Le Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport annuel 2025

Canada

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport annuel 2025

CP100F (Imprimé)
ISSN 2562-5128 (Imprimé)

CP100F-PDF (En ligne)
ISSN 2562-5136 (En ligne)

This publication is also available in English:
Annual Report 2025

C.P. 8015, Succursale T, Ottawa (Ontario) K1G 5A6
www.nsicop-cpsnr.ca

Rapport annuel 2025

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Message du Comité

C'est avec plaisir que nous présentons au premier ministre le huitième rapport annuel du Comité des parlementaires sur la sécurité nationale et le renseignement (le Comité). Le Comité a fait face à des changements importants dans la dernière année, en commençant par la dissolution de la 44e législature en mars 2025, qui a officiellement mis fin à la nomination de tous les membres du Comité. Le premier ministre Carney a nommé un nouveau Comité, qui est composé de quatre anciens membres et de sept nouveaux membres, ce qui représente le plus grand nombre de membres depuis la création du Comité.

En tant que Comité, nous reconnaissons le rôle important que nous jouons dans la réalisation, par des législateurs, d'examens indépendants et non partisans des activités de sécurité nationale et de renseignement dans l'ensemble du gouvernement fédéral. Ce mandat est particulièrement crucial dans le contexte de l'évolution des menaces envers la sécurité et la souveraineté du Canada. Le rôle du Comité est indispensable pour trouver un équilibre à l'égard de l'augmentation des ressources et des pouvoirs des organismes de la sécurité nationale et du renseignement qui en découle. Nous sommes impatients de poursuivre l'excellent travail accompli par les comités précédents dans le cadre de la réalisation de notre mandat.

Depuis la constitution du Comité, de nombreux exposés et comparutions détaillés lui ont été présentés par des organismes clés de l'appareil de la sécurité nationale et du renseignement. Les membres travaillent activement à reprendre et à conclure l'examen sur le rôle du conseiller à la sécurité nationale et au renseignement (CSNR) auprès du premier ministre entamé en avril 2024 par le Comité précédent. En novembre, le Comité a également annoncé un nouvel examen du cadre canadien de lutte contre le financement des activités terroristes, et se réjouit à l'idée de collaborer avec les ministres, ministères et organismes fédéraux concernés au cours de la prochaine année.

Malgré la prorogation, le Comité a présenté son Rapport annuel 2024 ainsi que la version classifiée du *Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement* au premier ministre en mars 2025. Des versions révisées des deux rapports ont été déposées au Parlement en septembre 2025. Le Comité est heureux d'avoir reçu une réponse officielle du gouvernement concernant le Rapport spécial, figurent à l'annexe A du Rapport annuel.

Le Comité tient à remercier les membres du Secrétariat pour leur dévouement et leur aide essentielle dans la réalisation du mandat du Comité. Le mandat d'examen du Comité permet d'améliorer la capacité de l'appareil de la sécurité et du renseignement de protéger les Canadiens et les Canadiennes, de respecter les principes démocratiques et de renforcer la responsabilisation et l'efficacité de l'appareil de la sécurité nationale et du renseignement du Canada. Nous sommes impatients de poursuivre ce travail inestimable au service de la population canadienne.

Le Comité des parlementaires sur la sécurité nationale et le renseignement

(Membres de la 45e législature)

L'honorable Darren Fisher, C.P., député, président

L'honorable Claude Carignan, C.P., sénateur

L'honorable Greg Fergus, C.P., député

Rhéal Fortin, député

Iqwinder Gaheer, député

L'honorable Marty Klyne, sénateur

Rob Morrison, député

L'honorable Rebecca Patterson, OMM, MSM, CD, sénatrice

L'honorable Ginette Petitpas Taylor, C.P., députée

Alex Ruff, député

Abdelhaq Sari, député

Table des matières

Introduction

1. Le Comité des parlementaires sur la sécurité nationale et le renseignement (le Comité ou CPSNR) est heureux de présenter son huitième rapport annuel au premier ministre. Le rapport fournit un aperçu des activités réalisées par le Comité au cours de la dernière année. Le rapport fournit également un résumé du *Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement.*

Les activités du Comité en 2025

2. Le Comité a connu de nombreux changements au cours de la dernière année, notamment la dissolution du Comité pour l'élection 2025, et la nomination subséquente d'un nouveau Comité.
3. Le Parlement a été prorogé du 6 janvier 2025 au 24 mars 2025. Malgré cela, le Comité précédent s'est réuni plusieurs fois durant la prorogation pour finaliser son rapport spécial sur l'accès légal et le Rapport annuel 2024.
4. Le Comité précédent a présenté le Rapport annuel 2024 et la version classifiée du *Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement* au premier ministre le 4 mars 2025. Les deux rapports ont ensuite été présentés au nouveau premier ministre après l'élection générale. Le 15 septembre 2025, le Rapport annuel 2024 et une version révisée du Rapport spécial du Comité ont été déposés au Parlement. Un résumé du Rapport spécial figure ci-dessous, de même que ses conclusions, ses recommandations et la réponse officielle du gouvernement présentées à l'Annexe A.
5. Le Comité actuel s'est réuni dix fois en 2025 et a assisté à de nombreux exposés et comparutions détaillés de la part d'organismes clés de l'appareil de la sécurité nationale et du renseignement. Le Comité a décidé de poursuivre l'examen sur le rôle du conseiller à la sécurité nationale et au renseignement (CSNR) auprès du premier ministre, reconnaissant le travail accompli par le Comité précédent et s'appuyant sur celui-ci.
6. Le 24 novembre 2025, le Comité a annoncé un examen du cadre canadien de lutte contre le financement des activités terroristes. Une lettre d'avis a été envoyée au premier ministre et aux ministres concernés. Les premières demandes d'information ont été envoyées aux ministères et organismes fédéraux concernés.

Examen de la Loi sur le CPSNR après cinq ans

7. Le Comité tient à souligner que l'examen après cinq ans de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* (Loi sur le CPSNR), adoptée en 2017, est toujours en retard.
8. Comme énoncé à l'article 34 de la Loi sur le CPSNR,

   > Cinq ans après la date de l'entrée en vigueur de la présente loi, un examen approfondi de ses dispositions et de son application est fait par un comité soit du Sénat, soit de la Chambre des communes, soit mixte, que le Parlement ou la chambre en question, selon le cas, désigne ou constitue à cette fin.

9. Un examen approfondi permettrait au Comité de formuler des recommandations précises sur la réforme et la modernisation de la Loi sur le CPSNR. Premièrement, des modifications à la Loi sur le CPSNR pourraient améliorer l'accès du Comité aux renseignements ainsi que sa capacité d'échanger des renseignements avec d'autres organismes d'examen. Deuxièmement, une réforme pourrait permettre d'améliorer l'indépendance et l'efficacité du Comité. Il est important pour le Comité que le gouvernement désigne le comité de la Chambre des communes ou du Sénat approprié pour faire l'examen de la Loi, qui est maintenant en retard de trois ans.

Exigences en matière de production de rapports pour 2025

Préjudice à la sécurité nationale et refus de communiquer un renseignement

10. La Loi sur le CPSNR comporte plusieurs exigences en matière de production de rapports. Le Comité doit inclure dans son rapport annuel le nombre de fois où, au cours de l'année précédente, un ministre compétent a empêché le Comité de réaliser un examen aux termes de l'alinéa 8(1)b) car il a déterminé que l'examen porterait atteinte à la sécurité nationale. Il doit aussi faire état du nombre de fois où un ministre compétent a décidé de refuser de communiquer un renseignement au Comité en vertu du paragraphe 16(1), parce qu'il était d'avis que le renseignement était un renseignement opérationnel spécial et que sa communication porterait atteinte à la sécurité nationale.

11. En 2025, aucun des examens proposés par le Comité n'a été considéré comme préjudiciable à la sécurité nationale par un ministre, et aucun ministre n'a refusé de fournir un renseignement demandé par le Comité pour ces raisons.

Examens portant préjudice à la sécurité nationale **0**

Refus de communiquer un renseignement **0**

Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères

12. Conformément à la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères,* douze organisations fédérales doivent présenter un rapport annuel à leur ministre concernant l'application de cette loi au cours de l'année civile précédente[1]. Les rapports annuels doivent faire état de ce qui suit :

- **a.** la communication de renseignements, à une entité étrangère, qui entraînerait un risque sérieux que de mauvais traitements soient infligés à un individu;
- **b.** la demande de renseignements, à une entité étrangère, qui entraînerait un risque sérieux que de mauvais traitements soient infligés à un individu;

[1] Les organisations fédérales devant présenter un rapport sont les suivantes : Agence des services frontaliers du Canada; Agence du revenu du Canada; Service canadien du renseignement de sécurité; Centre de la sécurité des télécommunications; Défense nationale et Forces armées canadiennes; Centre d'analyse des opérations et déclarations financières du Canada; Pêches et Océans Canada; Affaires mondiales Canada; Immigration, Réfugiés et Citoyenneté Canada; Sécurité publique Canada; Gendarmerie royale du Canada; Transports Canada.

c. l'utilisation de renseignements vraisemblablement obtenus par suite de mauvais traitements infligés à un individu par une entité étrangère.

13. La Loi oblige les ministres compétents à fournir une copie du rapport annuel de leur organisation sur les mauvais traitements au Comité et à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). Le Comité a reçu les douze rapports annuels.

Questions dont le Comité est saisi

14. Conformément à l'alinéa 8(1)c) de la Loi sur le CPSNR, tout ministre peut saisir le Comité de toute question relative à la sécurité nationale ou au renseignement aux fins d'examen. Le Comité n'a été saisi d'aucune question en 2025.

Autres rapports

15. La *Loi sur Investissement Canada* (LIC) prévoit l'examen des investissements importants au Canada effectués par des investisseurs non canadiens qui pourraient porter atteinte à la sécurité nationale. Le ministre de l'Industrie peut prendre un arrêté prolongeant l'examen d'un tel investissement si, après consultation du ministre de la Sécurité publique et de la Protection civile, il est d'avis que l'investissement pourrait porter atteinte à la sécurité nationale. Le ministre doit informer le Comité lorsqu'un examen donne lieu à la prise d'engagements par l'investisseur qui sont acceptés par le gouvernement, et de toute mesure prise par décret par le gouverneur en conseil en vertu de l'article 25.4 de la LIC.

16. Le ministre peut demander tout renseignement qu'il estime nécessaire à l'examen, et si l'investisseur non canadien soumet des engagements qui annulent l'atteinte à la sécurité nationale, l'examen est terminé, et on fait parvenir un avis à l'investisseur non canadien en vertu de l'alinéa 25.3(6)c) de la LIC. Ensuite, dans un délai de 30 jours, le ministre doit informer le Comité de l'identité de l'investisseur non canadien et de l'entreprise ou de l'entité qui a pris des engagements.

17. Le Comité a reçu quatre avis en vertu de l'alinéa 25.3(6)c) en 2025. Le Secrétariat du Comité conserve des exemplaires de tous les avis.

Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement

18. Le 15 septembre 2025, le premier ministre a déposé une version révisée du *Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement* devant les deux chambres du Parlement.

19. Le Rapport spécial portait sur l'examen du cadre pour l'interception licite de communications par les organismes de la sécurité et du renseignement. Le rapport décrit l'examen par le Comité du cadre législatif, réglementaire, stratégique et financier du Canada qui régit l'accès légal. Le rapport a été publié sur le site web du Comité le même jour, et il contient onze conclusions et sept recommandations.

20. L'accès légal consiste en l'interception autorisée de communications ainsi qu'en la collecte d'informations et de données utilisées par les organismes de renseignement et les services de police dans le cadre d'enquêtes. Les organismes de l'application de la loi, de la sécurité et du renseignement ont soutenu que la démonstration de l'accès légal (c.-à-d. un mandat judiciaire) ne peut garantir un accès aux données sur les communications, ce qui rend difficile l'accès à de l'information et à des éléments de preuve essentiels; ce qui, selon eux, a grandement limité leur capacité de réaliser des enquêtes.

21. Les difficultés liées à l'accès légal concernent les considérations en matière de sécurité et de protection des renseignements personnels des personnes relativement à leurs communications privées; le rôle et le pouvoir de l'État d'obliger des entreprises privées à fournir des données non chiffrées sur les communications d'un utilisateur en réponse à des demandes légales; et la nécessité de protéger les communications publiques et privées ainsi que les systèmes économiques contre les menaces numériques. Les groupes de libertés civiles, les défenseurs de la vie privée, les technologues et les entreprises privées ont soutenu qu'un chiffrement robuste est essentiel pour protéger les renseignements personnels et organisationnels, ainsi que les données publiques.

22. L'examen portait sur le cadre juridique de l'accès légal au Canada, notamment sur les lois pertinentes, comme la *Charte canadienne des droits et libertés,* le *Code criminel,* la *Loi sur le service canadien du renseignement de sécurité* et la *Loi sur le Centre de la sécurité des télécommunications,* ainsi que la *Loi sur la preuve au Canada* et la *Loi sur la protection des renseignements personnels.*

23. Le Comité s'est penché sur les difficultés entourant l'accès l'égal auxquelles les organismes de la sécurité et du renseignement font face dans le cadre d'enquêtes. Le Comité a également étudié l'efficacité du gouvernement pour répondre à ces difficultés et les atténuer, ainsi que la façon dont il assure un équilibre entre la nécessité de soutenir les efforts liés à la sécurité nationale et la protection du droit à la vie privée des Canadiens et Canadiennes. Dans le cadre de son évaluation, le Comité s'est fondé sur ses propres observations à cet égard.

24. Le Comité a recueilli les commentaires d'un vaste éventail de témoins, y compris des ministres, des représentants gouvernementaux, des groupes de la société civile, des experts en protection des renseignements personnels et des fournisseurs de services de communication (FSC). L'examen visait la période allant du 1er janvier 2012 au 9 janvier 2025 et concernait les organismes fédéraux suivants : le Service canadien du renseignement de sécurité (SCRS), le Centre de la sécurité des télécommunications, le ministère de la Justice, le ministère de la Sécurité publique et de la Protection civile (Sécurité publique Canada) et la Gendarmerie royale du Canada (GRC).

25. Le Comité a constaté que le SCRS et la GRC éprouvent des difficultés à accéder au contenu de communications numériques en raison de l'évolution rapide et de la prolifération des technologies de communication, de la nature internationale des communications et du cadre juridique désuet du Canada. Le Canada ne dispose pas de loi obligeant les FSC à s'assurer que leurs systèmes puissent intercepter des communications, et cette lacune entraîne des retards dans les enquêtes et des inefficacités financières pour le SCRS et la GRC.

26. Le Comité a appris que la GRC fait face à des difficultés supplémentaires pour trouver l'équilibre entre le recours à des techniques d'enquête sensibles et l'obligation légale de les divulguer devant les tribunaux. Par conséquent, la GRC évite souvent d'utiliser ces outils ou risque de ne pas pouvoir s'appuyer sur les éléments de preuve obtenus dans le cadre de poursuites; ce qu'on appelle le dilemme entourant le renseignement et la preuve.

27. Le Comité a conclu qu'il faut résoudre les difficultés liées à l'accès légal, sans quoi elles porteront atteinte à la sécurité nationale du Canada à long terme en entravant la capacité du SCRS et de la GRC à remplir leurs mandats respectifs. Si le Canada ne parvient pas à surmonter ces difficultés, celles-ci pourraient également nuire à sa capacité de contribuer efficacement à l'échange de renseignements et aux réponses conjointes aux menaces avec les partenaires du Groupe des cinq (Canada, États-Unis, Royaume-Uni, Australie et Nouvelle-Zélande).

Annexe A: Conclusions et recommandations du Rapport spécial sur l'accès légal aux communications par les organismes de sécurité et de renseignement

Conclusions

C1. Les organismes de sécurité et de renseignement du Canada ne consignent pas systématiquement la fréquence à laquelle ils font face à des difficultés technologiques dans le cadre d'enquêtes sur la sécurité nationale, et s'ils ont pu pallier ces difficultés.

C2. La GRC et le SCRS ont de la difficulté à accéder au contenu de communications, que les métadonnées ne peuvent pas nécessairement remplacer.

C3. Lors des comparutions, il y avait consensus qu'une loi obligeant la création d'un accès exceptionnel ou de portes dérobées sur les plateformes de chiffrement n'était ni nécessaire, ni souhaitée.

C4. La position publique du Canada concernant l'accès légal aux communications chiffrées n'est pas claire. Les praticiens de la sécurité nationale, les experts en cybersécurité et les défenseurs de la vie privée n'ont pas une compréhension commune du problème.

C5. L'inaction du gouvernement quant à l'élaboration et à la mise en œuvre d'une solution pour donner suite à la décision de la Cour suprême dans l'affaire *Spencer* nuit à la capacité du SCRS et de la GRC de répondre aux menaces envers la sécurité nationale.

C6. Sans une exigence légale générale obligeant les FSC à conserver des métadonnées pendant une période précise, les données demandées en vertu d'un mandat pourraient ne pas être disponibles.

C7. L'incapacité du gouvernement de faire progresser le dilemme entourant le renseignement et la preuve, surtout en ce qui concerne la protection des techniques d'enquête, a contribué à mettre la GRC dans une situation où elle doit choisir entre ne pas pouvoir utiliser d'outils et de techniques sensibles dans le cadre d'une enquête en raison des possibles enjeux de divulgation, ou risquer de ne pas pouvoir s'appuyer sur des éléments de preuve obtenus par le biais de ces outils et techniques devant les tribunaux, ou qu'une poursuite soit suspendue en raison d'une ordonnance de divulgation.

C8. Le gouvernement ne dispose pas de politiques officielles sur l'achat, la réglementation et l'utilisation d'outils d'enquête sur appareil commerciaux, ainsi que sur la production de rapports transparents concernant leur utilisation par les organismes d'application de la loi et le SCRS.

C9. L'absence de législation imposant aux fournisseurs de services de communication (FSC) de maintenir une capacité d'interception légale entraîne des risques inutiles pour tous les intervenants, y compris le SCRS, les organismes d'application de la loi fédéraux, provinciaux, territoriaux et municipaux, les FSC et, au bout du compte, la population canadienne. Elle fait également obstacle à la capacité du Canada de collaborer avec ses partenaires internationaux. Le fait de ne pas régler cette question sur le plan stratégique a poussé les organisations opérationnelles à élaborer elles mêmes des politiques et des procédures fondamentales, notamment un modèle d'indemnisation, visant à assurer une coopération continue de la part des FSC, à défaut d'une approche fondée sur des principes et orientée par les commentaires des ministres et du Parlement.

C10. Les risques associés à l'absence d'une législation obligeant les fournisseurs de services de communication à maintenir une capacité d'interception sont accentués par l'absence d'une autorité nationale centralisée qui coordonne, élabore et maintient les capacités d'interception légale au Canada.

C11. L'accord sur l'accès aux données entre le Canada et les États-Unis permettrait de surmonter des obstacles de longue date sur le plan des compétences qui empêchent l'accès judiciairement autorisé aux fournisseurs de services de communication des États-Unis, y compris les grandes plateformes de médias sociaux, et ce, sans compromettre le droit à la vie privée ou le chiffrement.

Recommandations

R1. Sous la direction du ministre de la Sécurité publique, le gouvernement élabore et met en œuvre une stratégie exhaustive visant à remédier aux défis d'accès légal du Canada, en s'appuyant sur l'examen et les conclusions du Comité. La stratégie devrait :

- établir les principes clés, comme la légitimité, la nécessité et la proportionnalité;
- cerner et consigner les principaux défis d'accès légal et les risques connexes et en rendre compte;
- comprendre des communications, la mobilisation des intervenants et des engagements en matière de transparence;
- prendre en compte les défis que peuvent poser les technologies émergentes, par exemple l'intelligence artificielle.

R2. Le gouvernement précise publiquement sa position concernant l'accès exceptionnel à l'information sur les communications protégée par chiffrement.

R3. Le gouvernement présente un projet de loi visant à établir de nouveaux pouvoirs dans la *Loi sur le Service canadien du renseignement de sécurité* et le *Code criminel* permettant la communication de renseignements de base sur les abonnés, et le gouvernement examine un projet de loi concernant la conservation des données.

R4. Pour donner suite à la recommandation du Comité en 2024 dans son *Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada,* à savoir que le gouvernement s'emploie à résoudre les difficultés liées au renseignement et à la preuve, le gouvernement élabore et met en œuvre une solution

visant à répondre aux préoccupations concernant la protection des outils d'enquête, ce qui pourrait nécessiter la modification des dispositions pertinentes de la *Loi sur la preuve au Canada.*

R5. Le gouvernement élabore des politiques et des lignes directrices concernant l'achat et l'utilisation d'outils d'enquête sur appareil commerciaux, ainsi que sur les exigences en matière de production de rapports à cet égard.

R6. Le gouvernement dépose une loi obligeant les fournisseurs de services de communication (FSC) à maintenir une capacité d'interception. La législation doit être neutre sur le plan du chiffrement et ne doit pas comporter d'exigence de déchiffrement. Le gouvernement doit également établir un modèle d'indemnisation pour les coûts liés au respect de la loi, c'est-à-dire qu'il doit déterminer si les FSC doivent être indemnisés pour les coûts d'élaboration, de maintenance et de fonctionnement liés à l'accès légal. La législation doit :

- mettre en place et désigner l'autorité nationale (c'est-à-dire le Centre national pour l'accès légal) pour la coordination des initiatives d'interception légale;
- définir le terme « fournisseur de services de communication » pour s'assurer d'inclure tout fournisseur de services qui mène des activités au Canada et qui offre des services ou des capacités de communication électronique;
- définir la capacité d'interception de façon à inclure un soutien à l'exploitation de réseau informatique;
- établir des normes techniques obligatoires, notamment en ce qui a trait à la cybersécurité.

R7. Le gouvernement priorise la signature et la mise en œuvre de l'accord sur l'accès aux données entre le Canada et les États-Unis.

État

Le gouvernement a fourni une réponse officielle à toutes les recommandations du Rapport annuel de 2025. Le gouvernement a accepté la plupart des recommandations et accepté en partie les R5 et R6.

Réponse à R1

Le gouvernement reconnaît la complexité croissante des menaces criminelles et de sécurité nationale et approuve la recommandation. Une stratégie globale visant à résoudre les problèmes d'accès légal garantirait que les organismes d'application de la loi et le Service canadien du renseignement de sécurité (SCRS) disposent des outils nécessaires pour accéder légalement aux renseignements électroniques dans le cadre de leurs enquêtes sur ces menaces, tout en respectant la vie privée, les droits et les libertés des Canadiens.

Dans un premier temps, le gouvernement a présenté la *Loi visant une sécurité rigoureuse à la frontière* (le projet de loi) le 3 juin 2025.

La partie 14 du projet de loi, intitulée *Accès aux données et aux renseignements en temps opportun,* propose de modifier le *Code criminel* pour traiter de questions nationales, notamment l'obtention rapide de réponses aux demandes légitimes de renseignements sur les abonnés présentées par les organismes d'application de la loi. Des modifications

parallèles à la Loi sur le SCRS permettront de disposer de pouvoirs correspondants en matière de sécurité nationale. La partie 14 mettrait à jour les outils existants pour faciliter l'accès aux données et aux renseignements qui sont particulièrement importants au cours des premières étapes des enquêtes criminelles et de sécurité nationale. La partie 14 modifierait également la *Loi sur l'entraide juridique en matière criminelle* afin de fournir un outil supplémentaire de coopération internationale aux partenaires canadiens et étrangers pour la production de renseignements sur les abonnés ou de données de transmission.

La partie 15 du projet de loi, à savoir la *Loi sur le soutien en matière d'accès autorisé à de l'information,* obligerait certains fournisseurs de services électroniques (FSE) à concevoir et à maintenir des capacités visant à aider les organismes d'application de la loi et le SCRS en ayant des systèmes qui permettent d'exécuter les autorisations légales d'accès à l'information.

Le ministre de la Sécurité publique, en collaboration avec les partenaires et les intervenants, étudiera la meilleure façon d'aborder les autres éléments de la recommandation qui ne sont pas couverts par les parties 14 et 15 du projet de loi, y compris le suivi, la transparence des rapports et les nouvelles technologies.

Réponse à R2

Le gouvernement est d'accord avec la recommandation selon laquelle il doit préciser publiquement sa position concernant l'accès exceptionnel à l'information sur les communications protégée par chiffrement. Le gouvernement reconnaît que le chiffrement est important afin de veiller à la cybersécurité et à la sécurité économique et de protéger la vie privée, mais qu'il pose également des problèmes importants dans le cadre des enquêtes criminelles et des enquêtes de renseignement.

La cybersécurité et les préoccupations relatives à la vie privée sont au cœur de l'accès légal, et le gouvernement reconnaît que la création de « portes dérobées » pourrait affaiblir la cybersécurité, augmentant ainsi le risque que des auteurs de menaces tirent parti de ces « portes dérobées » pour accéder à des données et compromettre la vie privée des Canadiens. Ainsi, le gouvernement ne soutient pas la mise en œuvre de mesures qui pourraient créer des vulnérabilités dans les protections électroniques (p. ex. le chiffrement et l'authentification).

La *Loi sur le soutien en matière d'accès autorisé à de l'information,* à savoir la partie 15 de la *Loi visant une sécurité rigoureuse à la frontière,* inclut des dispositions explicites visant à garantir que les FSE ne seront pas obligés de mettre en œuvre des exigences réglementaires ou des arrêtés ministériels qui introduiraient des vulnérabilités systémiques (p. ex. des « portes dérobées ») dans les protections électroniques ou qui empêcheraient un fournisseur de remédier à une telle vulnérabilité.

Réponse à R3

Le gouvernement approuve la recommandation de déposer un projet de loi créant de nouvelles dispositions dans la Loi sur le SCRS et le *Code criminel* pour permettre la production de renseignements sur les abonnés.

Pour combler cette lacune, la partie 14 de la *Loi visant une sécurité rigoureuse à la frontière* propose des modifications à la Loi sur le SCRS et au *Code criminel* afin de garantir que le SCRS et les organismes d'application de la loi disposent des pouvoirs nécessaires et appropriés pour obtenir des renseignements et des données sur les abonnés en temps opportun.

Le gouvernement approuve également la recommandation d'envisager la création d'une loi sur la conservation des données. En consultation avec les partenaires et les intervenants, le gouvernement étudiera la question, en tenant compte de divers facteurs, comme les implications en matière de protection de la vie privée et de cybersécurité, afin de déterminer la meilleure approche à adopter.

Réponse à R4

Les Canadiens attendent de leur gouvernement qu'il garantisse la sécurité publique, qu'il applique efficacement les lois et qu'il garantisse des procès équitables aux personnes accusées. Le gouvernement reconnaît que la divulgation de données de nature délicate sur les outils et techniques d'enquête a une incidence sur la capacité des services de police et de sécurité nationale à les utiliser dans d'autres enquêtes. Le gouvernement reconnaît également l'importance de trouver un équilibre entre le droit à un procès équitable et la nécessité de protéger les techniques d'enquête classifiées. Le gouvernement s'efforcera d'actualiser l'approche du cadre législatif actuel afin de pouvoir s'adapter à l'évolution rapide du paysage numérique.

Il convient également de noter que la *Loi canadienne sur la preuve,* récemment modifiée dans le cadre du projet de loi C-70, prévoit la création d'instances sécurisées de contrôle des décisions administratives devant la Cour fédérale. Ces instances sécurisées améliorent et normalisent les procédures et protections juridiques concernant les renseignements de nature délicate lorsqu'ils sont utilisés dans des décisions administratives soumises à un contrôle judiciaire. Il s'agit d'un premier pas vers un système de justice mieux équipé pour prendre en compte les preuves classifiées.

Réponse à R5

Le gouvernement reconnaît l'importance des outils d'enquête sur appareil (OEA) utilisés par les organismes d'application de la loi et le SCRS à l'appui des enquêtes.

Le gouvernement n'est pas tout à fait d'accord avec cette recommandation, car le SCRS et la GRC ont déjà mis en place des mesures de protection pour réglementer l'utilisation, l'acquisition et l'établissement de rapports sur ces types d'outils, y compris une autorisation judiciaire et des structures de gouvernance interne claires.

Par exemple, le SCRS obtient de la Cour fédérale des mandats autorisant le déploiement des OEA, ce qui garantit le contrôle judiciaire de leur utilisation autorisée. Le SCRS a également créé le Comité d'examen de la technologie opérationnelle (CETO) en 2020. Le CETO a pour mandat d'examiner les nouvelles technologies et les utilisations inédites des technologies existantes qu'il est proposé de déployer dans le cadre du mandat de collecte du SCRS. Toute proposition visant à acquérir ou à utiliser de nouvelles technologies en rapport avec les OEA relève du mandat du CETO. Le CETO comprend des représentants des intervenants concernés, afin de s'assurer que les risques sont évalués de manière approfondie lors de l'examen de ces technologies.

Dans le cas de la GRC, un juge de la Cour supérieure doit approuver et délivrer une autorisation, étayée par un mémoire technique décrivant les techniques proposées. Des conditions limitant la collecte des communications sont souvent imposées dans le cadre de l'autorisation. La GRC a créé le Programme national d'intégration de la technologie (PNIT) en 2021 afin de mettre en place un système centralisé permettant de déterminer, d'évaluer et de suivre les outils et technologies d'enquête nouveaux et émergents utilisés par la GRC, afin d'assurer une plus grande transparence.

En outre, en partenariat avec Affaires mondiales Canada, la GRC étudie la participation du Canada au processus Pall Mall, une initiative internationale menée par le Royaume-Uni et la France, qui invite les gouvernements, le secteur privé et la société civile à établir des lignes directrices et des principes pour relever les défis posés par la prolifération potentielle et l'utilisation irresponsable des capacités commerciales de cyberintrusion. Depuis 2020, la GRC fournit un rapport annuel au ministre de la Sécurité publique sur son utilisation de la surveillance électronique, qui comprend des statistiques. En outre, la GRC a fourni au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) de la Chambre des communes des statistiques sur son utilisation des OEA, qui peuvent être consultées à l'adresse suivante :

https://www.ourcommons.ca/content/Committee/441/ETHI/WebDoc/WD11922842/11922842/RoyalCanadianMountedPolice-DeploymentStats-f.pdf.

En novembre 2022, l'ETHI a publié le rapport « Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés », qui est accessible à l'adresse suivante :

https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-f.pdf.

Bien que des stratégies et des mesures d'atténuation aient été mises en place au sein du SCRS et de la GRC, le gouvernement reconnaît la nécessité d'une cohérence entre les différents organismes. Sécurité publique Canada, en collaboration avec le SCRS, le CST, le ministère de la Justice et la GRC, procédera à une évaluation des politiques et lignes directrices organisationnelles existantes afin de déceler les lacunes et de déterminer la meilleure façon de mettre en œuvre la recommandation.

Réponse à R6

Le gouvernement reconnaît que le cadre actuel n'a pas suivi l'évolution de la communication et de la technologie numériques. Les réseaux de communication sont devenus plus complexes en raison de l'essor des communications mobiles et Internet, des plateformes de messagerie, des revendeurs de services, des services d'hébergement en nuage et des nouvelles technologies de réseau. Par conséquent, les fournisseurs de services ne sont pas toujours en mesure de donner suite aux demandes de renseignements et d'interception légalement autorisées.

Le gouvernement est d'accord avec la recommandation et a déposé la *Loi sur le soutien en matière d'accès autorisé à de l'information,* à savoir la partie 15 de la *Loi visant une sécurité rigoureuse à la frontière,* pour obliger certains FSE à concevoir et à maintenir des capacités visant à soutenir les organismes d'application de la loi et le SCRS en ayant des systèmes qui permettent d'exécuter les autorisations légales d'accès à l'information. La *Loi sur le soutien en matière d'accès autorisé à de l'information* comprend des dispositions explicites

visant à garantir que les FSE ne seront pas obligés de mettre en œuvre des exigences réglementaires ou des arrêtés ministériels qui introduiraient des vulnérabilités systémiques dans les protections électroniques (p. ex. chiffrement et authentification), ou à empêcher un fournisseur de remédier à une telle vulnérabilité. Les obligations spécifiques pour les FSE sélectionnés seront définies dans le Règlement.

Bien que le gouvernement reconnaisse la valeur d'une autorité nationale centralisée pour la coordination de l'accès légal, il n'est pas d'accord avec la nécessité de l'établir dans la loi. Il est possible de créer un centre national d'accès légal sans prescrire l'organisation dans la loi.

Réponse à R7

Le gouvernement du Canada poursuivra les discussions avec les États-Unis sur l'accord sur l'accès aux données entre le Canada et les États Unis. En outre, la partie 14 de la Loi visant une sécurité rigoureuse à la frontière comprend des modifications au *Code criminel* et à la *Loi sur l'entraide juridique en matière criminelle* ajoutant des outils d'enquête permettant aux responsables canadiens et étrangers chargés de l'application de la loi d'obtenir des renseignements sur les abonnés transfrontaliers et des données de transmission par des moyens plus efficaces.

Annexe B: Recommandations en suspens des examens antérieurs

Rapport spécial sur les activités d'Affaires mondiales Canada en matière de sécurité nationale et de renseignement

Description

Le rapport donne un aperçu de la nature et de la portée des activités d'Affaires mondiales Canada liées à la sécurité nationale et au renseignement. Il examine les pouvoirs en vertu desquels le Ministère mène ces activités et la façon dont il les gère pour appuyer la responsabilité du ministre des Affaires étrangères. Il décrit les structures mises en place par le Ministère pour s'assurer que les activités et les politiques d'autres organisations ayant des responsabilités en matière de sécurité et de renseignement sont conformes aux objectifs canadiens en matière de politique étrangère. Enfin, le rapport souligne les domaines dans lesquels le Ministère joue un rôle prépondérant au sein du gouvernement, y compris deux études de cas récentes sur des prises d'otages par des terroristes à l'étranger.

Recommandations

R4. Le gouvernement du Canada établit un cadre clair pour répondre aux prises d'otages par des terroristes, y compris établir des principes pour guider l'intervention du gouvernement, définir les déclencheurs relatifs à l'orientation et à la participation ministérielles, mettre sur pied l'équipe de direction de l'intervention de l'ensemble du gouvernement aux incidents précis et fournir suffisamment de ressources pour répondre aux exigences opérationnelles pendant les incidents critiques.

État

Pour le Rapport annuel 2024, le gouvernement a fourni une réponse et fait le point sur l'état d'avancement de la mise en œuvre de certaines recommandations, mais n'a pas fourni de réponse officielle à la R4 concernant un cadre pour répondre aux prises d'otages par des terroristes. Le gouvernement a ensuite fourni une réponse officielle à toutes les recommandations du Rapport annuel de 2025.

Réponse à R4

Un cadre régissant l'intervention du gouvernement du Canada lors de prises d'otages par des entités terroristes a été élaboré en consultation avec les huit ministères et organismes qui forment le Groupe de travail interministériel (GTI) sur les incidents critiques internationaux. AMC vise à institutionnaliser le cadre par l'entremise d'accords de coopération et de protocoles d'entente entre les ministères membres du GTI. AMC a également progressé en ce qui a trait à la professionnalisation de la prestation de ces services spécialisés, en offrant une formation à plus de 160 fonctionnaires du gouvernement du Canada depuis l'examen de cette activité par le CPSNR.

La diversité et l'inclusion dans l'appareil de la sécurité et du renseignement

Description

Le Comité a examiné la représentation des femmes, des Autochtones, des personnes qui font partie des minorités visibles et des personnes handicapées dans l'appareil de la sécurité et du renseignement et a offert une évaluation de base. L'examen portait sur les objectifs, les initiatives, les programmes et les mesures mis en place par les ministères et organismes pour promouvoir la diversité et l'inclusion.

Recommandations

R4. L'appareil de la sécurité et du renseignement élabore un cadre commun de mesure du rendement et il accentue la responsabilisation à l'égard de la diversité et de l'inclusion en établissant des indicateurs de rendement significatifs et mesurables pour les directeurs et les gestionnaires dans l'ensemble des organisations.

État

Pour le Rapport annuel 2025, le gouvernement a fourni une réponse et fait le point concernant la recommandation du Comité d'élaborer un cadre commun de mesure du rendement pour renforcer la responsabilisation à l'égard de la diversité et de l'inclusion.

Réponse à la R4

On a envisagé un cadre commun de mesure du rendement. Toutefois, les ministères et organismes disposent de leurs propres plans d'équité en matière d'emploi, qui prévoient des objectifs et des indicateurs. Les ministères et organismes continuent d'améliorer et de mettre à jour leurs plans, notamment en élaborant des cadres de mesure du rendement, et en mesurant le rendement pour remédier à la sous-représentation. Récemment, le Bureau du dirigeant principal des ressources humaines a publié des directives sur la façon d'élaborer des indicateurs de rendement; et les ministères et organismes adapteront leurs indicateurs, au besoin.

Chaque ministère et organisme faisant partie de l'appareil de la sécurité et du renseignement mène ses activités dans des circonstances précises et joue un rôle unique, qui nécessite des compétences et de l'expérience variées. Les cadres de mesure du rendement propres aux ministères et organismes tiennent compte de leurs différences en ce qui concerne les besoins en main-d'œuvre, les stratégies de recrutement et toute lacune qu'ils doivent combler individuellement. Il est peu probable qu'un cadre commun tienne compte de ces différences de manière efficace, alors il ne serait probablement pas aussi efficace que les cadres ministériels individuels pour aborder les considérations relatives à la diversité et à l'inclusion.

Annexe C: Abréviations

ACS Plus	Analyse comparative entre les sexes Plus
CETO	Comité d'examen de la technologie opérationnelle
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement
CSNR	Conseiller à la sécurité nationale et au renseignement
CST	Centre de la sécurité des télécommunications
É.-U.	États-Unis d'Amérique
ETHI	Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique
FSC	Fournisseur de services de communication
FSE	Fournisseurs de services électroniques
GRC	Gendarmerie royale du Canada
GTI	Groupe de travail interministériel
LIC	Loi sur Investissement Canada
MJ	Ministère de la Justice
OEA	Outils d'enquête sur appareil
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement
PNIT	Programme national d'intégration de la technologie
RU	Royaume-Uni
SCRS	Service canadien du renseignement de sécurité