Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport annuel 2021

Canada

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport annuel 2021 (Version révisée selon le paragraphe 21(5) de la Loi sur le CPSNR)
CP100F-PDF (En ligne)
ISSN 2562-5136 (En ligne)

This publication is also available in English:
Annual Report 2021 (Revised version pursuant to subsection 21(5) of the NSICOP Act)

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

Rapport annuel 2021

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Mai 2022

Présenté au premier ministre le 18 mai 2022
en vertu du paragraphe 21(1) de la Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement

Version révisée déposée au Parlement le 28 septembre 2022
en vertu du paragraphe 21(5) de la Loi

Révisions

En application du paragraphe 21(1) de la Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement (Loi sur le CPSNR), le Comité doit présenter au premier ministre un rapport annuel. Conformément au paragraphe 21(5) de la Loi sur le CPSNR, le premier ministre peut, après consultation du président du Comité, ordonner au Comité de lui présenter un rapport révisé qui ne contient pas de renseignements dont il considère que la communication porterait atteinte à la sécurité ou à la défense nationale ou aux relations internationales, ou encore qui sont protégés par le secret professionnel d'un avocat.

Le présent rapport a été soumis au premier ministre le 18 mai 2022. Aucune révision n'a été apportée au document dans le but de retirer de l'information dont la communication, selon le premier ministre, aurait porté atteinte à la sécurité ou à la défense nationale ou aux relations internationales, ou qui serait protégée par le secret professionnel d'un avocat.

Message du président

Ottawa (Ontario) – 18 mai 2022

L'année dernière a posé encore une fois d'importants défis pour le Comité et tous les Canadiens. Pour sa part, le Comité a continué de recourir aux locaux sécurisés de l'appareil de la sécurité et du renseignement pour remplir son mandat en matière d'examen tout en respectant les règles de la santé publique en place au Canada. Ainsi, le Comité a pu terminer un rapport, qu'il a remis au premier ministre en août 2021, et préparé le terrain pour deux autres rapports, qui se poursuivent. Le Comité a été dissout en août lors de la délivrance des brefs électoraux, mais le Secrétariat du Comité a poursuivi l'important travail commencé par le Comité pendant son mandat.

En application de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement,* le Comité fait dans le présent rapport un résumé du rapport spécial présenté au premier ministre et remplit ses autres obligations en matière de rapport.

Le Comité est d'avis que les réponses à ses recommandations sont un élément essentiel au renforcement des opérations et de la responsabilisation des organisations de la sécurité et du renseignement.

Réalisations de 2021

L'année du Comité était bien remplie et a été fructueuse, malgré les défis liés à la santé publique. Son Rapport annuel 2020 a été déposé devant le Parlement en mars 2021. Il comprenait un résumé non classifié des grandes menaces qui pèsent sur la sécurité nationale du Canada. Le Comité a également réalisé un examen en profondeur des moyens de cyberdéfense du Canada, qui a été présenté au premier ministre en août 2021. Une version révisée a été déposée devant le Parlement en février 2022. J'incite les Canadiens à lire les deux rapports.

Le Comité a également poursuivi ses travaux sur deux autres examens. Le premier porte sur les activités liées à la sécurité et au renseignement d'Affaires mondiales Canada. Dans le cadre de cet examen, le Comité a analysé une myriade de documents et a tenu de nombreuses audiences. Il a également entamé un examen sur les activités de la Police fédérale de la Gendarmerie royale du Canada et prévoit d'organiser des séances d'information et des audiences connexes au printemps 2022.

Opportunités et difficultés

L'année qui vient offre au Comité et au Parlement nombre d'occasions exceptionnelles. Particulièrement, le Parlement devrait lancer son examen quinquennal de la Loi sur le CPSNR. Il s'agit d'un important jalon dans l'évolution du Comité et d'une occasion pour le Parlement de déterminer s'il est nécessaire d'apporter des modifications à la loi habilitante du Comité. Les membres du Comité et son Secrétariat attendent avec intérêt la perspective de contribuer aux discussions.

Cette année, le Comité s'est réjoui de constater qu'un enjeu de longue date a partiellement été résolu. Pour la première fois, le gouvernement a donné au Comité une réponse officielle

aux recommandations formulées dans l'un de ses rapports, soit le rapport spécial sur les moyens de cyberdéfense du gouvernement. Le Comité est d'avis que les réponses à ses recommandations sont un élément essentiel au renforcement des opérations et à la responsabilisation des organisations de la sécurité et du renseignement. Il accueille favorablement l'engagement du gouvernement, qu'il avait cerné comme élément à améliorer dans ses derniers rapports annuels. Le Comité encourage le gouvernement à répondre aux recommandations qu'il lui a présentées dans ses sept examens précédents des enjeux critiques de l'appareil de la sécurité et du renseignement, notamment l'autorisation légale du ministère de la Défense nationale et des Forces armées canadiennes à mener leurs activités de renseignement de défense, et l'absence d'une stratégie pangouvernementale pour répondre à l'ingérence étrangère au Canada. Au cours de la prochaine année, le Comité nouera le dialogue avec les organisations touchées par ses examens précédents afin de déterminer si elles acceptent les recommandations du Comité et les mesures prises pour y répondre.

Conclusion

Je tiens à exprimer ma sincère gratitude envers mes collègues du Comité. Le travail que nous accomplissons contribue à l'efficacité de l'appareil de la sécurité et du renseignement du Canada; votre contribution est inestimable. Je souhaite également remercier les représentants des organisations de la sécurité et du renseignement pour leur collaboration dans le cadre du processus d'examen. Enfin, au nom de tous mes collègues du Comité, nous remercions le Secrétariat pour son soutien indéfectible.

L'honorable David McGuinty, C.P., député,
Président
Comité des parlementaires sur la sécurité nationale et le renseignement

Le Comité des parlementaires sur la sécurité nationale et le renseignement

(Membres de la 43e législature)

L'honorable David McGuinty, C.P., député (président)

Mme Leona Alleslev, députée

M. Stéphane Bergeron, député

M. Don Davies, député

L'honorable Dennis Dawson, sénateur

M. Ted Falk, député (a démissionné le 15 juin 2021)

M. Peter Fragiskatos, député

Mme Iqra Khalid, députée

L'honorable Frances Lankin, C.P., C. M., sénatrice

M. Rob Morrison, député

M. Glen Motz, M.O.M., député (a démissionné le 15 juin 2021)

Mme Jennifer O'Connell, députée (a démissionné le 19 mars 2021)

Mme Brenda Shanahan, députée

L'honorable Vernon White, sénateur

Table des matières

Introduction

1. Le Comité des parlementaires sur la sécurité nationale et le renseignement (le Comité) est heureux de présenter son quatrième rapport annuel au premier ministre. Le rapport fait la synthèse de l'exhaustif *Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques,* un rapport spécial réalisé par le Comité en 2021, comprenant les conclusions et les recommandations de l'examen. Il comprend aussi les travaux réalisés par le Comité au cours de la dernière année.

2. Le rapport annuel de cette année diffère de ceux qui le précèdent. En 2021, le Comité a décidé de présenter ses examens futurs sous forme de rapports spéciaux. Ainsi, les examens du Comité se dissocieront du cycle de rapport annuel, permettant au Comité de mener des examens complexes sur différentes périodes et de présenter au premier ministre ses rapports dès qu'ils sont prêts. Par conséquent, les rapports seront déposés devant le Parlement et offerts aux Canadiens rapidement. Dorénavant, les rapports annuels du Comité porteront surtout sur les activités du Comité réalisées au cours de l'année précédente et serviront à répondre aux exigences en matière de rapport de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement.*

Les activités du Comité en 2021

3. Entre le 1er janvier 2021 et le 15 août 2021, le Comité s'est réuni à dix reprises, dont quatre fois dans le cadre d'audiences. Il a rencontré 22 représentants de quatre organisations différentes, employant une formule hybride de réunions en personne et de vidéoconférences sécurisées.

4. En 2021, au titre de l'alinéa 8(1)a) de la Loi sur le CPSNR, le Comité a réalisé un examen de cadre, soit le *Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques,* qui comprenait quatre conclusions et deux recommandations. Le Comité poursuit ses deux autres examens : les activités liées à la sécurité et au renseignement d'Affaires mondiales Canada et le mandat de la Police fédérale de la Gendarmerie royale du Canada (GRC).

5. En août 2021, le Comité a été dissout lors de la délivrance des brefs électoraux. Le Secrétariat du Comité a continué de travailler sur les examens en cours, mais aucun rapport n'a pu être rédigé puisqu'un nouveau Comité n'avait pas été nommé.

Exigences en matière de rapport

Préjudice à la sécurité nationale et refus de communiquer un renseignement

6. La Loi sur le CPSNR comporte certaines exigences en matière de rapport. Le Comité doit inclure dans son rapport annuel le nombre de fois où, au cours de l'année précédente, un ministre compétent a déterminé que l'examen visé

à l'alinéa 8(1)b) 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. En 2021, aucun des examens proposés par le Comité n'a été considéré comme préjudiciable à la sécurité nationale 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**

Éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères

7. Conformément à la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères,* 12 organisations fédérales doivent présenter un rapport annuel à leur ministre concernant l'application de cette loi au cours de l'année civile précédente. 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 tel risque;

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

8. La Loi demande à ce que les ministres concernés fournissent une copie des rapports annuels liés aux mauvais traitements pour leur organisation au Comité et à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement.

En 2021, le Comité a reçu des rapports des ministères et organismes suivants.

- Affaires mondiales Canada
- Agence des services frontaliers du Canada
- Agence du revenu du Canada
- Centre d'analyse des opérations et déclarations financières du Canada
- Centre de la sécurité des télécommunications
- Défense nationale et Forces armées canadiennes
- Gendarmerie royale du Canada
- Immigration, Réfugiés et Citoyenneté Canada
- Pêches et Océans Canada
- Sécurité publique Canada
- Service canadien du renseignement de sécurité
- Transports Canada

Questions dont le Comité est saisi

9. Le 4 juin 2021, la ministre de la Santé a saisi le Comité en vertu de l'alinéa 8(1)c) de la Loi sur le CPSNR d'une question portant sur de possibles incidents de sécurité au Laboratoire national de microbiologie à Winnipeg, au Manitoba, et le congédiement de deux scientifiques canadiens. Le Comité continue de se pencher sur la question.

Résumé de l'examen sur les moyens de cyberdéfense

10. Le 17 septembre 2020, le Comité a annoncé son examen du cadre et des activités du gouvernement du Canada pour défendre ses systèmes et réseaux contre les cyberattaques. La version classifiée du rapport spécial du Comité a été présentée au premier ministre le 11 août 2021 et déposée devant le Parlement le 14 février 2022. Ce premier examen du genre décrit la menace que les auteurs de cybermenaces malveillants font peser sur les systèmes du gouvernement, montre l'évolution des politiques et lois du gouvernement du Canada en matière de cyberdéfense, étudie les rôles et responsabilités des organisations gouvernementales compétentes, et examine des études de cas pertinentes présentant des cas où les systèmes du gouvernement ont été la cible de cyberattaques.

Les réseaux du gouvernement du Canada constituent un élément crucial des infrastructures essentielles du Canada.

11. Dans le cadre de cet examen, le Comité a étudié des documents en provenance des trois organisations jouant un rôle central dans le développement et la mise en œuvre du cadre de cyberdéfense du gouvernement : le Centre de la sécurité des télécommunications (CST), le Secrétariat du Conseil du Trésor du Canada (SCT) et Services partagés Canada (SPC). Le Comité a reçu des documents couvrant la période de 2001 à 2021, principalement pour explorer l'évolution de la compréhension du gouvernement sur les cybermenaces, ainsi que les autorisations, les mécanismes de gouvernance et les activités nécessaires pour y répondre. Le Comité a tenu quatre audiences, deux en 2020 et deux en 2021. Il a rencontré 12 cadres supérieurs du CST et du SCT, et a examiné plus de 2 500 documents, faisant plus de 37 000 pages au total.

12. Le Comité a formulé quatre conclusions (voir à l'annexe A). Premièrement, les cybermenaces contre les systèmes et réseaux du gouvernement présentent un risque considérable pour la sécurité nationale et la continuité des opérations du gouvernement. Les réseaux du gouvernement du Canada constituent un élément crucial des infrastructures essentielles du Canada. Le gouvernement y a recours pour recueillir et conserver de l'information, comme les dossiers fiscaux, et pour fournir des services fondamentaux, comme l'assurance-emploi, aux Canadiens et aux entreprises canadiennes. L'information que les réseaux détiennent représente également une valeur considérable pour les adversaires du Canada, comme les auteurs de cybermenaces parrainés par l'État et les cybercriminels.

13. Deuxièmement, le gouvernement a bâti un cadre de cyberdéfense « horizontal » solide pour défendre ses systèmes et réseaux contre les cyberattaques. L'évolution de ce cadre s'est déroulée de façon inattendue et réactive, mais aussi de façon

délibérée et prévue. Des modifications législatives ont fourni de nouveaux pouvoirs, notamment dans les autorisations ministérielles de 2001 liées aux activités de cyberdéfense dans le cadre desquelles des communications privées pourraient être interceptées et dans les autorisations ministérielles de 2019 pour protéger les infrastructures électroniques non fédérales, qui ont entraîné la création d'activités visant à renforcer la sécurité des systèmes gouvernementaux et, éventuellement, à mieux les défendre. Au même moment, les principaux auteurs de cybermenace ont forcé le gouvernement à adapter ses moyens de défense, particulièrement après des cyberincidents critiques qui ont entraîné d'importantes pertes de données et mis en exergue la vulnérabilité de ministères distincts et du gouvernement de façon générale. Le gouvernement a réagi en élaborant des stratégies et des politiques clés, en investissant dans la modernisation de la technologie de l'information et des moyens de cyberdéfense, et en créant des organisations dont la tâche est de corriger les faiblesses du système.

Le Comité a constaté que la force du système de cyberdéfense du gouvernement est affaiblie par l'application inégale des responsabilités en matière de sécurité et de l'utilisation variable des services de cyberdéfense.

14. Ce faisant, le gouvernement a abandonné son approche de cyberdéfense cloisonnée, ministère par ministère. Il considère désormais le gouvernement comme une « entreprise », où quelques organisations sont responsables de la cyberdéfense de l'ensemble du gouvernement. Au cœur de ce cadre se trouvent trois organisations : le SCT, SPC et le CST. Néanmoins, ce cadre horizontal semble de plus en plus incompatible avec la structure d'autorité « verticale » actuelle du gouvernement, établie par ministère et décrite dans la *Loi sur la gestion des finances publiques.* Cette structure d'autorité rend les administrateurs généraux responsables en définitive de la protection des systèmes respectifs de leur ministère. Elle leur donne également la latitude d'accepter ou de rejeter les directives du SCT, du CST ou de SPC, mettant ainsi en péril l'efficacité globale du cadre de cyberdéfense.

15. Troisièmement, le gouvernement a établi des mécanismes de gouvernance clairs pour soutenir l'élaboration d'une politique stratégique en matière de cyberdéfense, la gestion efficace des projets de technologie de l'information touchant les opérations de l'ensemble du gouvernement, ainsi que la réponse du gouvernement aux cyberincidents. Le cadre a évolué au fil du temps en réponse aux changements apportés aux politiques, à l'appareil et à l'environnement de cybermenace du gouvernement.

16. Quatrièmement, le Comité a constaté que la force du système de cyberdéfense du gouvernement est affaiblie par l'application inégale des responsabilités en matière de sécurité et de l'utilisation variable des services de cyberdéfense. En bref, les organisations fédérales ne bénéficient pas toutes d'une protection en matière de cyberdéfense. Plus important encore, un certain nombre d'organisations et d'intérêts fédéraux ne sont pas assujettis aux directives ou aux politiques du Conseil du Trésor en matière de cyberdéfense et ne sont donc pas obligés d'obtenir des services de cyberdéfense du gouvernement. Certaines de ces organisations, dont des sociétés d'État, ont choisi de ne pas recourir aux services de cyberdéfense du gouvernement, ce qui expose ces organisations et le gouvernement dans son ensemble à un risque considérable face aux cybermenaces les plus avancées. Même parmi les organisations fédérales qui reçoivent des services en matière de cyberdéfense du CST, la protection n'est pas uniforme : les organisations peuvent choisir les services qu'elles souhaitent

recevoir et en refuser d'autres. Le Comité a constaté que, bien que le CST fournisse certains services de cyberdéfense à 160 des 169 organisations fédérales, seulement 43 de ces organisations reçoivent l'ensemble des services du CST.

17. Le Comité a formulé deux recommandations pour renforcer le cadre de cyberdéfense du gouvernement et élargir ce cadre le plus possible à l'ensemble des organisations gouvernementales fédérales (voir l'annexe B). D'abord, le Comité a recommandé que le gouvernement continue de renforcer son cadre de défense de ses réseaux contre les cyberattaques en assurant la modernisation des pouvoirs et des programmes en matière de cyberdéfense à mesure de l'évolution de la technologie et d'autres facteurs pertinents. Ensuite, le Comité a recommandé que le gouvernement intègre les politiques, directives et services pertinents en matière de cyberdéfense à toutes les organisations fédérales, dans toute la mesure du possible.

18. Ensemble, les recommandations du Comité visent à assurer une meilleure harmonisation des pouvoirs gouvernementaux à l'« entreprise » de cyberdéfense et à veiller à ce que toutes les organisations fédérales soient les mieux protégées possible par le périmètre sécurisé du gouvernement.

19. Le Comité s'est réjoui de constater que, pour la première fois, le gouvernement a donné au Comité une réponse officielle à ses recommandations. Il s'agit là d'une étape importante vers le renforcement de la responsabilisation et de la transparence.

Annexe A : Conclusions et recommandations de l'examen sur les moyens de cyberdéfense

Description

Rapport spécial qui porte sur la menace que font peser les cyberacteurs malveillants sur les systèmes du gouvernement, examine l'évolution des politiques et lois du gouvernement du Canada en matière de cyberdéfense, évalue les rôles et responsabilités des organisations gouvernementales pertinentes, et examine des études de cas pertinentes sur des cas de cybercompromission des systèmes du gouvernement lors de cyberattaques.

Conclusions

Le Comité formule les conclusions suivantes :

C1. Les cybermenaces envers les systèmes et les réseaux du gouvernement présentent un risque important à la sécurité nationale et à la continuité des activités du gouvernement. Les États-nations constituent les auteurs de menace les plus sophistiqués, mais tout acteur ayant des intentions malveillantes et des capacités avancées expose les données et l'intégrité de l'infrastructure numérique du gouvernement à un risque.

C2. Le gouvernement a mis en place un cadre « horizontal » rigoureux dans le but de se défendre contre les cyberattaques. Le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada et le Centre de la sécurité des télécommunications jouent un rôle essentiel dans ce cadre. Néanmoins, ce cadre horizontal semble de moins en moins compatible avec les pouvoirs « verticaux » en place de chaque ministère au titre de la *Loi sur la gestion des finances publiques.*

C3. Le gouvernement a établi des mécanismes de gouvernance clairs à l'appui de l'élaboration de politiques de cyberdéfense stratégiques, de la gestion efficace des initiatives liées à la sécurité des technologies de l'information qui touchent les activités de l'ensemble du gouvernement, ainsi que de l'intervention du gouvernement face aux cyberincidents. Le cadre a évolué au fil du temps en réponse aux changements apportés aux politiques, à l'appareil et à l'environnement de cybermenace du gouvernement.

C4. L'efficacité du cadre est affaiblie en raison de l'application non uniforme des responsabilités en matière de sécurité et de l'utilisation incohérente des services de cyberdéfense. Voici certaines des faiblesses :

- Les politiques du Conseil du Trésor relatives à la cyberdéfense ne sont pas appliquées de manière uniforme aux ministères et aux organismes. Par conséquent, les organisations n'exercent pas les mêmes responsabilités, exigences et pratiques, créant ainsi des lacunes dans la protection des réseaux du gouvernement contre les cyberattaques.

- Les sociétés d'État, et possiblement certains secteurs d'intérêt du gouvernement, constituent des cibles connues des acteurs étatiques, mais ne sont pas assujetties aux directives ou aux politiques liées au cyberenvironnement du Conseil du Trésor, et ne sont pas tenues de se procurer les services de cyberdéfense du gouvernement. Cette situation expose l'intégrité de leurs données et de leurs systèmes à un risque, et expose possiblement ceux du gouvernement à un risque important.
- Les services de cyberdéfense sont offerts de manière non uniforme. Même si Services partagés Canada offre certains services à 160 des 169 organisations fédérales, seules 43 d'entre elles reçoivent l'ensemble complet de ses services. Le Centre de la sécurité des télécommunications fournit des services à l'appui de ceux de Services partagés Canada et dans le cadre d'ententes avec certaines organisations. Ce manque d'uniformité fait en sorte que ces organisations de même que le reste du gouvernement courent des risques, et limite l'efficacité globale du programme de cyberdéfense du CST.

Recommandations

Le Comité formule les recommandations suivantes :

R1 Le gouvernement doit continuer de renforcer son cadre visant à défendre ses réseaux contre les cyberattaques en s'assurant que ses pouvoirs et ses programmes de cyberdéfense sont modernisés à mesure qu'évoluent la technologie et d'autres facteurs pertinents, y compris de les harmoniser au cadre horizontal de la cyberdéfense qui est apparu au cours de la dernière décennie.

R2 Dans la mesure du possible, le gouvernement doit :

- appliquer les politiques du Conseil du Trésor relatives à la cyberdéfense de manière uniforme dans les ministères et organismes;
- étendre les politiques du Conseil du Trésor relatives à la cyberdéfense à toutes les organisations fédérales, y compris les petits organismes, les sociétés d'État et les autres organisations fédérales qui ne sont pas actuellement assujettis aux politiques et aux directives du Conseil du Trésor liées a la cyberdéfense;
- étendre les services avancés de cyberdéfense, notamment le Service Internet d'entreprise de Services partagés Canada et les capteurs de cyberdéfense du Centre de la sécurité des télécommunications, à toutes les organisations fédérales.

Statut

Le gouvernement a fourni les réponses suivantes aux recommandations du Comité.

Réponse à R1 : Approuvée. Sécurité publique Canada, le Centre de la sécurité des télécommunications et le Secrétariat du Conseil du Trésor du Canada conviennent que le gouvernement doit continuer de renforcer son cadre servant à défendre ses réseaux des cyberattaques, en veillant à ce que les pouvoirs et les programmes connexes soient modernisés à mesure qu'évoluent les technologies et les autres facteurs pertinents.

Sécurité publique Canada, le Centre de la sécurité des télécommunications et le Secrétariat du Conseil du Trésor du Canada continueront de travailler en collaboration en vue d'harmoniser le cadre horizontal de cybersécurité, dans le but de veiller à ce qu'une structure de gouvernance appropriée soit en place pour faire progresser la politique de cybersécurité.

Responsables : Sécurité publique Canada, en consultation avec le Centre de la sécurité des télécommunications et le Secrétariat du Conseil du Trésor du Canada.

Réponse à R2.1 : Approuvée. Le Secrétariat du Conseil du Trésor du Canada examinera le cadre stratégique du Conseil du Trésor afin de s'assurer que les politiques de cyberdéfense soient appliquées aussi uniformément que possible aux ministères et organismes. Cela comprend l'harmonisation de la portée de la *Politique sur la sécurité du gouvernement* avec la *Politique sur les services et le numérique.*

Responsable : Secrétariat du Conseil du Trésor du Canada.

Réponse à R2.2 : Approuvée. Le Secrétariat du Conseil du Trésor du Canada entreprendra un examen du cadre stratégique du Conseil du Trésor afin d'étudier et de cerner les options éventuelles permettant d'étendre les politiques du Conseil du Trésor relevant de la cyberdéfense à toutes les organisations fédérales, y compris les petits organismes, les sociétés d'État et les autres organisations fédérales qui ne sont pas actuellement assujettis aux politiques et aux directives du Conseil du Trésor en lien avec la cyberdéfense. Cet examen tiendra compte de la *Loi sur la gestion des finances publiques* et des pouvoirs attribués en vertu de celle-ci, ainsi que toute considération juridique.

Responsable : Secrétariat du Conseil du Trésor du Canada.

Réponse à R2.3 : Approuvée. Le Secrétariat du Conseil du Trésor du Canada, en consultation avec Services partagés Canada et le Centre de la sécurité des télécommunications, convient que le gouvernement devrait étendre à l'ensemble des organisations fédérales ses services de cyberdéfense avancés, notamment le service Internet d'entreprise de Services partagés Canada et les capteurs de cyberdéfense du Centre de la sécurité des télécommunications, dans la mesure du possible. Le Secrétariat du Conseil du Trésor du Canada continuera de renforcer ses mesures de cyberdéfense dans le cadre de ses modifications apportées à la *Politique sur les services et le numérique,* en s'appuyant notamment sur les procédures obligatoires décrites à l'annexe G : Norme relative aux configurations communes des services informatiques intégrés de la *Directive sur les services et le numérique* qui sera publiée au début de 2022.

Services partagés Canada, en consultation avec le Secrétariat du Conseil du Trésor du Canada et le Centre de la sécurité des télécommunications, évalue, dans le cadre d'une étude financée, la situation actuelle des petits ministères et organismes (PMO) qui n'ont pas adopté le service Internet d'entreprise de Services partagés Canada. L'évaluation a pour but de produire une analyse de rentabilisation chiffrée décrivant le financement nécessaire pour migrer les PMO au service Internet d'entreprise de Services partagés Canada, d'éliminer le recours à des services Internet qui ne sont pas gérés par Services partagés Canada, et de fournir d'autres services intégrés (y compris les capteurs de cyberdéfense du Centre de la sécurité des télécommunications), ce qui permettra d'améliorer la sécurité des PMO et de réduire l'exposition aux menaces des réseaux intégrés du gouvernement.

Le Centre de la sécurité des télécommunications, en consultation avec le Secrétariat du Conseil du Trésor du Canada, étudiera les options permettant de fournir les capteurs de cyberdéfense du Centre de la sécurité des télécommunications à l'ensemble des organisations fédérales.

Responsables : Secrétariat du Conseil du Trésor du Canada, en consultation avec Services partagés Canada et le Centre de la sécurité des télécommunications.

Annexe B : Recommandations des examens antérieurs

Rapport spécial sur les allégations entourant la visite officielle du premier ministre Trudeau en Inde en février 2018

Description

Rapport spécial sur les allégations entourant la visite du premier ministre en Inde en février 2018 en ce qui concerne l'ingérence étrangère dans les affaires politiques du Canada, les risques pour la sécurité du premier ministre et l'utilisation inappropriée de renseignements.

Recommandations

L'ingérence étrangère

R1 Dans l'intérêt de la sécurité nationale, il faudrait informer les députés de la Chambre des communes et les sénateurs des risques que représentent l'ingérence étrangère et l'extrémisme au Canada au moment de leur assermentation, et un suivi en ce sens devrait être effectué régulièrement par la suite. De plus, il faudrait rappeler aux ministres du Cabinet les attentes énoncées dans le document du gouvernement *Pour un gouvernement ouvert et responsable,* notamment le fait que l'on s'attend à ce que les ministres fassent preuve de discernement quant aux personnes qu'ils rencontrent et avec lesquelles ils établissent des liens et à ce qu'ils fassent clairement la distinction entre les messages officiels et les messages privés dans les médias. Il faudrait aussi leur rappeler que conformément à la *Loi sur les conflits d'intérêts,* les titulaires d'une charge publique doivent toujours accorder la priorité à l'intérêt public avant leurs intérêts personnels. ***

R2 Le ministre de la Sécurité publique et de la Protection civile devrait envisager de modifier *** afin d'y inclure un rôle officiel pour le conseiller à la sécurité nationale et au renseignement. En effet, selon l'information que le Comité a reçue, le CSNR a joué un rôle important ***. Le Comité estime qu'il est légitime que le CSNR formule des conseils en sa qualité de coordonnateur de la communauté de la sécurité et du renseignement et de conseiller auprès du premier ministre. ***

Sécurité

R3 Un examen interministériel devrait être entrepris à partir des conclusions du Comité afin que l'on définisse les principales leçons apprises dans la foulée de ces événements.

R4 Le gouvernement devrait élaborer et mettre en place une méthode uniforme pour la vérification des antécédents qui devrait être suivie par toutes les organisations qui prennent part à l'établissement des listes d'invités proposés en vue des événements auxquels le premier ministre participe à l'étranger.

Utilisation du renseignement

R5 Le premier ministre devrait réexaminer le rôle du CSNR en ce qui concerne la lutte contre les menaces pour la sécurité du Canada. Le Comité a déjà formulé une recommandation relativement au rôle du CSNR quant ***. Le Comité fait remarquer que d'autres ministères et organismes gouvernementaux ont déjà le pouvoir, en vertu de la loi, de prendre des mesures afin de protéger le Canada contre les menaces pour sa sécurité. Il faudrait aussi préciser le rôle du CSNR par rapport à ces organismes.

Statut

Le Comité demande une mise à jour du statut en 2022.

Examen du processus d'établissement des priorités en matière de renseignement

Description

Examen du processus du gouvernement du Canada relatif à l'établissement des priorités en matière de renseignement, axé sur la gouvernance du processus, la participation des organisations touchées, et la mesure du rendement et les dépenses relatives aux ressources.

Recommandations

R1 La conseillère à la sécurité nationale et au renseignement, avec l'appui du Bureau du Conseil privé, investit et joue un rôle de gestion et de direction plus important dans le processus lié à l'établissement des priorités en matière de renseignement afin de s'assurer que les réponses organisationnelles aux priorités en matière de renseignement sont mises en œuvre rapidement et uniformément.

R2 L'appareil de la sécurité et du renseignement élabore un aperçu stratégique des exigences permanentes en matière de renseignement pour s'assurer que le Cabinet reçoit la meilleure information possible pour prendre des décisions.

R3 Sous la direction de la conseillère à la sécurité nationale et au renseignement et avec l'appui du Bureau du Conseil privé, l'appareil de la sécurité et du renseignement élabore des outils pour relever les défis liés à la coordination et à l'établissement des priorités en lien avec les exigences permanentes en matière de renseignement.

R4 L'appareil de la sécurité et du renseignement, en consultation avec le Secrétariat du Conseil du Trésor, élabore un cadre de mesure du rendement uniforme dans le but d'examiner dans quelle mesure l'appareil répond aux priorités en matière de renseignement, y compris un examen robuste et uniforme des dépenses relatives aux ressources.

Statut

Le Comité demande une mise à jour du statut en 2022.

Examen des activités de renseignement du ministère de la Défense nationale et des Forces armées canadiennes

Description

Examen des activités de renseignement du ministère de la Défense nationale et des Forces armées canadiennes. Le Comité a examiné la portée de ces activités, leurs pouvoirs juridiques et les mécanismes de surveillance existants liés au contrôle et à la reddition de comptes.

Recommandations

R1 Le ministère de la Défense nationale et les Forces armées canadiennes (MDN/FAC) examinent et renforcent leur cadre administratif qui gouverne les activités du renseignement de défense, particulièrement en ce qui a trait à la Directive ministérielle sur le renseignement de défense, pour faire en sorte de respecter ses propres obligations de gouvernance et de rapport au ministre de la Défense nationale, et de bien faire le suivi du respect de ces obligations, notamment :

- Concevoir un processus normalisé, ou des principes, pour déterminer le lien entre une activité du renseignement de défense et une mission autorisée par la loi;
- Consigner le respect des obligations de la Directive, y compris les domaines de risque cernés dans la Directive qui ne sont pas actuellement inclus dans le rapport annuel à l'intention du ministre;
- Mettre en œuvre un processus normalisé de consultations interministérielles concernant le déploiement de capacités du renseignement de défense, qui comprend une norme minimale de documentation.

R2 Le gouvernement modifie le projet de loi C-59, *Loi concernant les questions de sécurité nationale,* de manière à ce que le mandat de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement proposé comporte une exigence explicite de faire rapport chaque année sur les activités du MDN/FAC liées à la sécurité nationale ou au renseignement.

R3 Se basant sur les évaluations et les conclusions du Comité, le gouvernement envisage sérieusement de fournir un pouvoir légal explicite pour la conduite des activités du renseignement de défense.

Statut

La lettre de mandat envoyée au ministre de la Défense le 13 décembre 2019, mentionne :

Appuyer le ministre de la Défense nationale afin de mettre en place un nouveau cadre régissant comment le Canada recueille, gère et utilise le renseignement de défense, comme le recommande le Comité des parlementaires sur la sécurité nationale et le renseignement.

Le Comité reconnaît que les événements ont rendu désuète la recommandation R2.

Le Comité demande une mise à jour du statut en 2022.

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

Description

Examen qui offre une évaluation de base de 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 examine 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

R1 Le Comité procède à un examen rétrospectif d'ici trois à cinq ans pour évaluer le progrès réalisé par l'appareil de la sécurité et du renseignement dans l'atteinte des objectifs et la mise en œuvre des initiatives en matière de diversité et d'inclusion, et pour examiner plus en profondeur la question de l'inclusion, y compris les questions de harcèlement, de violence et de discrimination, en sollicitant davantage les employés.

R2 L'appareil de la sécurité et du renseignement adopte une approche cohérente et transparente de la planification et du suivi des objectifs relatifs à l'équité en matière d'emploi et à la diversité, et qu'il procède régulièrement à des examens de ses politiques et de ses pratiques relatives à l'emploi (examens des systèmes d'emploi) pour relever les obstacles possibles à l'emploi auxquels se heurtent les femmes, les Autochtones, les personnes faisant partie des minorités visibles et les personnes handicapées.

R3 L'appareil de la sécurité et du renseignement améliore la robustesse de sa collecte et de son analyse de données, notamment au moyen d'évaluations ACS+ des mesures de dotation interne, des politiques de promotion et d'analyses segmentées de l'effectif. À ce sujet, le Comité souligne aussi que les organisations auront bientôt l'obligation d'enquêter sur tous les cas de harcèlement et de violence au travail, de les enregistrer et de les signaler.

R4 L'appareil de la sécurité et du renseignement élabore un cadre commun de mesure du rendement et qu'elle 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.

Statut

Le Comité demande une mise à jour du statut en 2022.

La réponse du gouvernement a l'ingérence étrangère

Description

Examen de la portée et de l'étendue de l'ingérence étrangère au Canada, de la réponse du gouvernement, des organisations touchées et de leurs moyens pour y répondre, de l'étendue de la coordination et de la collaboration parmi ces organisations, de la mesure dans laquelle le gouvernement travaille avec les autres ordres de gouvernement et les cibles d'ingérence étrangère, et de l'engagement du gouvernement auprès d'alliés à l'étranger.

Recommandations

R1 Le gouvernement du Canada élabore une stratégie exhaustive pour lutter contre l'ingérence étrangère et renforcer la résilience des institutions et de la population. Basée sur l'examen et les conclusions du Comité, la stratégie devrait :

- définir les risques et les préjudices à court et à long terme pour les institutions et les droits et libertés des Canadiens que fait peser la menace de l'ingérence étrangère;
- examiner et prendre en main la vaste étendue des vulnérabilités institutionnelles auxquelles s'attaquent les états étrangers hostiles, y compris les champs ne faisant expressément pas partie de l'examen du Comité;
- évaluer la validité des lois en vigueur liées à l'ingérence étrangère, comme la *Loi sur la protection de l'information* et la *Loi sur le Service canadien du renseignement de sécurité,* et permettre la proposition de modifications au besoin;
- élaborer des mécanismes opérationnels et stratégiques pratiques et pangouvernementaux pour cerner les activités des états hostiles et y réagir;
- mettre en place des mécanismes réguliers de collaboration avec les paliers infranationaux du gouvernement et les organismes d'application de la loi, y compris fournir les cotes de sécurité nécessaires;
- comprendre une approche à l'intention des ministres et des hauts dirigeants afin qu'ils nouent le dialogue avec les institutions fondamentales et la population;
- orienter la coopération avec les alliés au sujet de l'ingérence étrangère.

R2 Le gouvernement du Canada appuie cette stratégie exhaustive grâce à une direction et une coordination centrales durables. Pour donner un exemple d'entité de coordination centrale visant à agir sur l'ingérence étrangère, le Comité renvoie à la nomination et au mandat du coordonnateur de la lutte nationale contre l'ingérence étrangère de l'Australie.

Statut

Le Comité demande une mise à jour du statut en 2022.

Les activités de l'Agence des services frontaliers du Canada relatives à la sécurité nationale et au renseignement

Description

Examen des activités de sécurité nationale et de renseignement de l'Agence des services frontaliers du Canada (ASFC), axé sur la gouvernance de l'ASFC sur les activités de sécurité nationale et de renseignement du programme d'exécution de la loi et du renseignement de l'ASFC, de la conduite des activités sensibles de sécurité nationale et de renseignement de l'ASFC, et des relations de l'ASFC avec ses partenaires clés de la sécurité nationale et du renseignement.

Recommandations

R1 Le ministre de la Sécurité publique et de la Protection civile fournit des directives par écrit à l'Agence des services frontaliers du Canada à l'égard de la conduite d'activités sensibles relatives à la sécurité nationale et au renseignement. Cette directive doit inclure des attentes claires en matière de reddition des comptes et des obligations relatives à la présentation de rapports annuels.

R2 L'Agence des services frontaliers du Canada doit mettre en place un processus d'évaluation et de présentation de rapport sur les risques et les résultats de ses activités sensibles relatives à la sécurité nationale et au renseignement.

Statut

Le 16 février 2022, le ministre de la Sécurité publique a émis la *Ministerial Direction to the Canada Border Services Agency on Surveillance and Confidential Human Sources,* qui commande à l'Agence d'établir des mécanismes de gestion des risques et d'établissement de rapports liés à la surveillance et aux sources humaines confidentielles.

Rapport spécial sur la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens dans le contexte des activités du renseignement de défense du ministère de la Défense nationale et des Forces armées canadiennes

Description

Rapport spécial sur la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens dans le contexte des activités de renseignement de défense du ministère de la Défense nationale et des Forces armées canadiennes, axé sur le contexte opérationnel, le cadre juridique, la directive fonctionnelle CANCIT, et le traitement de l'information sur des Canadiens avant la directive.

Recommandations

Le Comité formule les recommandations suivantes :

R1 Le ministère de la Défense nationale / les Forces armées canadiennes (MDN/FAC) abroge la *Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information* et, en consultation avec le commissaire à la protection de la vie privée, revoit toutes ses directives fonctionnelles et autres instruments stratégiques qui ont trait à la collecte, à l'utilisation, à la conservation et à la diffusion de renseignements sur les Canadiens pour assurer une gouvernance cohérente de ces activités.

R2 Afin de régler la question de l'application extraterritoriale de la *Loi sur la protection des renseignements personnels,* le ministre de la Défense nationale doit veiller à ce que le MDN/FAC respecte la lettre et l'esprit de la *Loi sur la protection des renseignements personnels* dans toutes ses activités du renseignement de défense, au Canada et à l'étranger.

R3 Le ministre de la Défense nationale présente un projet de loi régissant les activités du renseignement de défense du MDN/FAC, notamment pour déterminer dans quelle mesure le MDN/FAC est autorisé à recueillir, à utiliser, à conserver et à communiquer de l'information sur des Canadiens dans l'exécution de ses missions autorisées.

Statut

Le Comité demande une mise à jour du statut en 2022.

Annexe C : Le processus d'examen

Type d'examen

Cadre

Examen des cadres législatif, réglementaire, stratégique, financier et administratif de la sécurité nationale ou du renseignement.

Activité

Examen des activités des ministères liées à la sécurité nationale ou au renseignement.

Critères d'examen

Pour que le Comité envisage un examen, la question doit se rapporter à un membre principal de l'appareil de la sécurité et du renseignement et :

- dans le domaine de la sécurité nationale, être considérée se rapporter aux menaces envers la sécurité du Canada telles qu'elles sont définies dans la Loi sur le SCRS ou à la criminalité de nature et de gravité nationale;
- dans le domaine du renseignement, se rapporter principalement à l'utilisation de sources ou de méthodes clandestines, secrètes ou privilégiées.

Éléments à prendre en compte pour l'examen

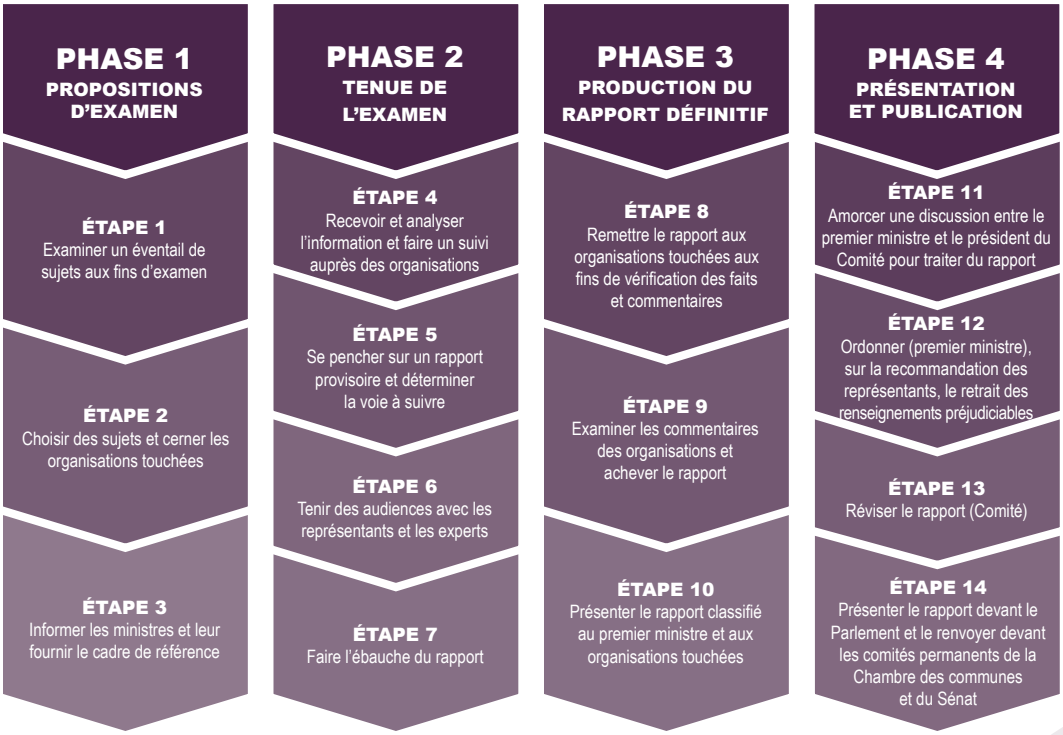
Concernant l'organisation

- L'organisation a déjà fait l'objet d'un examen;
- la portée de ses activités liées à la sécurité ou au renseignement et la mesure dans laquelle elles sont connues;
- les activités sont régies par une loi ou une directive gouvernementale.

En général

- La mesure dans laquelle une activité ou une question touche les droits des Canadiens;
- la mesure dans laquelle une activité ou une question touche les alliances canadiennes ou les relations avec l'étranger;
- l'activité ou la question suscite un grand intérêt du public;
- l'activité ou la question touche la souveraineté du Canada ou l'intégrité de ses institutions, de son économie ou de la société;
- le Parlement ou un autre organisme d'examen a déjà examiné l'activité ou la question

Processus d'examen



Abréviations

Cabinet	Cabinet du Canada
AMC	Affaires mondiales Canada
ASFC	Agence des services frontaliers du Canada
BCP	Bureau du Conseil privé
CPM	Cabinet du premier ministre
CSNR	Conseiller à la sécurité nationale et au renseignement auprès du premier ministre
CST	Centre de la sécurité des télécommunications
FAC	Forces armées canadiennes
GC	Gouvernement du Canada
GRC	Gendarmerie royale du Canada
MDN	Ministère de la Défense nationale
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement
SCRS	Service canadien du renseignement de sécurité
SCT	Secrétariat du Conseil du Trésor
SP	Sécurité publique Canada
SPC	Services partagés Canada