, l'élément clé pour minimiser la menace d'IE est de favoriser la confiance du public dans les processus démocratiques et la société. Ceci est un défi complexe nécessitant une approche pansociétale plutôt qu'une approche limitée à de simples changements législatifs ou politiques²⁰.

15. La réponse du Canada à l'IE nécessite à la fois urgence et adaptabilité à mesure que la menace évolue. Il n'existe pas de panacée. Toutes les facettes de gouvernement et de la société doivent collaborer pour y répondre²¹.

16. Le Canada a investi des ressources considérables dans le développement de sa capacité à détecter, prévenir et contrer l'IE dans les processus électoraux et les institutions démocratiques. Outre les investissements décrits dans le cadre de la première phase d'enquête de la Commission, le Canada a investi dans les initiatives suivantes :

- a. 10 millions de dollars sur cinq ans pour l'Unité de protection de la démocratie au Bureau du Conseil privé (BCP)²²;

²⁰ Transcription de la table ronde sur les politiques, [volume 36](#), pp [134-135](#).

²¹ Ministre LeBlanc, Transcription de l'audience publique, [volume 34](#), pp [203-205](#); Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), pp [85-86](#).

²² Bureau du Conseil privé, Rapport institutionnel de l'étape 2, [CAN.DOC.000037](#), p [8](#).

- b. 13,4 millions de dollars sur cinq ans pour les efforts continus du Mécanisme de réponse rapide du Canada (MRR) à Affaires mondiales Canada (AMC)²³;
- c. 13,5 millions de dollars sur cinq ans pour le coordonnateur national de la lutte contre l'ingérence étrangère à Sécurité publique²⁴;
- d. 48,9 millions de dollars sur trois ans alloués à la Gendarmerie royale du Canada (GRC) pour aider à contrer les activités hostiles parrainées par des acteurs étatiques²⁵;
- e. 31 millions de dollars sur quatre ans à Patrimoine canadien pour le Programme de contribution en matière de citoyenneté numérique pour contribuer à renforcer la résilience de la société canadienne²⁶;
- f. 917,4 millions de dollars sur cinq ans et 145,8 millions de dollars par année pour permettre au Centre de la sécurité des télécommunications Canada (CST) et à AMC d'améliorer leurs programmes de renseignement et de cyberopérations afin de répondre aux menaces évolutives à la sécurité nationale²⁷;
- g. plus de 655,7 millions de dollars sur huit ans pour permettre au Service canadien du renseignement de sécurité (SCRS) d'améliorer ses capacités en matière de renseignement, de suivre le rythme des progrès technologiques et d'améliorer sa capacité de détection, de prévention et de lutte contre l'ingérence étrangère²⁸.

17. Le Canada a mis plusieurs mesures en place pour détecter, prévenir et contrer l'IE dans les processus électoraux et les institutions démocratiques, y compris : 1) des mécanismes structurels pour surveiller et défendre les processus électoraux; 2) la collaboration avec les parlementaires, les partis politiques et les autres gouvernements; 3) l'information mise à la

²³ Affaires mondiales Canada, Rapport institutionnel de l'étape 2, [CAN.DOC.000031](#), p 4.

²⁴ Le gouvernement du Canada fait le point sur les recommandations visant à lutter contre l'ingérence étrangère, [COM0000609](#) à la p 6; Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), p 92.

²⁵ Résumé de l'entrevue : Gendarmerie royale du Canada (Commissaire Michael Duheme et sous-commissaire, Police fédérale, Mark Flynn), [WIT0000108.FR](#), para 29.

²⁶ Patrimoine canadien, Rapport institutionnel, [CAN.DOC.000035](#), p 2.

²⁷ Centre de la sécurité des télécommunications, Rapport institutionnel de l'étape 2, [CAN.DOC.000029](#), p 7.

²⁸ Service canadien du renseignement de sécurité, Rapport institutionnel de l'étape 2 [CAN.DOC.000044](#), p 9.†

disposition du public afin de développer la résilience des Canadiens, particulièrement les communautés culturelles, à l'égard de l'IÉ; 4) des outils optimisés dont disposent les organismes chargés de la sécurité nationale; et 5) la coordination et la gouvernance au sein du gouvernement, incluant entre les différentes agences. Chacune est abordée dans les sous-sections suivantes.

1. Renforcer le système électoral du Canada

18. Comme la Commission l'a entendu à la première étape de l'enquête, le Canada a annoncé le Plan pour protéger la démocratie en 2019, lequel comprend des mesures visant à renforcer notre système électoral. Le Plan repose sur les quatre piliers d'action suivants : a) améliorer la préparation des citoyens et citoyennes; b) renforcer la préparation organisationnelle; c) lutter contre l'IÉ; et d) bâtir un écosystème de l'information sain²⁹. Les composantes essentielles du Plan comprennent le Groupe d'experts et le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (Groupe de travail) qui ont fait l'objet d'un examen approfondi lors de la première étape.

19. De nouvelles mesures ont été mises en place depuis les élections générales de 2021 et d'autres sont en cours de développement, comme le renouvellement du Plan pour protéger la démocratie³⁰. L'intention est de mettre en œuvre toute mesure qui serait prête pour les prochaines élections générales.

a) Le Groupe d'experts/Le Protocole public en cas d'incident électoral majeur

20. Comme discuté lors de la première étape de la Commission, le Protocole public en cas d'incident électoral majeur a établi le Groupe d'experts, habilitant des hauts fonctionnaires chevronnés, impartiaux et non partisans à la surveillance quotidienne des élections générales et à la coordination de l'intervention du Canada en cas d'activité potentielle d'IÉ pendant la période de transition³¹.

21. Le Groupe d'experts continue d'examiner et de peaufiner son approche. Par exemple, il surveille les élections à l'étranger afin d'en apprendre davantage sur les pratiques exemplaires

²⁹ Bureau du Conseil privé, Transcription de l'audience publique, [volume 11](#), pp 5-11.

³⁰ Bureau du Conseil privé, Transcription de l'audience publique, [volume 23](#), p 120.

³¹ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 63-64.

mises en place par d'autres juridictions. Le Groupe d'experts est prêt à répondre en utilisant différentes approches selon le type d'IE qui se présente³². Le Groupe d'experts élabore également une nouvelle stratégie de communication qui lui permettrait d'accroître sa visibilité avant, pendant et après les élections³³, d'expliquer son rôle et de favoriser la confiance chez les Canadiens. Le public devrait être sensibilisé au rôle qu'occupe le Groupe d'experts avant qu'il n'y ait un incident menaçant l'intégrité d'une élection³⁴.

22. Le Groupe d'experts se prépare activement bien avant les prochaines élections générales³⁵. Les nouveaux membres du Groupe d'experts ont reçu des séances d'information introductives³⁶ et des séances d'information de la part du Groupe de travail sur le contexte actuel de la menace³⁷. Le Groupe d'experts a également rencontré des représentants de la société civile et des représentants des pays alliés pour en apprendre davantage sur leurs expériences en matière d'ingérence électorale³⁸.

23. Afin de se préparer pour son rôle durant la période de transition, le Groupe d'experts a entrepris un travail important pour élaborer des réponses à divers scénarios, notamment, les incidents qui ne dépassent pas le seuil requis pour procéder à une annonce. Le gouvernement doit s'assurer de ne pas jouer le rôle d'arbitre de la vérité et de ne pas intervenir dans le discours démocratique légitime, tout en s'assurant que la population soit mise au courant, le cas échéant³⁹. Le Groupe d'experts doit également veiller à ne pas amplifier la désinformation par inadvertance lorsqu'il prend des mesures pour sensibiliser le public.

24. Il n'est pas nécessaire de modifier fondamentalement la composition du Groupe d'experts. Ces hauts fonctionnaires disposent d'une vaste expérience et compétence dans leurs domaines respectifs et sont habiles à prendre des décisions non partisans. Ils possèdent une

³² Résumé de l'interrogatoire à *huis clos*: John Hannaford et Nathalie G. Drouin, [WIT0000150](#), para 8.†

³³ Résumé de l'interrogatoire à *huis clos*: Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 40.

³⁴ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 64-65.

³⁵ Résumé de l'interrogatoire à *huis clos*: Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 40.

³⁶ Ministère de la Justice Canada, Transcription de l'audience publique, [volume 23](#), pp 219-220.

³⁷ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 61-62.

³⁸ Bureau du Conseil privé, Transcription de l'audience publique, [volume 23](#), pp 148-149; Ministère de la Justice Canada, Transcription de l'audience publique, [volume 23](#), pp 221-223.

³⁹ Résumé de l'interrogatoire à *huis clos* : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 42.

expertise en matière de sécurité nationale, de droits fondamentaux de la personne et d'IE. De plus, ils peuvent exercer de larges pouvoirs afin de répondre rapidement aux menaces, incluant celles qui n'atteignent pas le seuil établi.

b) Le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections

25. Comme étudié en détail lors de la première étape de la Commission, le Groupe de travail regroupe des experts du CST, du SCRS, d'AMC et de la GRC qui coordonnent les efforts de collecte et d'analyse de l'information et du renseignement concernant les menaces qui pèsent sur les processus électoraux. Chaque membre travaille dans le cadre de son mandat pour surveiller et répondre à ces menaces⁴⁰.

26. Le premier ministre a activé le Groupe de travail pour douze élections partielles en 2023 et 2024 ainsi que pour des élections partielles futures. Des opérations plus fréquentes ont permis d'accroître la cohésion du groupe et de mettre en place des nouvelles pratiques tel qu'un exercice impliquant l'intelligence artificielle générative⁴¹.

27. Durant les élections partielles, la période de transition n'est pas en vigueur, donc le Protocole n'est pas déclenché. Le Groupe de travail présente alors le résultat de ses enquêtes au Comité des sous-ministres sur la réponse du renseignement (CSMRR), plutôt qu'au Groupe d'experts. Le CSMRR est un comité présidé par la conseillère à la sécurité nationale et au renseignement auprès du premier ministre (CSNR) qui réunit, entre autres, des sous-ministres de la communauté de la sécurité nationale et le Secrétaire adjoint du Cabinet responsable pour les institutions démocratiques. Le CSMRR se réunit régulièrement pour discuter de l'information et du renseignement nécessitant une réponse opportune⁴². S'il avait observé des activités d'IE, ce comité en aurait informé les ministres responsables et invoqué leurs mandats respectifs⁴³. Après les élections partielles, le Groupe de travail a également fourni un rapport classifié au premier ministre, aux ministres auxquels les organismes membres rendent compte ainsi qu'aux présidents

⁴⁰ Résumé d'entrevue: M. Lyall King, Mme Tara Denham, Mme Gallit Dobner, M. Eric Gordon, représentant du SCRS, [WIT0000045.FR](#), paras 1, et 10-15.

⁴¹ Résumé de l'interrogatoire à huis clos : Représentant #1 du SCRS, Représentant #2 du SCRS, Ryan Macdonald, Robin Wettlaufer, Greg O'Hayon, [WIT0000139](#), para 16.

⁴² Bureau du Conseil privé, Rapport institutionnel, [CAN.DOC.000037](#), pp 29.

⁴³ Security and Intelligence Threats Task Force and the 19 June 2023 Federal By-Elections, [CAN031449](#).†

du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) et de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR)⁴⁴. Par souci de transparence, le Groupe de travail a également publié des rapports non classifiés à la suite des élections partielles afin d'informer le public de ses conclusions⁴⁵. Cette approche a été adoptée pour rassurer les Canadiens sur le fait que les élections partielles ont été libres et justes et pour normaliser le rôle du Groupe de travail auprès de la population canadienne⁴⁶.

28. Le Groupe de travail joue un rôle important dans la surveillance des processus électoraux. L'activation permanente du groupe est présentement étudiée, mais aucune décision ne sera prise avant le dépôt du rapport final de la Commission afin de prendre en compte les avantages et les inconvénients qui s'y rapportent⁴⁷.

2. Collaboration avec les parlementaires, les partis politiques et les autres gouvernements

a) Le Canada a rendu le système politique plus résilient

29. Le Canada reconnaît qu'un élément crucial de sa réponse à l'IE dans les institutions démocratiques est de renforcer la résilience des parlementaires. Les députés et les sénateurs peuvent être, et ont été, des cibles d'IE en raison de leurs positions⁴⁸.

30. Le Canada informe les parlementaires des risques d'IE au moyen de séances d'information générales sur la sécurité, de breffages préventifs, de mesures de réduction de la menace (MRM), de séances d'information non classifiées à l'intention des partis politiques et de séances d'information classifiées aux chefs des partis reconnus à la Chambre des communes ayant l'habilitation de sécurité requise. Ceci est en sus des séances d'information sur la sécurité,

⁴⁴ Threats to the Canadian Federal By-Elections – June 2023 After Action Report, CAN021929 et Final Reports on Foreign Interference in the June 2023 By-Elections, CAN032238. *Documents ne sont pas disponibles sur le site web de la Commission.

⁴⁵ Security and Intelligence to Elections Task Force – Threats to the Canadian Federal By-Elections June 2023, [COM0000606.EN](#).†

⁴⁶ Résumé de l'interrogatoire à *huis clos* : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 47.

⁴⁷ Résumé d'interrogatoire à *huis clos* : l'honorable Dominic LeBlanc, [WIT0000162.FR](#), para 16.

⁴⁸ Ciblage des parlementaires, [CAN.SUM.000018](#), para 3.†

de la formation en cybersécurité et des breffages précédant les voyages dispensés par la Chambre des communes⁴⁹ et le Sénat⁵⁰, qui ont la responsabilité d’informer et de protéger leurs membres contre l’IÉ.

i. Séances d’information générales sur la sécurité à l’intention des parlementaires

31. Le Canada a depuis longtemps mené des séances d’information générales de sécurité à l’intention des nouveaux parlementaires, des ministres et de leur personnel⁵¹ pour les informer des questions de sécurité et de renseignement, incluant l’IÉ. Le Canada a récemment commencé à mener des séances de « rappel » auprès des bureaux de ministres⁵².

ii. La lettre du 18 décembre 2020 aux parlementaires

32. L’ancien ministre de la Sécurité publique, M. Blair, a envoyé une lettre à tous les parlementaires le 18 décembre 2020, afin d’informer les députés des risques d’IÉ et des options qui s’offrent à eux s’ils ont des préoccupations⁵³. Il était nécessaire d’informer tant les députés que les Canadiens de la nature de la menace, du risque qu’elle représentait, et de la manière d’y faire face⁵⁴.

iii. Directives ministérielles sur la menace aux parlementaires

33. En 2023, l’ancien ministre de la Sécurité publique M. Mendicino a émis les *Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires* (les Directives ministérielles). Celles-ci enjoignaient au SCRS de continuer à s’efforcer, dans la mesure du possible, de veiller à ce que les parlementaires soient informés des menaces à la sécurité du Canada qui sont dirigées contre eux⁵⁵. Les Directives ministérielles ont

⁴⁹ Rapport institutionnel de l’Administration de la Chambre des communes, [HOC0000001.FR](#), pp 9-14.

⁵⁰ Résumé de l’entrevue : Administration du Sénat (David Vatcher, Julie Lacroix et Shaila Anwar), [WIT0000126.FR](#), paras 15, 20 et 21.

⁵¹ Résumé de l’interrogatoire à huis clos : Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, [WIT0000143](#), p 2.†

⁵² Résumé de l’interrogatoire à huis clos : Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, [WIT0000143](#), p 8.†

⁵³ Letter to Minister of Public Safety, [CAN003326](#).†

⁵⁴ Ministre Blair, Transcription de l’audience publique, [volume 33](#), p 73.

⁵⁵ Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians, [CAN021931](#).†

depuis été complémentées par un protocole de gouvernance qui précise exactement comment les Directives ministérielles doivent être mises en œuvre⁵⁶.

iv. Les breffages préventifs et les MRM

34. Dès 2018, le SCRS a fourni des breffages préventifs à plus de 70 députés afin d'accroître leur sensibilisation et leur résilience, et celle de leur personnel, à l'égard de l'IE, et de leur expliquer l'ensemble de la menace à laquelle ils pourraient faire face en tant qu'élus⁵⁷.

35. En plus des breffages préventifs, le SCRS a utilisé son pouvoir d'effectuer des MRM pour offrir de l'information aux députés qui ont été la cible d'IE⁵⁸. Sous réserve de l'exigence d'un mandat dans certains cas, le SCRS peut utiliser son pouvoir de prendre des MRM lorsqu'il y a des motifs raisonnables de croire qu'il y a une menace à la sécurité nationale et qu'une MRM peut réduire celle-ci. Les MRM se retrouvent généralement parmi l'une des trois catégories suivantes : les mesures de dissuasion, où de l'information est transmise à un sujet dans le but d'influencer son comportement; les mesures d'exploitation, par laquelle de l'information est divulguée à une tierce partie afin de permettre à celle-ci d'utiliser ses propres pouvoirs pour empêcher le sujet de mener des activités liées à la menace; et les mesures d'ingérence, par laquelle le SCRS influe directement sur la capacité du sujet de faire quelque chose⁵⁹. Entre janvier 2019 et aujourd'hui⁶⁰, le SCRS a réalisé neuf (9) MRM sans mandat touchant l'IE à l'égard des institutions et des processus démocratiques du Canada. Bien que les MRM peuvent autoriser le SCRS de partager certains renseignements classifiés afin de permettre à des tiers d'agir contre des activités liées à une menace identifiée, le SCRS doit tenir compte des risques d'agir ainsi. Partager de l'information classifiée avec un individu qui n'a pas la cote de sécurité

⁵⁶ Implementation of Ministerial Direction to the Canadian Security Intelligence Service on Threats to Parliament and Parliamentarians, [CAN021638_0001](#).†

⁵⁷ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 10](#), pp [255-256](#) et [258-259](#).

⁵⁸ Les députés Chong, O'Toole, Kwan et Chiu ont été breffés par le SCRS en vertu de son pouvoir de MRM.

⁵⁹ Mesures de réduction de la menace prises par le SCRS, [CAN.SUM.000028](#).†

⁶⁰ Mesures de réduction de la menace prises par le SCRS, [CAN.SUM.000028](#), pp [2-3](#)†; Service canadien du renseignement de sécurité, Rapport institutionnel de l'étape 2, Annexe G - Aperçu des mesures de réduction de la menace prises contre l'ingérence étrangère de 2019 à aujourd'hui, [CAN.DOC.000018.003](#).

requis, et qui n'est pas assujéti à l'obligation de garder l'information confidentielle, peut entraîner un grave préjudice à la sécurité nationale⁶¹.

36. En 2023, le SCRS a utilisé son pouvoir en matière de MRM pour fournir des breffages préventifs aux députés Chong, Chiu, Kwan et O'Toole. S'appuyant sur des breffages antérieurs, les breffages effectués dans le cadre de MRM ont été le fruit de la discussion plus large sur les menaces aux députés suivant la mise en œuvre des Directives ministérielles⁶².

v. Séances d'information aux partis politiques et aux caucus

37. En juin 2024, le Canada a fourni des séances d'information non classifiées sur l'IE aux caucus des partis à la Chambre des communes⁶³. Ces séances d'information avaient pour but d'augmenter le niveau de sensibilisation à l'IE parmi les députés et de fournir de l'information spécifique visant la protection de leur « identité numérique »⁶⁴. Ces séances d'information ont été développées à la demande et avec la contribution du sergent d'armes⁶⁵, compte tenu de sa responsabilité à l'égard de la sécurité de certains aspects du Parlement et des députés⁶⁶. Bien qu'il y ait des allégations devant cette Commission selon lesquelles la mise en œuvre de ces séances d'information aurait tardé, ces allégations font fi du contexte, soit des défis extraordinaires liés à la pandémie de Covid-19 et, par la suite, aux élections de 2021. Quoiqu'il en soit, les députés avaient déjà été alertés de la menace d'IE par la lettre du ministre Blair de décembre 2020 et par les séances d'information générales sur la menace donnée à tous les nouveaux députés. Tel que discuté, le SCRS a fourni de nombreux breffages préventifs à des députés spécifiques⁶⁷.

⁶¹ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), p 67.

⁶² Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), pp 56-60.

⁶³ Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), pp 132-133.

⁶⁴ Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), p 133.

⁶⁵ Ministre LeBlanc, Transcription de l'audience publique, [volume 34](#), p 151; Résumé d'interrogatoire à huis clos : Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère, [WIT0000144](#), para 53.†

⁶⁶ Ministre LeBlanc, Transcription de l'audience publique, [volume 34](#), pp 150-152.

⁶⁷ Cabinet du Premier ministre, Transcription de l'audience publique, [volume 34](#), pp 31-32.

38. Le Groupe de travail a également fourni des séances d'information non classifiées aux représentants des partis politiques avant chaque élection partielle depuis juin 2023⁶⁸. Tous les partis politiques étaient invités⁶⁹.

vi. Séances d'information aux chefs des partis politiques

39. Le Canada a offert des séances d'information classifiées aux chefs des partis politiques depuis 2023, à l'aide d'ensembles de produits de renseignement assemblés sur mesure pour le chef de parti pour inclure l'information que le chef de parti a « besoin de connaître ». Les chefs des partis rencontrent des agents de sécurité et du renseignement et peuvent poser des questions pour confirmer leur compréhension⁷⁰. Afin de recevoir des séances d'information très secrètes, les chefs de parti doivent obtenir l'habilitation de sécurité requise. À noter, le fait d'être membre du Conseil privé du Roi ne donne pas, en soi, le droit aux députés ou aux chefs de partis d'accéder à des renseignements classifiés⁷¹.

40. À ce jour, le but de ces séances d'information a principalement été d'informer les chefs des partis politiques des activités d'IÉ qui peuvent affecter leurs membres et leurs partis, et de les outiller pour prendre les mesures qu'ils estiment nécessaires afin de protéger leurs partis contre l'IÉ. Ces séances d'information leur permettent d'utiliser les outils qu'ils détiennent pour traiter des activités d'IÉ au sein de leur propre parti, telle que l'approbation finale des candidats du parti ou la nomination à différents rôles qui pourraient exacerber des risques particuliers⁷². À l'avenir, ces séances d'information vont inclure l'information allant au-delà de l'ingérence étrangère.

⁶⁸ Résumé d'entrevue: Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (représentant du CST, trois représentants du SCRS au sein du Groupe de travail, Robin Wettlaufer, Greg O'Hayon), [WIT0000109.FR](#), para 49; SITE TF Briefing to Unclassified Political Parties, [CAN044590](#)†; Security and Intelligence Threats to the Elections Task Force (SITE TF) Foreign Interference: A Threat to Canada's National Security, [CAN044568](#)†; Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, Transcription de l'audience publique, [volume 27](#), pp 153-154.

⁶⁹ Bureau du Conseil privé, Transcription de l'audience publique, [volume 29](#), pp 50, 80-83.

⁷⁰ Résumé de l'interrogatoire à *huis clos*: Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, [WIT0000143](#), pp 8-9.†

⁷¹ Comme il est indiqué dans la preuve, les ministres sont soumis à une évaluation de sécurité qui, bien qu'elle diffère d'une habilitation de sécurité, constitue un processus équivalent.

⁷² Résumé de l'interrogatoire à *huis clos* : Cabinet du Premier ministre, [WIT0000163](#), para 27†; Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 59-67; Ad-Hoc Classified Briefings, [CAN047007](#).†

vii. Soutien pour la cybersécurité des partis politiques

41. Le Centre canadien pour la cybersécurité du CST maintient un point de contact pour les partis politiques en matière de cybersécurité et fournit des conseils et des orientations personnalisés pour les candidats sur son site web⁷³.

b) Partenariats du Canada avec les autres ordres de gouvernement

42. L'IE affecte non seulement tous les aspects de la société, mais aussi tous les ordres de gouvernement⁷⁴. La coopération entre les différents ordres de gouvernement est essentielle compte tenu du partage constitutionnel des compétences au Canada⁷⁵. Bien que les organismes de sécurité nationale du Canada puissent partager de l'information à propos de l'IE et de ses répercussions possibles à l'échelle locale et régionale, les provinces et les territoires ont compétence en matière d'administration municipale, d'éducation, de littératie numérique et d'éducation civique. Ils jouent un rôle essentiel de veiller à ce que les pratiques démocratiques soient transmises aux générations suivantes⁷⁶.

43. Le Canada a priorisé une vaste collaboration avec les gouvernements provinciaux, territoriaux, municipaux et autochtones sur l'IE et les questions connexes. Le Canada a soulevé le besoin d'augmenter la littératie numérique et médiatique afin de combattre la manipulation de l'information et le rôle que joue le système d'éducation provincial pour augmenter cette littératie⁷⁷. Il a partagé un guide sur la désinformation et des trousseaux d'outils sur l'IE⁷⁸. Le

⁷³ Centre de la sécurité des télécommunications, Rapport institutionnel, [CAN.DOC.000006](#), p 11.

⁷⁴ Résumés des pays, [CAN.SUM.000030](#), p 4†; Foreign Interference and You, [COM0000061](#), p 3; Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, Transcription de l'audience publique, [volume 27](#), p 111; Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), pp 11-12.

⁷⁵ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 77, 78-79.

⁷⁶ Bureau du Conseil privé, Transcription de l'audience publique, [volume 23](#), pp 189-190.

⁷⁷ Résumé de l'interrogatoire à *huis clos* : John Hannaford et Nathalie G. Drouin, [WIT0000150](#), para 41†; Résumé d'entrevue: ministère de la Justice (Shalene Curtis-Micallef, Samantha Maislin Dickson, Heather Watts, Michael Sousa, [WIT0000100.FR](#), para 18.

⁷⁸ Bureau du Conseil privé, Transcription de l'audience publique, [volume 23](#), pp 135-136; Résumé de l'interrogatoire à *huis clos* : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 22.

Canada envisage également un plan d'action national intégré avec les provinces et les territoires sur la manipulation de l'information⁷⁹.

44. Les ministres de la Justice et de la Sécurité publique du Canada profitent de leurs réunions régulières avec leurs homologues pour discuter des questions relatives à l'IE⁸⁰. Des hauts fonctionnaires, comme le greffier du Conseil privé, le commissaire de la GRC et plusieurs sous-ministres, ont également discuté d'IE et de sujets connexes avec leurs homologues provinciaux, territoriaux et autochtones, y compris du besoin de mettre en place l'infrastructure de sécurité nécessaire afin de permettre le partage d'information classifiée⁸¹. Des discussions similaires ont eu lieu au niveau opérationnel⁸². Enfin, le Canada aide à protéger les infrastructures électorales provinciales, territoriales, et municipales, notamment en fournissant des conseils et des orientations en matière de cyber résilience⁸³.

c) La coordination du Canada avec ses partenaires internationaux

45. Le Canada n'est pas seul à subir de l'IE ; plusieurs de ses alliés ont subi des variantes de ces efforts néfastes. Le Canada s'engage avec ses alliés et des pays semblables par rapport aux questions opérationnelles et politiques pour développer une réponse collective à la menace commune d'IE dans les processus électoraux et institutions démocratiques, et s'inspirer de l'expérience nationale de chacun.

46. Parmi celles-ci, la collaboration du Canada avec ses alliés du Groupe des cinq est un point de contact international inestimable et est fondamental pour le Canada. La raison d'être de

⁷⁹ Résumé d'entrevue: Isabelle Mondou et Amy Awad, [WIT0000098.FR](#), paras [32](#) et [55](#).

⁸⁰ Ministre LeBlanc, Transcription de l'audience publique, [volume 34](#), p [127](#).

⁸¹ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp [77-78](#); Résumé d'entrevue: ministère de la Justice (Shalene Curtis-Micallef, Samantha Maislin Dickson, Heather Watts, Michael Sousa, [WIT0000100.FR](#), para [18](#); Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), p [138](#); Gendarmerie Royale du Canada, Transcription de l'audience publique, [volume 27](#), at pp [9-10](#), [15-17](#), [24](#); Résumé d'interrogatoire à *huis clos* : Michael Duheme, commissaire de la GRC, Mark Flynn, sous-commissaire de la Police fédérale, et Brigitte Gauvin, commissaire adjointe de la Police fédérale, Sécurité nationale, [WIT0000137](#), para [31](#).†

⁸² Résumé d'entrevue: ministère de la Justice (Shalene Curtis-Micallef, Samantha Maislin Dickson, Heather Watts, Michael Sousa, [WIT0000100.FR](#), para [17](#).

⁸³ Résumé d'entrevue : Centre de la sécurité des télécommunications (Caroline Xavier, Rajiv Gupta, Alia Tayyeb), [WIT0000122.FR](#), paras [8-9](#).

l'alliance du Groupe des cinq est l'échange de renseignements⁸⁴. La compréhension du Canada de l'IE est sophistiquée en partie grâce à l'étendue du renseignement qu'il partage et reçoit de ses partenaires du Groupe des cinq⁸⁵. Ces partenaires partagent de façon collaborative de l'information tant opérationnelle que relativement au développement de politiques, notamment par l'entremise du Forum sur la politique du renseignement (qui coordonne la communauté de la sécurité et du renseignement au sein du Groupe des cinq sur des questions de politiques tournées vers l'avenir dans une sphère qui évolue rapidement)⁸⁶. Le Groupe des cinq collabore également au niveau ministériel. Dans chacune de ses alliances, le Canada est de plus en plus reconnu comme un chef de file en matière de lutte contre l'IE⁸⁷.

47. Le Canada s'est entretenu avec ses homologues internationaux pour discuter des meilleures pratiques pour détecter, prévenir et contrer l'IE dans les élections, en suivant une approche collaborative et lucide. Des responsables canadiens ont rencontré leurs homologues du Royaume-Uni et de la France pour connaître leur expérience avec l'IE dans leurs élections⁸⁸, ainsi que des groupes de la société civile taïwanaise à l'avant-garde de la détection de la désinformation en ligne⁸⁹. Le Canada apprend de ses partenaires internationaux et travaille avec eux sur le sujet des cadres réglementaires pour les plateformes des médias sociaux, qui sont importants pour le succès des démocraties à contrecarrer la désinformation⁹⁰. En 2023, en partenariat avec les Pays-Bas, le Canada a lancé la première Déclaration globale sur l'intégrité de

⁸⁴ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), p 19; Résumé d'entrevue : Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), paras 43-44; Résumé d'entrevue : Gendarmerie Royale du Canada (commissaire Michael Duheme et sous-commissaire, Police fédérale, Mark Flynn), [WIT0000108.FR](#), para 33; Résumé d'interrogatoire à huis clos : à propos: Rapport CPSNR: David Vigneault, Michelle Tessier, Cherie Henderson, Vanessa Lloyd, Bo Basler, [WIT0000136](#), para 26.†

⁸⁵ Résumé d'entrevue : Centre de la sécurité des télécommunications (Caroline Xavier, Rajiv Gupta, Alia Tayyeb), [WIT0000122.FR](#), para 53.

⁸⁶ Résumé d'entrevue : Bureau du Conseil privé – Secrétariat de la sécurité et du renseignement et Secrétariat de l'évaluation du renseignement (Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, Martin Green et Lisa Ducharme), [WIT0000110.FR](#), para 5.

⁸⁷ Résumé d'entrevue : Marco Mendicino, député fédéral de la circonscription d'Eglinton-Lawrence, [WIT0000105](#), para 15†; Résumé d'entrevue : l'honorable Dominic LeBlanc, [WIT0000103.FR](#), para 24.

⁸⁸ Bureau du Conseil privé, Transcription de l'audience publique, [volume 23](#), p 148.

⁸⁹ Bureau du Conseil privé, Transcription de l'audience publique, [volume 23](#), p 164.

⁹⁰ Résumé d'entrevue : l'honorable Pascale St-Onge [WIT0000097.FR](#), para 16; Ministre St-Onge, Transcription de l'audience publique, [volume 33](#), pp 119-120.

l'information en ligne qui établit une série d'engagements internationaux visant à servir de cadre et de guide aux gouvernements pour faire respecter l'intégrité de l'information en ligne⁹¹.

3. Le Canada bâtit la résilience du public à l'IE

48. Une population bien informée, engagée envers la démocratie, est la défense principale du Canada contre l'IE⁹². En mettant la lumière sur la menace, en éduquant la population, en favorisant la participation informée, une approche pansociétale peut prendre forme⁹³. La résilience des Canadiens va continuer à prendre de l'ampleur par le travail présent et futur avec le public en général, les communautés culturelles, et les organisations de la société civile.

49. Comme les autres démocraties, la réponse du Canada à la manipulation de l'information et la désinformation est complexifiée par la difficulté technologique d'identifier les vrais auteurs derrière l'information en ligne, le besoin d'établir un équilibre entre la prise d'actions concernant de l'IE en ligne avec la liberté d'expression, et le contrôle limité que chaque pays a vis-à-vis le contenu sur l'Internet. Le Canada continue d'explorer de nouveaux moyens de développer la résilience du public face à la manipulation de l'information en ligne et la désinformation.

50. Le Canada a considérablement accru ses communications avec le public, afin d'assurer une plus grande transparence concernant la nature de la menace d'IE, la réponse du gouvernement et les mesures que le public peut adopter afin de se protéger⁹⁴. Depuis 2017, le Canada rend accessible au public, dans plusieurs langues, des produits pertinents sur l'IE dans les processus et institutions démocratiques, afin de sensibiliser les groupes culturels, religieux et

⁹¹ Résumé d'entrevue: l'honorable Mélanie Joly, [WIT0000096.FR](#), para 13; Résumé d'entrevue : l'honorable Mélanie Joly, [WIT0000148](#), para 10; Ministre Joly, Transcription de l'audience publique, [volume 32](#), p 128.

⁹² Ministre Gould, Transcription de l'audience publique, [volume 14](#), p 15.

⁹³ Bureau du Conseil privé, Transcription de l'audience publique, [volume 30](#), p 145; Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), pp 216-217; Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 4](#), p 79.

⁹⁴ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 15](#), p 12; Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 10](#), pp 148-149; Rapport institutionnel du Service canadien du renseignement de sécurité (SCRS), Phase 2, [CAN.DOC.000044](#), p 16†; Résumé d'entrevue: Centre de la sécurité des télécommunications, (Caroline Xavier, Rajiv Gupta, Alia Tayyeb) [WIT0000122.FR](#), paras 4-5, 12, 51-52; Résumé d'interrogatoire à *huis clos* : Caroline Xavier, Alia Tayyeb, Sami Khoury [WIT0000133](#), paras 5-15, 72-75†; Centre de la sécurité des télécommunications Canada, Transcription de l'audience publique, [volume 23](#), pp 10-19; Gendarmerie royale du Canada, Transcription de l'audience publique, [volume 27](#), p 21.

ethniques aux auteurs de menace d'IE et à leurs méthodes⁹⁵. La communication d'information au public peut également atténuer une menace pour la sécurité publique, comme l'a récemment fait la GRC dans le contexte de l'implication d'agents du gouvernement de l'Inde dans des activités criminelles graves au Canada⁹⁶.

51. De plus, cette Commission a attiré une attention importante du public sur la menace d'IE dans les processus électoraux et les institutions démocratiques. Pour contribuer à cet effort, le Canada a fourni un accès sans précédent à de l'information classifiée et des renseignements confidentiels du Cabinet à l'appui des travaux de la Commission et a également collaboré avec la Commission pour offrir, autant que possible, un accès au public à cette information.

a) *La collaboration avec les communautés culturelles*

52. Les efforts du Canada pour détecter, prévenir et contrer l'IE requièrent l'établissement de relations de confiance avec les communautés culturelles, car elles sont souvent les premières victimes de l'IE. Tant le SCRS que la GRC se consacrent au développement de telles relations, sous la coordination de Sécurité publique; toutefois, le Canada reconnaît que davantage d'efforts sont requis⁹⁷. Il est essentiel de créer des occasions régulières et officielles pour un dialogue entre le public et le gouvernement afin d'établir ces importantes relations, comme par exemple la Table ronde transculturelle sur la sécurité (Table ronde) qui fournit des conseils et de la rétroaction aux ministres de la Sécurité publique et de la Justice⁹⁸. Les consultations avec la Table ronde et d'autres groupes de communautés culturelles ont aidé le gouvernement à rédiger la *Loi sur la lutte contre l'ingérence étrangère* qui offre un cadre robuste pour aborder les

⁹⁵Rapport institutionnel du Service canadien du renseignement de sécurité (SCRS), Phase 2, [CAN.DOC.000044](#), p 16†; Gendarmerie royale du Canada, Transcription de l'audience publique, [volume 27](#), p 21; Bureau du Conseil privé, Transcription de l'audience publique, [volume 21](#), pp 140-142; Résumé d'entrevue: Centre de la sécurité des télécommunications (Caroline Xavier, Rajiv Gupta, Alia Tayyeb), [WIT0000122.FR](#), paras 4-5, 12, 51-52; Résumé d'interrogatoire à huis clos : Caroline Xavier, Alia Tayyeb, Sami Khoury, [WIT0000133](#), paras 5-15, 72-75†; Centre de la sécurité des télécommunications Canada, Transcription de l'audience publique, [volume 23](#), pp 10-19 et 88; Résumé de l'interrogatoire à huis clos : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 23.

⁹⁶ [GRC Déclaration de la GRC sur l'activité criminelle au Canada ayant des liens avec des agents du gouvernement indien.](#)

⁹⁷ Résumé d'interrogatoire à huis clos : Michael Duheme, commissaire de la GRC, Mark Flynn, sous-commissaire de la Police fédérale, et Brigitte Gauvin, commissaire adjointe de la Police fédérale, Sécurité nationale, [WIT0000137](#), para 58†; Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), pp 136-137; Résumé d'interrogatoire à huis clos : Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère, [WIT0000144](#), para 70†; Service Canadien du Renseignement de Sécurité, Transcription de l'audience publique, [volume 24](#), p 89.

⁹⁸ Ministère de la Justice Canada, Transcription de l'audience publique, [volume 23](#), pp 215-216.

activités néfastes qui font obstruction aux intérêts canadiens⁹⁹, tout en s’assurant que les mesures ne vont pas trop loin et qu’elles ne marginalisent pas les communautés culturelles ou ne limitent pas leur voix et leur expression politique¹⁰⁰. Les consultations avec les communautés permettent le partage d’un large éventail de points de vue, ce qui contribue à éclairer les politiques et les conseils au gouvernement préparés par des ministères comme Sécurité publique¹⁰¹.

b) Collaborer avec des organisations de la société civile afin de bâtir la résilience

53. Une approche pansociétale est requise pour aborder efficacement la menace d’IÉ qui se présente par la manipulation de l’information et la désinformation. Bâtir une population résiliente et vigilante en renforçant la capacité des citoyens canadiens d’examiner de manière critique les médias qu’ils consomment et en collaborant avec des organisations de la société civile, telles que CIVIX et Digital Public Square, afin de dénoncer activement la désinformation est essentiel pour développer une réponse efficace à l’IÉ¹⁰². Le Canada a une stratégie à plusieurs volets qui inclut l’Initiative de citoyenneté numérique, le Réseau canadien de recherche sur les médias numériques, l’appui aux médias forts et indépendants et la Déclaration du Canada sur l’intégrité électorale en ligne.

i. Initiative de citoyenneté numérique

54. L’Initiative de citoyenneté numérique vise à doter les citoyens des outils dont ils ont besoin afin de prendre des décisions éclairées en tant que consommateurs d’information, en bâtissant la résilience des citoyens face à la désinformation en ligne et en établissant des partenariats pour soutenir un écosystème d’information sain¹⁰³.

55. Le Canada a également créé le Programme de contribution en matière de citoyenneté numérique, qui soutient les priorités de l’Initiative de citoyenneté numérique en fournissant une aide financière de durée limitée pour la recherche et les activités axées sur les citoyens. L’accent

⁹⁹ *Loi sur la lutte contre l’ingérence étrangère*, [LC 2024](#), ch. 16.

¹⁰⁰ Ministère de la Justice Canada, Transcription de l’audience publique, [volume 23](#), pp [215-219](#).

¹⁰¹ Résumé d’interrogatoire à *huis clos* : Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère, [WIT0000144](#), para [78](#).†

¹⁰² Résumé d’entrevue: l’honorable Pascale St-Onge, [WIT0000097.FR](#), para [12](#).

¹⁰³ Résumé d’entrevue: l’honorable Pascale St-Onge, [WIT0000097.FR](#), para [12](#).

a récemment été mis sur la lutte à la désinformation provenant d'États étrangers, tels que la RPC, et son impact sur les communautés culturelles¹⁰⁴.

ii. Réseau canadien de recherche sur les médias numériques (RCRMN)

56. Il y a et devrait y avoir des limites à la capacité de l'État d'intervenir contre la désinformation. En développant des politiques en réponse à la désinformation, le Canada doit assurer l'équilibre entre la liberté d'expression et les préjudices que la désinformation pourrait causer¹⁰⁵. Les Canadiens ont à la fois le droit de s'exprimer librement et de recevoir de l'information en ligne. Il serait incompatible avec le droit et les valeurs canadiennes que le Canada se présente comme l'ultime arbitre de qui dit la « vérité » dans l'espace numérique¹⁰⁶. Les représentants du gouvernement doivent être prudents lorsqu'ils font des commentaires à propos de fausses informations en ligne, particulièrement pendant une élection, car ils risqueraient d'outrepasser leur rôle non partisan¹⁰⁷.

57. Financé par le Canada grâce à une subvention de recherche¹⁰⁸, le RCRMN est un réseau de chercheurs et d'universitaires dont le noyau se trouve à l'Observatoire de l'écosystème médiatique¹⁰⁹. Indépendant du gouvernement, le RCRMN surveille l'écosystème numérique national pour détecter la manipulation de l'information et déterminer si cette manipulation a un impact ou est amplifiée de façon artificielle dans l'écosystème médiatique¹¹⁰. Lorsqu'un incident lié à l'information est détecté, comme la dissémination artificielle de désinformation, le RCRMN répond par des alertes publiques, des mises à jour d'incidents et des résumés d'incidents¹¹¹. Le RCRMN envisage de surveiller l'écosystème numérique national pendant la prochaine élection

¹⁰⁴ Résumé d'entrevue: l'honorable Pascale St-Onge, [WIT0000097.FR](#), paras [13-14](#).

¹⁰⁵ Résumé d'entrevue: Isabelle Mondou et Amy Awad, [WIT0000098.FR](#), para [11](#).

¹⁰⁶ Résumé d'entrevue: Isabelle Mondou et Amy Awad, [WIT0000098.FR](#), para [37](#).

¹⁰⁷ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), p [199](#). À noter, l'attention est portée sur l'amplification artificielle de l'information relative aux processus électoraux.

¹⁰⁸ Le Programme de contribution en matière de citoyenneté numérique a fourni au RCRMN un financement de 5,5 millions de dollars sur 3 ans, Enquête publique sur l'ingérence étrangère, Rapport institutionnel (RI) – Patrimoine Canadien, [CAN.DOC.000035](#), p [4](#); Observatoire de l'écosystème des médias, transcription de l'audience publique, [volume 22](#), p [60](#).

¹⁰⁹ Résumé d'entrevue: Observatoire de l'écosystème médiatique (Aengus Bridgman, Peter Loewen et Taylor Owen), [WIT0000089.FR](#), paras [30](#), [40-41](#).

¹¹⁰ Résumé d'entrevue: Observatoire de l'écosystème médiatique (Aengus Bridgman, Peter Loewen et Taylor Owen), [WIT0000089.FR](#), paras [56-60](#); Observatoire de l'écosystème des médias, transcription de l'audience publique, [volume 22](#), pp [72-73](#).

¹¹¹ Résumé d'entrevue: Observatoire de l'écosystème médiatique (Aengus Bridgman, Peter Loewen et Taylor Owen), [WIT0000089.FR](#), paras [61-67](#).

générale pour identifier toute manipulation de l'information et ses impacts¹¹². Bien qu'indépendant du gouvernement, le travail du RCRMN alimente celui des responsables gouvernementaux, notamment le Groupe d'experts¹¹³. Ses rapports contribuent également au travail d'élaboration des politiques du Canada¹¹⁴.

iii. Appui aux médias forts et indépendants

58. L'accès à des sources d'information fiables et reconnues est un élément vital de l'écosystème démocratique. En tant que profession régie par des normes éthiques bien établies, les institutions et pratiques journalistiques traditionnelles jouent un rôle important pour fournir de l'information fondée sur les faits au public. Cette information factuelle joue un rôle clé dans la lutte contre la mésinformation et la désinformation¹¹⁵.

59. Le Canada a adopté des mesures pour soutenir un écosystème de médias forts et indépendants. L'Initiative de journalisme local, le Crédit d'impôt pour la main-d'œuvre journalistique canadienne, et la *Loi sur les nouvelles en ligne*¹¹⁶ répondent aux défis auxquels les agences de presse sont confrontées à être rémunérées pour leur travail. Le Canada a fait un bon investissement dans son radiodiffuseur public national pour s'assurer que les citoyens ont accès à une source d'information fiable¹¹⁷.

iv. La Déclaration du Canada sur l'intégrité électorale en ligne (la Déclaration)

60. Le Canada collabore avec les plateformes de médias sociaux pour favoriser des élections justes, libres et sûres. La Déclaration est une entente volontaire entre le Canada et les plateformes de médias sociaux qui énonce leurs responsabilités de base quant à l'intégrité et la transparence¹¹⁸. Elle crée un point de contact avec les plateformes et les responsabilise quant à

¹¹² Résumé d'entrevue: Observatoire de l'écosystème médiatique (Aengus Bridgman, Peter Loewen et Taylor Owen), [WIT0000089.FR](#), para 44.

¹¹³ Résumé d'entrevue: Observatoire de l'écosystème médiatique (Aengus Bridgman, Peter Loewen et Taylor Owen), [WIT0000089.FR](#), paras 32-33; Observatoire de l'écosystème des médias, transcription de l'audience publique, [volume 22](#), p 139.

¹¹⁴ Résumé d'entrevue: Isabelle Mondou et Amy Awad, [WIT0000098.FR](#), para 49.

¹¹⁵ Résumé d'entrevue: l'honorable Pascale St-Onge, [WIT0000097.FR](#), paras 3 et 5.

¹¹⁶ *Loi sur les nouvelles en ligne*, [LC 2023](#), ch. 23.

¹¹⁷ Résumé d'entrevue: l'honorable Pascale St-Onge, [WIT0000097.FR](#), paras 6-9.

¹¹⁸ Résumé de l'interrogatoire à *huis clos* : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 35.

leur engagement de mettre en œuvre leurs lignes directrices communautaires¹¹⁹. Quatre plateformes ont signé la déclaration en 2019 et trois autres l'ont fait en 2021¹²⁰.

61. Le Canada est entré à nouveau en contact avec les diverses plateformes pour discuter de la Déclaration en prévision de la prochaine élection générale. Une des initiatives prises par le Canada a été de communiquer avec Tencent, la société mère de WeChat, pour qu'elle s'engage à respecter la Déclaration¹²¹.

4. La communauté de la sécurité nationale du Canada a la capacité de détecter, prévenir, et contrer l'IÉ

62. La communauté de la sécurité nationale du Canada est guidée par les Priorités en matière de renseignement du Cabinet, qui identifient tous les deux ans les sujets qui ont un intérêt stratégique pour le gouvernement et qui nécessitent le soutien du renseignement pour promouvoir les intérêts canadiens. En se basant sur ces Priorités, les ministères et agences développent des Besoins liés au renseignement détaillés pour guider leur travail¹²². Pour les périodes d'exercice 2017-2019 à 2023-2025, le Cabinet a continuellement identifié l'IÉ dans les processus électoraux et les institutions démocratiques comme une priorité de renseignement du Canada¹²³.

63. Les systèmes du Canada pour détecter, prévenir et contrer l'IÉ dans nos processus électoraux et institutions démocratiques sont robustes. Les quatre agences qui sont au cœur de la réponse du Canada à l'IÉ fournissent leur expertise que ce soit dans le domaine du renseignement d'origine humaine (SCRS), du renseignement électromagnétique étranger et de la cybersécurité (CST), de la politique étrangère et de la manipulation de l'information en ligne (AMC), ou de l'application de la loi (GRC). Que ce soit par l'entremise d'une enquête, du dépôt d'accusations, de la coordination d'une réponse diplomatique avec des États et des alliés qui

¹¹⁹ Résumé de l'interrogatoire à huis clos : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 35.

¹²⁰ Résumé de l'interrogatoire à huis clos : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 35.

¹²¹ Bureau du Conseil privé, Transcription de l'audience publique, [volume 23](#), p 138.

¹²² Résumé de l'interrogatoire à huis clos : Nabih Eldebs, Adelle Ferguson, Marie-Hélène Chayer, Bridget Walshe, Michael MacDonald, [WIT0000143](#), pp 6-7.†

¹²³ Résumé d'entrevue : L'honorable Bill Blair, ministre de la Défense nationale, [WIT00000102.FR](#), para 8.

partagent notre point de vue, ou d'une MRM pour réduire et atténuer le préjudice, la communauté de la sécurité nationale est outillée pour détecter, prévenir et contrer les activités d'IÉ sous toutes leurs formes. En agissant en vertu de leurs mandats respectifs, ces agences protègent le Canada, nos institutions et processus démocratiques, et l'ensemble de nos citoyens.

64. Grâce à une vigilance constante et à la collaboration des ministères et agences face à la menace de l'IÉ, les institutions et processus démocratiques du Canada sont forts et résilients. Le Canada et les Canadiens doivent continuer d'accroître cette force.

65. L'ajout législatif le plus récent à la capacité du Canada à détecter, prévenir et contrer l'IÉ est C-70, la *Loi concernant la lutte contre l'ingérence étrangère*. Appuyé par tous les partis politiques dans la Chambre des communes¹²⁴, C-70 offre aux agences de sécurité nationale du Canada des pouvoirs modernisés pour lutter contre les tactiques utilisées par les acteurs étatiques hostiles qui évoluent constamment. Les recommandations de la Commission sont les bienvenues pour déterminer la meilleure façon de contrer l'IÉ à la lumière de ces nouveaux outils.

a) *SCRS – Outils de renseignement*

66. Le SCRS est bien équipé contre l'IÉ, notamment avec ses demandes de mandats, ses breffages préventifs, ses MRM et les changements récents apportés par C-70. Le SCRS peut dorénavant émettre des alertes non classifiées pour sensibiliser davantage le public et les gouvernements infranationaux à propos des actes hostiles commis par des États étrangers, comme des tentatives d'IÉ¹²⁵.

67. C-70 a modifié la *Loi sur le Service canadien de renseignement de sécurité*¹²⁶ pour permettre au SCRS de mieux opérer dans un monde numérique et répondre à l'évolution des menaces¹²⁷. Il autorise également le SCRS à partager des renseignements avec ses partenaires à l'extérieur du gouvernement fédéral sous réserve d'une habilitation de sécurité appropriée et d'un « besoin de savoir »¹²⁸. Cette modification va contribuer à accroître la résilience de la

¹²⁴ Rapport Sommaire : Résumé de la *Loi sur la lutte contre l'ingérence étrangère* (projet de loi C-70), [COM0000586.FR](#), para 79; Résumé d'entrevue : l'honorable Dominic LeBlanc, [WIT0000103.FR](#), para 21.

¹²⁵ Résumé d'interrogatoire à huis clos : Service canadien du renseignement de sécurité, [WIT0000134](#), paras 25-28.†

¹²⁶ *Loi sur le Service canadien du renseignement de sécurité*, [LRC 1985](#), c C-23.

¹²⁷ Résumé d'entrevue: Service canadien du renseignement de sécurité, [WIT0000125.FR](#), para 46.

¹²⁸ Résumé d'entrevue: Service canadien du renseignement de sécurité, [WIT0000125.FR](#), para 46.

population canadienne face à l'IE et permettre des enquêtes et des poursuites relatives à l'IE, notamment par le biais de partages de renseignements avec les premiers ministres provinciaux et les organismes électoraux provinciaux qui ont le pouvoir d'enquêter¹²⁹.

b) CST – Renseignement électromagnétique étranger et outils de cyberdéfense

68. Le CST, en tant que responsable de la collecte de renseignement électromagnétique étranger du Canada, maximise tous les volets de son mandat pour détecter, prévenir et contrer les activités d'IE¹³⁰, incluant les cyberopérations étrangères. Dans le cadre de son mandat de cybersécurité et d'assurance de l'information, le CST fournit des avis, des conseils et des services afin d'aider à protéger l'information électronique et les infrastructures de l'information¹³¹.

69. Le CST est un chef de file mondial en cyberdéfense¹³². Le CST utilise une vaste gamme de capteurs pour défendre les systèmes du Canada et d'autres systèmes d'importance comme les infrastructures électorales provinciales et territoriales¹³³. Ces capteurs permettent la détection d'activités suspectes et de cyber incidents. Les défenses du CST bloquent en moyenne 6,6 milliards d'actes malveillants par jour contre les réseaux du gouvernement du Canada¹³⁴.

70. Lorsque le CST prend connaissance d'une cybermenace potentielle, le Centre canadien pour la cybersécurité coordonne ses actions avec les propriétaires des systèmes visés pour atténuer la menace. Ceci est illustré par la réponse du CST à la campagne de liens de pistage menée par APT-31 contre les comptes de courriels de parlementaires. Lorsque le CST a découvert cet acte malveillant originaire de la RPC qui ciblait les systèmes parlementaires, il a immédiatement bloqué le nom de domaine suspect et informé les responsables de la sécurité

¹²⁹ Résumé d'entrevue: Service canadien du renseignement de sécurité, [WIT0000125.FR](#), para 46.

¹³⁰ Centre de la sécurité des télécommunications, Rapport institutionnel Partie C, [CAN.DOC.000029](#), pp 3-4.

¹³¹ Opérations par courriel de la RPC contre les parlementaires, [CAN.SUM.000027](#), para 2†; Centre de la sécurité des télécommunications, Rapport institutionnel Partie C, [CAN.DOC.000029](#), p 4.

¹³² Centre de la sécurité des télécommunications Canada, Transcription de l'audience publique, [volume 23](#), p 34.

¹³³ Centre de la sécurité des télécommunications Canada, Transcription de l'audience publique, [volume 23](#), p 13.

¹³⁴ Centre de la sécurité des télécommunications Canada, Transcription de l'audience publique, [volume 23](#), p 34; Résumé d'entrevue: Centre de la sécurité des télécommunications (Caroline Xavier, Rajiv Gupta, Alia Tayyeb), [WIT0000122.FR](#), paras 17 et 20; Opérations par courriel de la RPC contre les parlementaires, [CAN.SUM.000027](#), para 5.

informatique de la Chambre des communes¹³⁵. Le CST a offert des séances d'information classifiées à propos de l'incident aux responsables de la sécurité informatique de la Chambre des communes et a fourni de nombreux rapports techniques qui contenaient des recommandations détaillées¹³⁶. Pour les cas où le courriel avec le lien de pistage aurait été ouvert avant l'application de mesures d'atténuation, la campagne n'aurait acquis que des renseignements techniques généraux à propos de la réception du lien de pistage et n'aurait pas obtenu de contenu des appareils. Cet incident a été atténué avec succès et la cybersécurité des parlementaires n'a pas été compromise¹³⁷.

c) *AMC – Outils diplomatiques*

71. Les réponses diplomatiques sont des outils importants; elles comprennent les communications formelles comme des démarches ou des notes diplomatiques, les communications publiques sur la position du Canada à propos de diverses questions, le refus de visas diplomatiques, la déclaration du personnel diplomatique *persona non grata* (PNG), et la fermeture de missions étrangères¹³⁸. De concert avec les agences qui ont un mandat national, AMC utilise ses outils diplomatiques pour répondre à l'IE de façon stratégique. Ceci comprend des échanges bilatéraux avec les pays qui se livrent à l'IE pour envoyer un message clair que l'IE est inacceptable pour le Canada¹³⁹.

i. Échanges bilatéraux

72. Lorsque des informations appuient l'utilisation d'outils diplomatiques, comme des informations fiables à propos de comportements inappropriés de la part de diplomates, AMC et

¹³⁵ Résumé d'interrogatoire à *huis clos* : Caroline Xavier, Alia Tayyeb, Sami Khoury, [WIT0000133](#), para 31†; Centre de la sécurité des télécommunications Canada, Transcription de l'audience publique, [volume 23](#), pp 36-49; Voir la chronologie des événements [CAN.SUM.000027.001](#) pour les mesures prises par le Centre pour la cybersécurité et le SCRS pour aviser et aider les fonctionnaires de la Chambre des communes.†

¹³⁶ Centre de la sécurité des télécommunications Canada, Transcription de l'audience publique, [volume 23](#), pp 105-106.

¹³⁷ Centre de la sécurité des télécommunications Canada, Transcription de l'audience publique, [volume 23](#), pp 37-38.

¹³⁸ Rapport institutionnel partie C, Affaires Mondiales Canada, [CAN.DOC.000031](#), p 2-3.

¹³⁹ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp 27-32.

la ministre des Affaires étrangères agissent¹⁴⁰. Un exemple se trouve dans les échanges avec la RPC à propos de l'IE, lesquels ont abouti à l'expulsion du diplomate chinois Zhao Wei¹⁴¹.

73. Le Canada a soulevé ses préoccupations face aux tentatives d'IE de la RPC à plusieurs reprises et à divers niveaux avant 2023¹⁴². À celles-ci s'ajoutent d'autres irritants à la relation bilatérale comme les postes de police étrangers, discutés ailleurs¹⁴³, et l'entrée des ballons-espions chinois dans l'espace aérien souverain canadien. Le Canada a fréquemment eu recours à des communications diplomatiques pour envoyer un message clair que l'IE est inacceptable et qu'il y aurait des conséquences si elle se poursuivait¹⁴⁴. Ceci comprenait un avertissement que le premier ministre a donné directement au président Xi en novembre 2022, de même que le refus d'octroyer des visas et de créer de nouveaux postes pour des diplomates de la RPC.

74. L'expulsion potentielle d'un diplomate de la RPC avait été envisagée en 2022 et 2023¹⁴⁵. La couverture médiatique identifiant le diplomate chinois Zhao Wei a offert une occasion supplémentaire à AMC pour envoyer un message ferme à la RPC et aux autres pays qui pouvaient considérer ou se livraient à de l'IE au Canada¹⁴⁶. Sept jours après le reportage médiatique, la ministre des Affaires étrangères a déclaré Zhao Wei PNG¹⁴⁷. En réponse, la RPC a expulsé une diplomate canadienne, ce qui avait été anticipé¹⁴⁸.

75. Tel qu'il se doit, le Canada utilise ses outils diplomatiques avec prudence, en fonction du contexte bilatéral et global¹⁴⁹. Les pays qui se livrent à l'IE le font dans le cadre d'une stratégie plus large et le Canada doit tenir compte de la situation dans son ensemble¹⁵⁰. L'État étranger peut tenter de provoquer une réaction ou créer une distraction par rapport à d'autres activités. Le recours à des outils plus sévères, comme la déclaration d'une personne PNG, comporte une

¹⁴⁰ Ministre Joly, Transcription de l'audience publique, [volume 32](#), pp [115-117](#); Résumé d'entrevue : l'honorable Mélanie Joly, [WIT0000148](#), para [7](#).

¹⁴¹ Déclaration de Zhao Wei *persona non grata*, [CAN.SUM.000016](#)†; Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [56-57](#).

¹⁴² Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [51-58](#).

¹⁴³ Postes de police de la République populaire de Chine, [CAN.SUM.000015](#).†

¹⁴⁴ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), p [31](#).

¹⁴⁵ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), p [50](#).

¹⁴⁶ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [49-52](#) et [56](#).

¹⁴⁷ Ministre Joly, Transcription de l'audience publique, [volume 32](#), pp [145-149](#).

¹⁴⁸ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), p [57](#).

¹⁴⁹ Résumé d'entrevue : l'honorable Mélanie Joly, [WIT0000148](#), para [8](#).

¹⁵⁰ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [11](#) et [33](#).

attente que l'autre pays va répondre, *au minimum*, en expulsant un diplomate canadien. Il peut aussi répondre de façon encore plus sévère, comme quand l'Inde a expulsé 41 diplomates canadiens après la déclaration du premier ministre à la Chambre des communes à propos du meurtre d'Hardeep Singh Nijjar¹⁵¹. L'expulsion de diplomates canadiens porte préjudice aux intérêts du Canada. Sans présence diplomatique, le Canada perd des porte-paroles qui défendent ses intérêts, des personnes sur le terrain qui le tiennent au courant de ce qui se passe dans l'autre pays, et des canaux de communication qu'il utilise notamment en réponse aux comportements inappropriés¹⁵².

76. Bien que l'expulsion de diplomates doive être faite de façon stratégique, le Canada le fera si la situation l'exige. Le Canada a récemment envoyé un message très fort à l'Inde que ses activités d'IÉ et de répression transnationale sont inacceptables en expulsant six diplomates et agents consulaires indiens¹⁵³.

ii. Échanges multilatéraux

77. La réponse d'AMC à l'IÉ ne se limite pas à agir contre des diplomates particuliers. Avoir des échanges avec des États impliqués dans l'IÉ peut démontrer que le Canada est au courant de cette IÉ et qu'il ne va pas la tolérer¹⁵⁴. De plus, le fait d'avoir des échanges avec la communauté internationale par l'entremise d'organismes multilatéraux peut mettre une plus grande lumière sur l'IÉ et contribuer au développement de normes internationales pour la contrer¹⁵⁵. Le Canada est un chef de file dans cette sphère, confrontant la menace de l'IÉ avec ses partenaires du G7, du G20, de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Association des nations de l'Asie du Sud-Est (ANASE), et dans ses échanges bilatéraux¹⁵⁶.

¹⁵¹ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp 59-62.

¹⁵² Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), p 20.

¹⁵³ Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 55-58.

¹⁵⁴ Voir Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp 67-68 pour un exemple.

¹⁵⁵ Voir Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp 47-48 pour la manière dont cela est fait par rapport à la Déclaration sur l'intégrité et l'information en ligne.

¹⁵⁶ Ministre Joly, Transcription de l'audience publique, [volume 32](#), p 103; Résumé d'entrevue: l'honorable Pascale St-Onge, [WIT000097.FR](#), para 16.

iii. MRR du Canada

78. Sous le leadership du Canada, les nations du G7 ont développé le MRR du G7 pour partager de l'information sur les menaces à la démocratie, avec une attention particulière portée à la désinformation¹⁵⁷. Le MRR du G7 tire parti des partenariats internationaux du Canada pour sensibiliser un auditoire plus large contre les menaces à la démocratie. Le Canada est le président permanent du MRR du G7 et coordonne le réseau plus large du MRR du G7¹⁵⁸. Dans le cadre de ce réseau, le MRR du Canada surveille l'information de source ouverte étrangère comme les médias sociaux afin d'identifier la désinformation et la manipulation d'information qui pourrait constituer une menace à la démocratie¹⁵⁹.

79. Un exemple du succès de cette initiative est que le MRR a pu détecter et contrer un incident de « Spamouflage » en 2023. Sur la base d'informations partagées par un partenaire du réseau du MRR du G7, le MRR du Canada a déterminé que la RPC tentait de discréditer un Canadien qui critiquait la RPC en créant du contenu sur les médias sociaux qui dénigrait les politiciens canadiens et était faussement attribué à cette personne. Le MRR du Canada, avec l'approbation du CSMRR, a contacté le Canadien visé, les plateformes de médias sociaux, de même que les politiciens qui étaient dénigrés par les faux contenus¹⁶⁰.

80. Bien que le MRR du Canada surveille l'écosystème d'information national pendant les élections, et plus récemment pendant les élections partielles dans le cadre du Groupe de travail, cette tâche détourne l'équipe de son mandat principal¹⁶¹. Le Canada reconnaît l'importance de surveiller l'écosystème d'information national en ligne de façon continue et non seulement lors

¹⁵⁷ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [34-35](#).

¹⁵⁸ Résumé d'entrevue : Affaires mondiales Canada (David Morrison, Alexandre Lévêque, Weldon Epp, Philippe Lafortune et Tara Denham), [WIT0000104.FR](#), paras [6-7](#); Résumé d'interrogatoire à *huis clos* : Affaires mondiales Canada (David Morrison, Cindy Termorshuizen, Alexandre Lévêque, Weldon Epp, Philippe Lafortune et Tara Denham), [WIT0000142](#), paras [29-32](#)†; Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [35-36](#).

¹⁵⁹ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), p [37](#).

¹⁶⁰ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [81-83](#).

¹⁶¹ Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, Transcription de l'audience publique, [volume 27](#), pp [171-172](#); Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [38-41](#).

d'élections. Des discussions sont en cours pour déterminer où cette expertise devrait résider dans la structure gouvernementale¹⁶².

d) *GRC – Outils d'application de la loi*

i. Interruption

81. La GRC met l'accent sur le volet de son mandat qui vise à assurer la sécurité publique et atténuer la menace, dans l'optique d'interrompre les activités reliées à l'IE et empêcher qu'elles se reproduisent¹⁶³. Cette approche est illustrée par la réponse de la GRC aux postes de police étrangers, décrite plus bas.

ii. Nouvelles infractions criminelles

82. Faisant écho aux activités d'IE observées et à la suite de consultations étendues auprès de diverses parties prenantes¹⁶⁴, C-70 a créé et mis à jour des infractions criminelles¹⁶⁵ permettant aux organismes d'application de la loi d'intervenir dans des activités d'IE criminelle potentielle plus tôt, et dans un plus grand éventail de circonstances¹⁶⁶. Ces modifications comprennent l'application extraterritoriale de certaines infractions¹⁶⁷ et la création d'une infraction interdisant toute conduite subreptice ou trompeuse en vue d'influencer un processus politique ou gouvernemental. Celle-ci s'appliquerait aux activités d'IE visant différents ordres de gouvernement et les élections scolaires, ainsi qu'aux activités d'IE dans les processus des partis politiques¹⁶⁸.

¹⁶² Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp 38-41; Résumé de l'interrogatoire à *huis clos* : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 55; Résumé d'interrogatoire à *huis clos* : l'honorable Dominic LeBlanc, [WIT0000162.FR](#), para 14; Ministre LeBlanc, Transcription de l'audience publique, [volume 34](#), pp 134-135.

¹⁶³ Résumé d'interrogatoire à *huis clos* : Michael Duheme, commissaire de la GRC, Mark Flynn, sous-commissaire de la Police fédérale, et Brigitte Gauvin, commissaire adjointe de la Police fédérale, Sécurité nationale, [WIT0000137](#), paras 48-49.†

¹⁶⁴ Il s'agissait notamment des gouvernements provinciaux, territoriaux et autochtones; de parties prenantes; de l'industrie; d'universitaires; et de communautés touchées.

¹⁶⁵ Voir par exemple l'article 20 de la *Loi sur l'ingérence étrangère et la protection de l'information*, [LRC 1985](#), ch O-5 ("LIEPI") et l'article 52 du *Code criminel*, [LRC 1985](#), ch C-46.

¹⁶⁶ Gendarmerie Royale du Canada, Transcription de l'audience publique, [volume 27](#), p 85.

¹⁶⁷ [LIEPI](#), article 20.1; Résumé d'entrevue: Gendarmerie royale du Canada (commissaire Michael Duheme et sous-commissaire, Police fédérale, Mark Flynn), [WIT0000108.FR](#), para 22.

¹⁶⁸ [LIEPI](#), article 20.4; Gendarmerie royale du Canada, Transcription de l'audience publique, [volume 27](#), p 85; Résumé d'entrevue: Gendarmerie royale du Canada (commissaire Michael Duheme et sous-commissaire, Police fédérale, Mark Flynn), [WIT0000108.FR](#), para 22.

e) Sécurité publique – Outils réglementaires

83. Le Canada met aussi en place un registre visant la transparence en matière d'influence étrangère, qui rendra accessible au public canadien plus de renseignements sur les activités d'influence menées pour le compte d'États étrangers. Toute personne ou entité qui conclut un arrangement d'influence étrangère devra fournir certains renseignements au commissaire à la transparence en matière d'influence étrangère. Le registre vise à dissuader les acteurs et États étrangers, ainsi que leurs intermédiaires, de prendre part à des activités qui constituent une ingérence dans les affaires du Canada¹⁶⁹.

5. La réponse du gouvernement aux menaces d'IE est coordonnée

84. Les partenaires fédéraux collaborent afin que la réponse aux activités d'IE incorpore les mandats et perspectives de toutes les agences. L'échange d'avis ainsi encouragé permet la prise de meilleures décisions visant à contrer la menace de l'IE, et ce de manière ni insuffisante ni excessive¹⁷⁰. Cette collaboration a lieu dans le contexte de comités du Cabinet, au niveau des sous-ministres, via le coordonnateur national de la lutte contre l'ingérence étrangère, et par le biais d'une dissémination efficace du renseignement.

a) Le Conseil de la sécurité nationale (CSN)

85. En 2023, le premier ministre a établi le CSN, un comité du Cabinet chargé de se pencher sur des questions de sécurité nationale. Le CSN a été créé afin de permettre une approche stratégique et pangouvernementale aux enjeux de sécurité nationale¹⁷¹. Il sert de forum à des discussions auxquelles contribuent de hauts fonctionnaires, et où les ministres peuvent délibérer sur le renseignement et donner des instructions sur l'orientation des politiques¹⁷². Cela constitue

¹⁶⁹ Breffage technique à huis clos sur le projet de loi C-70, *Loi concernant la lutte contre l'ingérence étrangère*: [Sébastien Aubertin-Giguère, sous-ministre adjoint, Secteur de la sécurité et de la cybersécurité nationale, Sécurité publique Canada, Nicole Giles, sous-ministre adjointe principale et sous-directrice des Politiques et des Partenariats stratégiques au SCRS, Greg Koster, directeur et avocat général, Section de la politique en matière de droit pénal au ministère de la Justice, Mark Scrivens, avocat-conseil, Section de la politique en matière de droit pénal au ministère de la Justice, et Sarah Estabrooks, directrice générale des politiques et des relations étrangères au SCRS] [WIT0000132.FR](#), paras 1 et 4.

¹⁷⁰ Bureau du Conseil privé, transcription de l'audience publique, [volume 31](#), pp 102-104.

¹⁷¹ Résumé d'entrevue : Le très honorable Justin Trudeau, [WIT0000106.FR](#), para 16; Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 25-26.

¹⁷² Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para 12.

un complément aux activités du Groupe d'intervention en cas d'incident, soit le comité du Cabinet chargé de répondre à des incidents spécifiques¹⁷³.

86. Le CSN mène la réponse du Canada à des enjeux stratégiques de sécurité nationale et revêt une valeur importante. Il représente un ajout essentiel à la gouvernance de la communauté de la sécurité nationale, créant un forum au niveau du Cabinet qui est dédié à la discussion d'enjeux de sécurité nationale¹⁷⁴. Le CSN offre aussi l'opportunité de faire usage du renseignement de manière plus délibérée dans le contexte de considérations politiques et opérationnelles. De plus, les discussions au CSN produisent des retombées, car elles mènent à des conversations qui rassemblent les différentes agences impliquées¹⁷⁵. Le cycle du CSN est fluide, permettant à la communauté de la sécurité nationale de soulever un enjeu, mettre en œuvre les instructions du CSN, et ensuite revenir au CSN avec une évaluation ou de nouveaux développements pour obtenir des instructions supplémentaires¹⁷⁶.

b) La coordination entre sous-ministres

87. Dans le cadre de ses efforts pour augmenter et renforcer la coordination, le Canada a révisé la structure de gouvernance par laquelle les hauts fonctionnaires de différents ministères examinent les enjeux, y compris l'IE, du point de vue des politiques publiques et du point de vue opérationnel. Parmi les forums clés, on retrouve : le CSMRR, où l'on discute de rapports de renseignement particulièrement sensibles et/ou qui nécessitent une réponse en temps opportun; le Comité des sous-ministres sur la sécurité nationale, qui considère les réponses de politique publique aux enjeux de sécurité nationale; et le Comité des sous-ministres sur la coordination opérationnelle, qui aborde les mesures opérationnelles liées au renseignement et à d'autres informations¹⁷⁷.

¹⁷³ Résumé de l'interrogatoire à *huis clos* : Sous-greffière du Conseil privé et conseillère à la sécurité nationale et au renseignement et Sous-conseiller à la sécurité nationale et au renseignement, [WIT0000152](#), para 44.†

¹⁷⁴ Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para 12.

¹⁷⁵ Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para 13; Résumé de l'interrogatoire à *huis clos* : John Hannaford et Nathalie G. Drouin, [WIT0000150](#), para 31.

¹⁷⁶ Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para 13.

¹⁷⁷ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 37-41; Partie C : Rapport Institutionnel du Bureau du Conseil privé, [CAN.DOC.000037](#), pp 29-30; Rapport institutionnel pour le Bureau du Conseil privé, [CAN.DOC.000012](#), p 17-18.

88. Le Comité de coordination de la sécurité des élections, qui comprend les hauts fonctionnaires d'Élections Canada et ceux de la fonction publique centrale, s'assure que l'infrastructure électorale essentielle du Canada soit protégée contre l'IE¹⁷⁸.

c) Le coordonnateur national de la lutte contre l'ingérence étrangère

89. Détecter, prévenir, et contrer l'IE dans les institutions démocratiques et ailleurs implique plusieurs ministères et agences tant à l'intérieur qu'à l'extérieur du gouvernement. Reconnaisant l'importance de ce travail, le Canada a nommé un coordonnateur national de la lutte contre l'ingérence étrangère. Celui-ci a pour rôle de coordonner l'approche du Canada à l'égard de l'IE du point de vue des politiques publiques et d'accroître la transparence de cette approche en menant une conversation publique avec la population canadienne dans son entièreté, y compris les groupes culturels, le milieu universitaire, les organisations non gouvernementales, et d'autres partenaires nationaux et internationaux¹⁷⁹. Le coordonnateur a été très impliqué dans les consultations portant sur le projet de loi C-70 et travaille présentement sur la mise en œuvre de celui-ci.

d) La dissémination du renseignement

90. Le Canada a mis en œuvre des processus pour s'assurer que le renseignement soit correctement reçu et compris à travers le gouvernement¹⁸⁰. Alors qu'auparavant certains produits de renseignement étaient partagés par courriel sécurisé, ils sont maintenant consignés dans une base de données sécurisée maintenue par le CST, ce qui permet un suivi simultané de qui a accédé à quels produits¹⁸¹. Le personnel de différents ministères et agences ayant les autorisations de sécurité nécessaires reçoit un accès direct à la base de données afin de pouvoir

¹⁷⁸ Partie C : Rapport Institutionnel du Bureau du Conseil privé, [CAN.DOC.000037](#), pp 28-29 et 32; Résumé de l'interrogatoire à huis clos : Allen Sutherland, secrétaire adjoint du Cabinet, Institutions démocratiques et appareil gouvernemental, [WIT0000123.FR](#), para 16.

¹⁷⁹ Rapport institutionnel de Sécurité publique Canada (partie C), [CAN.DOC.000041](#), p 1.

¹⁸⁰ Résumé d'entrevue : Centre de la sécurité des télécommunications (Caroline Xavier, Rajiv Gupta, Alia Tayyeb), [WIT0000122.FR](#), paras 34-41; Rapport institutionnel du Service canadien du renseignement de sécurité, [CAN.DOC.000018](#), pp 5-6; Service canadien du renseignement de sécurité, Transcription de l'audience publique, volume 24, p 46; Affaires mondiales Canada, Transcription de l'audience publique, volume 28, pp 54-55; Résumé de l'interrogatoire à huis clos : Sous-greffière du Conseil privé et conseillère à la sécurité nationale et au renseignement et Sous-conseiller à la sécurité nationale et au renseignement, [WIT0000152](#), paras 7-10.

¹⁸¹ Résumé d'interrogatoire à huis clos supplémentaire: Service Canadien du Renseignement de Sécurité, [WIT0000135](#), para 52†; Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para 16.

consulter le renseignement. De plus, des fonctionnaires qu'on appelle « agents des relations avec la clientèle » demeurent chargés de la dissémination du renseignement par le biais de produits de renseignement ou de breffages verbaux ciblés, ainsi que du suivi sur toute question que les destinataires pourraient avoir¹⁸².

91. Pour prendre l'exemple de Sécurité publique, le ministère a investi de manière importante dans le suivi du renseignement et un groupe est chargé de faire le triage et le suivi du renseignement envoyé aux hauts fonctionnaires¹⁸³. Un agent de liaison du SCRS est affecté à Sécurité publique pour faire parvenir des ensembles de produits de renseignement taillés sur mesure et provenant de collecteurs canadiens ainsi que de pays alliés¹⁸⁴. Cela assure un suivi précis de la dissémination du renseignement et la fourniture d'informations plus justes aux hauts fonctionnaires en temps opportun¹⁸⁵. L'amélioration du suivi de la dissémination du renseignement permet à Sécurité publique de déterminer ce qui a été envoyé à son ministre avec plus d'efficacité¹⁸⁶.

92. De plus, un processus plus rigoureux et centralisé encadre le renseignement envoyé au Cabinet du premier ministre et au premier ministre, afin de s'assurer que celui-ci reçoit ce dont il doit prendre connaissance. Ce processus est en train d'être peaufiné et amélioré¹⁸⁷.

93. Bien qu'il soit important d'assurer un suivi approprié de la dissémination du renseignement et d'informations, il ne faut pas confondre la réception d'éléments de

¹⁸² Résumé d'interrogatoire à *huis clos* supplémentaire: Service Canadien du Renseignement de Sécurité, [WIT0000135](#), para 53†; Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para 17.

¹⁸³ Résumé d'entrevue: Sécurité publique Canada (Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère), [WIT0000095.FR](#), para 6.

¹⁸⁴ Résumé d'entrevue: David Vigneault, Michelle Tessier, Cherie Henderson, [WIT000041](#), p 7†; Résumé d'interrogatoire à *huis clos* : Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère, [WIT0000144](#), para 9†; Rapport institutionnel de Sécurité publique Canada (partie C), [CAN.DOC.000041](#), p 23; Résumé d'entrevue : Sécurité publique Canada (Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère), [WIT0000095.FR](#), paras 12-13.

¹⁸⁵ Rapport institutionnel de Sécurité publique Canada (partie C), [CAN.DOC.000041](#), p 23.

¹⁸⁶ Résumé d'entrevue: Sécurité publique Canada (Shawn Tupper, Tricia Geddes, Sébastien Aubertin-Giguère), [WIT0000095.FR](#), para 15.

¹⁸⁷ Résumé de l'interrogatoire à *huis clos* : Cabinet du Premier Ministre, [WIT0000163](#), paras 5-6; Résumé d'entrevue : Le très honorable Justin Trudeau, [WIT0000106.FR](#), para 2; Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), paras 14-18; Cabinet du Premier Ministre, Transcription de l'audience publique, [volume 34](#), pp 7-9; Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 4-6.

renseignement individuels avec la connaissance et la compréhension du contexte plus large de la menace qui sont nécessaires pour prendre des mesures adéquates. Aucun décideur de haut rang ne devrait lire chaque produit de renseignement généré par la communauté de la sécurité nationale, soit environ 71 000 produits en 2023 seulement, et il ne devrait pas y avoir une telle attente non plus¹⁸⁸. Trier cet « océan de renseignement » en une quantité de matériel gérable requiert un important degré de jugement et de compréhension des besoins du destinataire¹⁸⁹. Il est compréhensible que le renseignement destiné aux rangs supérieurs ait une portée plus large, mais qu'il implique une plus faible quantité de produits de renseignement en tant que tels¹⁹⁰. Pour que le renseignement soit utile, il doit ajouter de la valeur aux considérations de politiques stratégiques ou tactiques, ou être exploitable¹⁹¹. En ce qui concerne le premier ministre, il s'attend raisonnablement à recevoir de l'information sur des enjeux qui ont un impact direct sur la population canadienne ou qui présentent une menace pour elle, des informations qui sont liées à des décisions de politique publique particulières que le gouvernement doit prendre, et des informations dont le premier ministre doit avoir connaissance avant d'interagir avec d'autres dirigeants¹⁹².

94. De même, ce ne sont pas tous les produits de renseignement et produits associés qui sont disséminés avec l'intention que les destinataires agissent en conséquence. L'objectif de certains produits est uniquement d'informer¹⁹³, comme l'illustre le cas d'une note de gestion des enjeux informant de hauts fonctionnaires de breffages préventifs à certains députés fédéraux¹⁹⁴. Bien que les personnes dont le nom figurait sur la liste de destinataires ne se souvenaient pas avoir vu ce produit spécifique, elles n'auraient rien fait même si elles l'avaient vu¹⁹⁵. Dans cette situation, le fait que des individus à qui le produit de renseignement était destiné ne se souvenaient pas

¹⁸⁸ Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para 18.

¹⁸⁹ Résumé de l'interrogatoire à *huis clos* : Sous-greffière du Conseil privé et conseillère à la sécurité nationale et au renseignement et Sous-conseiller à la sécurité nationale et au renseignement, [WIT0000152](#), para 15 et 17.

¹⁹⁰ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 30-31.

¹⁹¹ Résumé de l'interrogatoire à *huis clos* : John Hannaford et Nathalie G. Drouin, [WIT0000150](#), para 31.†

¹⁹² Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 6-7.

¹⁹³ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), p 45.

¹⁹⁴ Defensive briefings to two Members of Parliament regarding PRC foreign interference activity, [CAN018796](#).†

¹⁹⁵ Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), pp 14-19; Zita Astravas, Transcription de l'audience publique, [volume 31](#), pp 232-233; Ministre Blair, Transcription de l'audience publique, [volume 33](#), p 13.

d'avoir vu ce produit n'a eu aucun impact sur la capacité du Canada de détecter, prévenir, et contrer l'IE.

95. Tel que l'indique le témoignage de plusieurs hauts dirigeants du gouvernement, tant élus que fonctionnaires, ceux-ci reçoivent l'information dont ils ont besoin pour agir afin de détecter, prévenir, et contrer l'IE¹⁹⁶.

D. La réponse du Canada à des cas et allégations spécifiques

1. Les processus des partis politiques relèvent des partis politiques

96. Les processus politiques, y compris ceux des partis politiques, doivent être protégés contre l'IE. Les partis politiques sont des entités privées qui ont la responsabilité de prendre les décisions les concernant et d'en répondre, notamment les décisions portant sur qui peut représenter le parti au niveau local¹⁹⁷. Cette indépendance signifie qu'il incombe aux partis politiques de s'assurer que leurs processus sont robustes¹⁹⁸.

97. Le rôle que le gouvernement peut jouer pour aider les partis politiques à combattre ces vulnérabilités potentielles ne revient pas à poser une question binaire, à savoir celle de légiférer ou de s'en abstenir : il existe plusieurs avenues pour aider les partis politiques à renforcer leurs processus qui ne vont pas jusqu'à leur imposer de la législation, par exemple la transparence accrue et les séances d'information¹⁹⁹. De plus, il existe déjà des mesures visant des domaines qui présentent des vulnérabilités particulières, comme les contributions aux campagnes électorales²⁰⁰.

¹⁹⁶ Résumé d'entrevue : l'honorable Dominic LeBlanc, [WIT0000103.FR](#), para 36; Résumé de l'interrogatoire à huis clos : Marco Mendicino, [WIT0000147](#), para 24†; Ministre Blair, Transcription de l'audience publique, [volume 33](#), p 43; Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#).

¹⁹⁷ Élections Canada, Transcription de l'audience publique, [volume 21](#), pp 211-212.

¹⁹⁸ Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 76-77.

¹⁹⁹ Ministre LeBlanc, Transcription de l'audience publique, [volume 34](#), p 157.

²⁰⁰ Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), p 75.

2. Les débats au sein de la fonction publique relativement à l'IE constituent une force, non une faiblesse

98. L'existence de différentes perspectives, voire de débats, au sein de la fonction publique quant à savoir si certaines activités constituent de l'IE ne doit pas être vue comme un désaccord sur l'existence de l'IE, ni un défaut de répondre à celle-ci. Il existe une définition fonctionnelle de l'IE qui guide la fonction publique dans son approche d'évaluation des situations au cas par cas²⁰¹.

99. Depuis l'élection de 2016 aux États-Unis, il y a eu une évolution nécessaire et importante des points de vue à travers le gouvernement concernant ce qui constitue de l'IE et comment sa définition fonctionnelle pourrait s'appliquer à des circonstances particulières. Les acteurs étatiques hostiles changent constamment leurs tactiques. Les discussions et les débats sont nécessaires²⁰². En effet, la « pensée de groupe » est dangereuse dans le domaine de la sécurité nationale²⁰³. Puisque les acteurs de l'IE opèrent intentionnellement de manière à obscurcir leurs activités d'IE, il est normal que différentes organisations qui approchent l'IE à partir d'angles différents arrivent à des points de vue discordants et conçoivent la même situation de façons différentes²⁰⁴. Ce n'est pas seulement normal, mais c'est intentionnel. La mobilisation de différentes perspectives lors de l'évaluation d'informations est une caractéristique du système et est encouragée²⁰⁵. L'échange de diverses perspectives et connaissances au sein de la communauté de la sécurité nationale lors de discussions portant sur l'IE résulte en de meilleures décisions sur l'opportunité et la manière de répondre²⁰⁶.

3. Les postes de police étrangers

100. Lorsqu'une organisation non gouvernementale a publiquement révélé l'existence de centres – communément appelés « postes de police étrangers » – offrant des services pour le

²⁰¹ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), p 88; Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 124-125.

²⁰² Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp 91-92, 94-95.

²⁰³ Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para 60.

²⁰⁴ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), p 26.

²⁰⁵ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 102-103.

²⁰⁶ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), p 103.

compte du gouvernement de la RPC à travers le monde, y compris au Canada, le Canada a agi rapidement afin d'enquêter sur les postes et de combattre les activités illégales. Ces postes offraient des services à la communauté chinoise au Canada, mais semblent aussi avoir surveillé et recueilli du renseignement sur d'anciens résidents de la RPC vivant au Canada, et ce dans le cadre plus large de la campagne transnationale d'anti-corruption, de répression et de rapatriement de la RPC²⁰⁷.

101. En réponse, le Canada a pris une série de mesures diplomatiques, d'atténuation, et d'enquête²⁰⁸. AMC a indiqué de façon claire à l'ambassadeur de la RPC que de tels postes étaient inacceptables en droit international, car ils offraient des services gouvernementaux dans des lieux non accrédités en vertu des conventions de Vienne²⁰⁹. La GRC a immédiatement agi pour interrompre ces activités et a mené enquête pour assurer la fermeture des postes²¹⁰. Ceci a aussi signalé aux communautés ciblées que la GRC prenait la situation au sérieux²¹¹. La réponse du gouvernement du Canada aux postes de police a démontré, d'une part, un effort coordonné au sein du gouvernement et, d'autre part, la nécessité de travailler de manière étroite avec les communautés affectées afin d'assurer leur sécurité et leur résilience vis-à-vis de telles activités.

4. Le document sur le ciblage et le rapport spécial n'ont pas été fournis au premier ministre

102. Ce ne sont pas tous les produits de renseignement qui sont destinés au premier ministre²¹². Ainsi, le simple fait que certains produits de renseignement ne se sont pas rendus à lui ne devrait susciter aucune inquiétude. Certains produits de renseignement sont destinés à d'autres acteurs, et d'autres produits sont à un stade trop préliminaire²¹³.

²⁰⁷ Postes de police de la République populaire de Chine, [CAN.SUM.000015](#).†

²⁰⁸ Résumé d'interrogatoire à *huis clos* : Michael Duheme, commissaire de la GRC, Mark Flynn, sous-commissaire de la Police fédérale, et Brigitte Gauvin, commissaire adjointe de la Police fédérale, Sécurité nationale, [WIT0000137](#), paras [50-52](#).†

²⁰⁹ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp [65-67](#).

²¹⁰ Gendarmerie royale du Canada, Transcription de l'audience publique, [volume 27](#), pp [26-30](#).

²¹¹ Résumé d'interrogatoire à *huis clos* : Michael Duheme, commissaire de la GRC, Mark Flynn, sous-commissaire de la Police fédérale, et Brigitte Gauvin, commissaire adjointe de la Police fédérale, Sécurité nationale, [WIT0000137](#), para [50](#).†

²¹² Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para [30](#).

²¹³ Résumé d'entrevue: Bureau du Conseil privé (John Hannaford, Nathalie G. Drouin, Daniel Rogers, Janice Charette, Jody Thomas et Stephen de Boer), [WIT0000116.FR](#), para [29](#).

103. Les produits de renseignement auxquels on réfère maintenant comme « le document sur le ciblage » et « le rapport spécial » n'avaient pas besoin d'être vus par le premier ministre. Ils n'auraient rien changé à sa compréhension des enjeux non plus, car il avait pleine connaissance de la menace que pose l'IE de la RPC et des tactiques utilisées par les États hostiles, et il était pleinement impliqué dans l'élaboration de la réponse²¹⁴. Ni le CSNR ni les hauts fonctionnaires du BCP n'avaient l'intention de porter ces produits à l'attention du premier ministre²¹⁵.

104. Aucune activité visant à détecter, prévenir ou contrer l'IE n'a été mise à mal en raison du fait que le premier ministre n'a pas pris connaissance des deux produits de renseignement en question. Il existe des mécanismes pour s'assurer que le premier ministre soit mis au courant s'il y a du renseignement qu'il doit connaître : la CSNR joue un rôle essentiel à cet égard, mais le CSN et le Groupe d'intervention en cas d'incident constituent aussi des forums où l'on discute de renseignement clé en matière de sécurité nationale²¹⁶. De plus, le greffier du Conseil privé a un accès direct au premier ministre et l'a souvent conseillé sur des enjeux de sécurité nationale et de renseignement.

5. Mandats du SCRS et délai d'approbation de l'un d'entre eux

105. Avec respect, des allégations extrêmement graves d'obstruction politique ont été formulées au cours de l'audience, sans aucun fondement factuel. Il n'y a aucune preuve d'interférence politique ou de tout autre faute dans l'exercice d'une charge publique par quiconque ayant été impliqué dans l'approbation de la demande de mandat par le ministre de la Sécurité publique à l'époque. De plus, il n'y a aucune preuve, ou même une suggestion, d'un préjudice causé à l'enquête du SCRS en raison du passage du temps²¹⁷. Le temps nécessaire pour obtenir l'autorisation ministérielle de chaque mandat varie selon la nature du mandat, les

²¹⁴ Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 13-16.

²¹⁵ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 31 et 34.

²¹⁶ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 42-47; Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 26-32.

²¹⁷ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), p 76; Zita Astravas, Transcription de l'audience publique, [volume 31](#), p 225; Ministre Blair, Transcription de l'audience publique, [volume 33](#), pp 34-42; Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), pp 34-36.

pouvoirs qu'il sollicite, s'il s'agit d'un renouvellement et s'il y a une urgence opérationnelle liée aux circonstances générales²¹⁸.

106. Lorsque l'approbation d'une demande de mandat est urgente, il existe des processus pour s'assurer que le SCRS, Sécurité publique et le Cabinet du ministre sont tous au courant de la nécessité de la traiter sur une base accélérée. La relation directe entre le directeur du SCRS et le ministre de la Sécurité publique signifie que le SCRS peut porter un mandat particulier directement à l'attention du ministre au besoin²¹⁹.

107. Le directeur du SCRS et le sous-ministre de la Sécurité publique n'ont pas identifié d'urgence relative à la demande de mandat en question et n'ont pas exprimé de préoccupations quant au moment où l'autorisation du ministre a été obtenue²²⁰. La chef de cabinet a nié avoir retardé le mandat, que ce soit pour des raisons partisans ou autres. Elle a expliqué qu'il y avait de nombreuses autres questions nécessitant l'attention du ministre à ce moment, notamment les confinements et la vaccination durant la pandémie de COVID. D'autres exemples non classifiés comprennent les mises à jour de la liste des entités terroristes, les priorités en matière de renseignement et les discussions de politiques autour de 5G²²¹. De plus, les hauts fonctionnaires du SCRS n'ont pas perçu que la chef de cabinet du ministre avait intentionnellement retardé le mandat²²².

108. La demande de mandat en question a été approuvée par le ministre dès son examen, et le mandat a été accordé par la Cour fédérale²²³. L'explication fournie, à savoir que la chef de

²¹⁸ Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), pp 79-80 et 193-194.

²¹⁹ Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), pp 34, 47 et 81; Addendum au résumé d'interrogatoire à *huis clos* : M. David Vigneault, Mme. Michelle Tessier et Mme. Cherie Henderson, [WIT0000121.FR](#), para 9; Résumé d'interrogatoire à *huis clos* : [Rob Stewart, ancien sous-ministre de la Sécurité publique, Dominic Rochon, anciennement sous-ministre adjoint principal de la Sécurité publique, Secteur de la sécurité et de la cybersécurité nationale], [WIT0000153](#), para 46.†

²²⁰ Addendum au résumé d'interrogatoire à *huis clos* : M. Rob Stewart, [WIT0000154](#), paras 6 et 8 †; Résumé d'interrogatoire à *huis clos* : [Rob Stewart, ancien sous-ministre de la Sécurité publique, Dominic Rochon, anciennement sous-ministre adjoint principal de la Sécurité publique, Secteur de la sécurité et de la cybersécurité nationale], [WIT0000153](#), paras 30 et 46 †; Sécurité publique Canada, Transcription de l'audience publique, [volume 30](#), p 34; Addendum au résumé d'interrogatoire à *huis clos* : M. David Vigneault, Mme. Michelle Tessier et Mme. Cherie Henderson, [WIT0000121.FR](#), para 9.

²²¹ Zita Astravas, Transcription de l'audience publique, [volume 31](#), pp 222-226, 252, 275 et 279.

²²² Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), p 76.

²²³ Résumé d'interrogatoire à *huis clos* : Zita Astravas, [WIT0000158](#), para 51 †; National Security and Intelligence Committee of Parliamentarians, Annual Report 2020, [COM0000156](#) †; Ministre Blair, Transcription de l'audience publique, [volume 33](#), p 96.

cabinet n'a pas accordé la priorité à un mandat que le directeur du SCRS n'a pas signalé comme étant urgent, est entièrement raisonnable et conforme avec la preuve. Le Canada note que la Commission a été en mesure d'examiner cette question, parmi d'autres, plus en détail à *huis clos*. Chaque témoin qui a témoigné publiquement à propos du mandat a été incapable de répondre à certaines allégations en raison de confidentialité pour des motifs de sécurité nationale. Leur incapacité à discuter publiquement en détail de sujets classifiés n'est pas un fondement juste ou raisonnable de remettre en question leur conduite ou de spéculer quant à un abus de pouvoir, que ce soit à propos de ceci ou de tout autre sujet devant la Commission.

6. Le Mémoire au Cabinet sur les Activités hostiles parrainées par des acteurs étatiques (AHAÉ) et le projet de loi C-70

109. La preuve est claire que l'IE est complexe, qu'elle a une portée internationale et que les acteurs étatiques hostiles changent constamment leurs tactiques²²⁴. Le Canada est un pays qui accorde de l'importance à la primauté du droit et à la *Charte canadienne des droits et libertés*, tout en répondant aux menaces qui évoluent. Certains ont suggéré qu'il aurait fallu en faire davantage plus tôt, notamment faire progresser l'initiative AHAÉ et la présentation du projet de loi C-70. Le Canada n'est pas d'accord. Ces initiatives très importantes avaient besoin d'attention et de temps; certaines nécessitant des consultations approfondies. Lorsqu'il s'agit d'élaborer une réponse sociétale à un problème complexe, et lorsque les droits d'expression et les droits démocratiques des Canadiens sont en jeu, agir soigneusement n'équivaut pas à un manque de diligence.

E. Les Canadiens peuvent et doivent avoir confiance

1. Confiance dans les 43^e et 44^e élections générales

110. La Commission a eu un accès sans précédent à des informations et à des renseignements classifiés. À la lumière de cette information, la Commission peut et devrait conclure que les élections fédérales et les processus démocratiques du Canada sont solides. La preuve démontre que l'IE n'a pas influencé quel parti a formé le gouvernement en 2019 ou 2021²²⁵. Les élections

²²⁴ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), p [239](#).

²²⁵ [Rapport Initial](#), pp [167-168](#).

générales de 2019 et de 2021 ont été libres et équitables, et le résultat a été décidé par les Canadiens.

2. Confiance dans les processus démocratiques

111. Bien que l'IE dans les processus électoraux et les institutions démocratiques du Canada constitue une menace importante, le gouvernement est vigilant et continue de développer sa capacité à détecter, à prévenir et à contrer cette menace²²⁶. Il est important de ne pas sous-estimer ou exagérer la gravité de la menace²²⁷. Le Canada n'a pas été la cible d'une campagne nationale visant à miner nos processus électoraux ou nos institutions démocratiques, comme on l'a vu dans d'autres pays²²⁸.

a) Reportages médiatiques sur l'IE en fin 2022 et début 2023

112. Les reportages des médias sur l'IE à la fin de 2022 et au début de 2023, sur la base de fuites illégales, ont inutilement et erronément ébranlé la confiance des Canadiens dans l'intégrité de nos processus électoraux et de nos institutions démocratiques. La divulgation non autorisée de renseignements classifiés s'est avérée être un obstacle à une meilleure compréhension du public et à un discours constructif sur l'IE. Les fuites peuvent même avoir aidé les auteurs de menace étrangers à réaliser leurs objectifs d'ingérence étrangère. Cette divulgation était illégale, irresponsable et elle a mis en péril non seulement les sources et les méthodes de nos agences de sécurité nationale, mais aussi la confiance des Canadiens dans la capacité de leur gouvernement à répondre aux menaces dirigées contre le Canada. En effet, le Rapporteur spécial indépendant sur l'ingérence étrangère, qui a examiné les informations classifiées sous-jacentes (qui étaient disponibles à la Commission) a conclu que lorsque les renseignements rapportés dans les médias étaient considérés dans leur contexte, les questions étaient moins préoccupantes ou, dans certains cas, racontaient une histoire différente de ce qui avait été rapporté²²⁹.

²²⁶ *LIEPI*; Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), pp 79 et 216.

²²⁷ Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 189-190.

²²⁸ Affaires mondiales Canada, Transcription de l'audience publique, [volume 28](#), pp 221-222; Cas soupçonnés d'ingérence étrangère, CAN.SUM.000031 *Document n'est pas disponible sur le site web de la Commission; Bureau du Conseil privé, Transcription de l'audience publique, [volume 31](#), pp 195-198.

²²⁹ Responsables du renseignement de sécurité nationale, Transcription de l'audience publique, [volume 4](#), pp 81-82.

113. Lorsque des informations classifiées sélectives ou incomplètes entrent dans le domaine public sans contexte approprié, elles peuvent être interprétées de manière incorrecte²³⁰. Les agences de renseignement ne sont pas en mesure de commenter les renseignements divulgués, car cela pourrait révéler des informations classifiées²³¹. En conséquence, des allégations incorrectes et incomplètes circulent en public sans qu'il soit possible de les éclaircir ou de les corriger²³². Un environnement d'information responsable est la base de la démocratie, pour ceci et bien d'autres raisons.

114. En s'appuyant sur les conclusions exprimées dans son rapport initial, cette Commission a l'occasion de fournir au public un portrait plus clair de la nature et de l'étendue de la menace et de confirmer au public qu'ils peuvent et devraient avoir confiance dans les institutions démocratiques.

3. Confiance dans les parlementaires

115. Le Rapport spécial du CPSNR sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada (le Rapport spécial du CPSNR), déposé au Parlement le 3 juin 2024, a été interprété par certains comme signifiant que les parlementaires travaillent pour d'autres pays ou que certains sont des « traîtres ». Le CPSNR est un organisme parlementaire important qui contribue à la sécurité nationale et à la transparence²³³. La Commission a eu l'occasion d'examiner la version non caviardée du rapport spécial du CPSNR et d'examiner à la fois les renseignements sous-jacents et les témoins, ce qui lui permet de fournir son opinion indépendante des conclusions du CPSNR et de les mettre dans le contexte approprié.

116. Les témoins du SCRS ont déclaré qu'ils avaient des réserves à l'égard de certaines des conclusions factuelles du CPSNR. Ils estiment que le rapport spécial du CPSNR est généralement exact dans la description de la nature de la menace, mais ont indiqué que les évaluations ou le libellé étaient plus forts que ceux que le SCRS aurait choisis. Plus précisément, les témoins du SCRS ont déclaré qu'il y avait des divergences factuelles entre les renseignements

²³⁰ Responsables du renseignement de sécurité nationale, Transcription de l'audience publique, [volume 4](#), p 85.

²³¹ Responsables du renseignement de sécurité nationale, Transcription de l'audience publique, [volume 4](#), pp 77-78.

²³² Responsables du renseignement de sécurité nationale, Transcription de l'audience publique, [volume 4](#), p 78.

²³³ Le très honorable Justin Trudeau, Transcription de l'audience publique, [volume 35](#), pp 78-81.

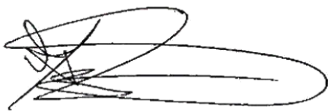
du SCRS et les conclusions du rapport spécial du CPSNR²³⁴, et que certains des renseignements sur lesquels s'appuyait le CPSNR contenaient des erreurs factuelles ou étaient considérés comme plus définitifs qu'ils ne l'étaient²³⁵.

117. La CSNR a noté que le rapport spécial du CPSNR avait perdu les nuances du renseignement en résumant les renseignements, ce qui est toujours un défi²³⁶. Elle n'a pas vu de preuve indiquant qu'un député se serait engagé dans des activités d'espionnage ou de sabotage ou de députés qui auraient mis la sécurité du Canada en péril.

F. Conclusion

118. Bien que l'ingérence étrangère soit à la fois présente et en évolution, les processus électoraux et les institutions démocratiques au Canada sont sûrs. La compréhension du Canada de l'IE et ses défenses à l'encontre de l'IE sont solides. Le Canada continue de raffiner ces défenses. Le gouvernement reconnaît la nécessité d'une vigilance sans faille et d'une détermination inébranlable.

119. Le Canada accueille favorablement les recommandations de la Commission visant à renforcer davantage ses défenses et remercie la Commission pour son examen minutieux de ces questions importantes et difficiles.



Gregory Tzemenakis
Avocat général principal
Avocat pour le Gouvernement du Canada



Barney Brucker
Avocat général principal par intérim
Avocat pour le Gouvernement du Canada

²³⁴ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), pp [117-118](#) et [127-128](#).

²³⁵ Service canadien du renseignement de sécurité, Transcription de l'audience publique, [volume 24](#), pp [119-121](#) et [123-127](#).

²³⁶ Résumé d'interrogatoire à *huis clos* : John Hannaford et Nathalie G. Drouin (Motion de la Chambre), WIT0000149, para 23. *Document n'est pas disponible sur le site web de la Commission.