Office de surveillance des activités en matière de sécurité nationale et de renseignement

National Security and Intelligence Review Agency

Canada

OSSNR

2023 // Rapport Annuel

Numéro ISSN : 2563-5786
Numéro de catalogue PS106-9F-PDF

26 septembre 2024

Le très honorable Justin Trudeau, C.P., député
Premier ministre du Canada
Bureaux du premier ministre et du Conseil privé
Ottawa (ON)
K1A 0A2

Monsieur le Premier ministre,

Au nom de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), j'ai le plaisir de vous présenter notre cinquième rapport annuel. Conformément au paragraphe 38(1) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, le rapport comprend des renseignements sur nos activités tout au long de 2023, ainsi que nos conclusions et nos recommandations.

Conformément à l'alinéa 52(1)b) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, notre rapport a été préparé après consultation des administrateurs généraux concernés afin de s'assurer qu'il ne contient pas de renseignements dont la divulgation porterait atteinte à la sécurité nationale, à la défense nationale, aux relations internationales, au secret professionnel des avocats et des notaires ou au privilège relatif au litige.

Veuillez agréer, Monsieur, l'expression de mes sentiments distingués.

L'honorable Marie Deschamps, C.C.

Présidente // Office de surveillance des activités en matière de sécurité nationale et de renseignement

Table des matières

Message des membres

A titre de membres de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), nous sommes heureux de présenter notre rapport annuel de 2023, qui marque le cinquième anniversaire du parcours de notre organisme. Le rapport englobe toutes nos activités de la dernière année et représente une occasion de réfléchir aux progrès et à l'évolution de notre organisme depuis 2019.

Au fil des événements mondiaux, le rythme des activités en matière de sécurité et de renseignement s'est accéléré, et la présence de notre organisme n'a jamais été aussi importante. Depuis la création de l'OSSNR, notre mandat consiste à assurer une surveillance et une reddition de comptes indépendantes des activités du Canada en matière de sécurité nationale et de renseignement. Au cours des cinq dernières années, nous avons offert au public canadien une plus grande transparence quant à ces activités, et nous sommes fiers des progrès que nous avons réalisés dans le cadre de notre mandat crucial.

Notre organisme a évolué et s'est amélioré de nombreuses façons. Nous avons renforcé notre capacité de mener des enquêtes et des examens exhaustifs et efficaces sur les diverses activités de sécurité nationale et de renseignement de notre pays. Nous avons formé une équipe de professionnels dévoués possédant une riche expertise dans de nombreux domaines, ce qui nous permet de gérer des enjeux complexes et de fournir des évaluations et des recommandations éclairées.

Nous avons également favorisé l'entretien de relations constructives avec les entités examinées, les organismes partenaires, les comités parlementaires et les organisations de la société civile. Ces partenariats ont contribué à faciliter notre accès à l'information, ont appuyé notre participation à des conversations significatives, ainsi que notre capacité de promouvoir la transparence et la responsabilité.

Au cours des cinq dernières années, nous avons amélioré la sensibilisation et la compréhension du public quant aux enjeux importants en matière de sécurité nationale et de renseignement. Par la publication de nos rapports, nous avons cherché à démystifier ce domaine souvent hors de portée et à permettre aux Canadiens de participer à des discussions éclairées sur leur sécurité et leurs droits.

Alors que nous réfléchissons à ce que nous avons accompli jusqu'à maintenant, nous demeurons conscients des défis qui nous attendent. Le domaine de la sécurité nationale et du renseignement évolue constamment, et les nouvelles menaces et les avancées technologiques créent de nouveaux défis. Alors que les organismes de sécurité et de renseignement du Canada doivent fournir des

réponses adaptatives et souples, l'OSSNR continuera d'évaluer si ces réponses sont légales, raisonnables et nécessaires.

En ce qui concerne l'avenir, nous sommes déterminés à poursuivre notre travail essentiel. Nous demeurerons dévoués et vigilants dans notre rôle visant à assurer la responsabilisation au sein du cadre canadien de sécurité nationale et de renseignement et à veiller à ce que les activités de sécurité nationale et de renseignement respectent les droits et libertés de tous les Canadiens.

Nous remercions tous les membres, anciens et actuels, du personnel du secrétariat, dont le dévouement et le soutien ont contribué à l'évolution de l'OSSNR au cours des cinq dernières années. Leurs efforts inestimables ont façonné notre organisme et notre travail au service du public canadien.

Marie Deschamps	Marie-Lucie Morin	Foluke Laosebikan	Jim Chu
Craig Forcese	Matthew Cassar	Colleen Swords	

Sommaire

1. L'année 2023 a été importante pour l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). Des efforts constants visant à améliorer les processus de l'Office et à professionnaliser ses approches permettent à l'OSSNR de mener des examens et des enquêtes conformes aux normes les plus rigoureuses qui soient. Le présent rapport souligne les résultats positifs obtenus grâce à des méthodes raffinées, des partenariats solides et un engagement inébranlable envers tous les Canadiens en vue d'assurer la responsabilité et la transparence des activités de sécurité nationale et de renseignement du gouvernement du Canada.

Les cinq premières années de l'OSSNR

2. L'OSSNR a célébré son cinquième anniversaire en juillet 2024 et a profité de cette occasion pour réfléchir à sa croissance et à son évolution, ainsi qu'aux leçons retenues. L'OSSNR s'est consacré à son mandat vaste et unique en effectuant des examens touchant de nombreuses organisations et en améliorant la transparence dans la mise en œuvre de son mandat d'enquête. L'OSSNR a accordé la priorité à la croissance et au perfectionnement de son personnel, a amélioré la littératie en matière d'examen dans l'ensemble des entités examinées et a continué de maintenir les pratiques exemplaires et les normes les plus élevées dans l'application de son mandat.

Valeur des partenariats élargis

3. L'OSSNR a élargi et mis à profit son réseau de partenaires de surveillance par le biais de nombreux engagements auprès d'homologues internationaux et de participations à des forums internationaux au cours de 2023. Toutes les parties ont pu profiter de l'échange de pratiques exemplaires, de leçons tirées, d'expertise et de recherches. L'intégration de l'OSSNR au sein de la communauté internationale de surveillance en matière de sécurité nationale et de renseignement a appuyé le perfectionnement de l'Office et lui a permis d'améliorer sa capacité d'exécuter son mandat.

Examens

4. Les points saillants des examens terminés en 2023, ainsi que les principaux résultats, sont présentés ci-dessous (les examens en cours ne sont pas inclus.) L'annexe B énumère toutes les conclusions et recommandations tirées des examens effectués en 2023 s'il y a lieu.

Service canadien du renseignement de sécurité

5. L'OSSNR a réalisé les examens suivants de certaines activités visées du Service canadien du renseignement de sécurité (SCRS) :

    - un examen du régime applicable aux ensembles de données du SCRS, y compris sa mise en œuvre, dont les aspects concernant la gouvernance, la gestion de l'information, les pratiques de conservation et la formation;
    - un examen annuel des activités du SCRS, qui a servi, en partie, à orienter le rapport annuel classifié de 2023 de l'OSSNR à l'intention du ministre de la Sécurité publique du Canada.

Centre de la sécurité des télécommunications

6. L'OSSNR a réalisé les examens suivants de certaines activités visées du Centre de la sécurité des télécommunications (CST) :

    - un examen de l'utilisation du polygraphe par le CST dans le cadre du filtrage de sécurité, qui s'est penché sur la façon dont le CST gère son programme de polygraphe et sur le rôle du Secrétariat du Conseil du Trésor du Canada (SCT) dans l'établissement de la Norme sur le filtrage de sécurité qui oriente l'utilisation du polygraphe pour le filtrage de sécurité au sein du gouvernement du Canada.
    - un examen des solutions réseau du CST et des activités connexes de cybersécurité et d'assurance de l'information. Il s'agissait du premier examen de ces activités par l'OSSNR, qui a également mené son premier examen de Services partagés Canada (SPC).
    - un examen annuel des activités du CST, qui a servi, en partie, à orienter le rapport annuel classifié de 2023 de l'OSSNR à l'intention du ministre de la Défense nationale du Canada.

Agence des services frontaliers du Canada

7. L'OSSNR a effectué un examen du programme des sources humaines confidentielles (SHC) de l'Agence des services frontaliers du Canada (ASFC) dans le but d'examiner les cadres juridiques et politiques régissant le programme, en portant une attention particulière à la gestion et à l'évaluation du risque, à la gestion du devoir de diligence de l'ASFC à l'égard de ses sources et au caractère suffisant de la direction et de la responsabilité ministérielle en ce qui concerne le programme.

Ministère de la Défense nationale et les Forces armées canadiennes

8. L'OSSNR a réalisé un examen du programme de gestion des sources humaines du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC), qui a vérifié si le MDN et les FAC mènent leurs activités de gestion des sources humaines de manière légale, éthique et responsable.

Examens multiministériels

9. L'OSSNR a procédé à un examen de la collaboration opérationnelle entre le CST et le SCRS. Il s'agissait du premier examen de l'OSSNR visant à évaluer l'efficacité de la collaboration en examinant les mandats respectifs et les interdictions connexes. L'examen a également satisfait à l'exigence annuelle de l'OSSNR d'examiner un aspect de la prise, par le SCRS, de mesures pour réduire les menaces (MRM) envers la sécurité du Canada, au titre de l'article 8(2) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (Loi sur l'OSSNR).

10. L'OSSNR a effectué deux examens multiministériels annuels en 2023 :

    - un examen des directives émises en lien avec la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*;
    - un examen de la divulgation de renseignements au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC).

Enquêtes sur les plaintes

11. Le secrétariat de l'OSSNR, en consultation avec les membres de l'OSSNR, a établi des normes de service pour les enquêtes sur les plaintes et a fixé comme objectif d'effectuer 90 % de ces enquêtes dans le respect des normes de service. L'engagement appuie les enquêtes sur les plaintes de l'OSSNR en assurant de prompts résultats. L'OSSNR a également mis en œuvre un

processus de vérification indépendant pour les plaintes contre le CST. En outre, l'Office a mené une étude sur la collecte de données fondées sur la race et d'autres données démographiques.

12. L'OSSNR a observé une augmentation des plaintes contre le SCRS, dans le cadre de l'article 16 de la Loi sur l'OSSNR, alléguant des retards dans le processus de filtrage de sécurité de demandes d'immigration ou de citoyenneté.

01 //

Introduction

1.1 Mandat

13. L'OSSNR est un organisme indépendant qui relève du Parlement et qui a le pouvoir d'examiner de manière intégrée toutes les activités en matière de sécurité nationale et de renseignement du gouvernement du Canada, ce qui confère au Canada l'un des systèmes d'examen indépendant de la sécurité nationale les plus complets au monde. L'OSSNR a le double mandat de mener des examens et des enquêtes sur des plaintes en rapport avec les activités en matière de sécurité nationale ou de renseignement du Canada. Dans l'exécution de son mandat, l'OSSNR est appuyé par un secrétariat dirigé par un directeur général.

Examens

14. Le mandat de l'OSSNR en matière d'examen est vaste, comme le stipule le paragraphe 8(1) de la Loi sur l'OSSNR.[1] Il comprend l'examen des activités du SCRS, du CST, ainsi que des activités liées à la sécurité nationale ou au renseignement de tous les autres ministères et organismes fédéraux. [2] L'OSSNR peut également examiner toute question liée à la sécurité nationale ou au renseignement qu'un ministre de la Couronne lui soumet.[3]

Enquêtes

15. L'OSSNR a la responsabilité d'enquêter sur les plaintes liées à la sécurité nationale ou au renseignement. Cette responsabilité est énoncée à l'alinéa 8(1)d) de la Loi sur l'OSSNR et consiste à enquêter sur :

    - les plaintes concernant les activités du SCRS ou du CST;

---

[1] La Loi sur l'OSSNR (L.C. 2019, ch. 13, art. 2) se trouve au https://laws-lois.justice.gc.ca/fra/lois/n-16.62/page-1.html.
[2] Une liste complète des abréviations utilisées dans le présent rapport se trouve à l'annexe A.
[3] De plus amples renseignements sur le mandat de l'OSSNR, y compris les rapports annuels précédents, se trouvent au https://nsira-ossnr.gc.ca.

- les plaintes qui lui sont soumises par la Commission civile d'examen et de traitement des plaintes (CCETP)[4] et qui portent sur la conduite de membres de la Gendarmerie royale du Canada (GRC), lorsqu'elles concernent la sécurité nationale;

- les plaintes liées aux décisions de refuser ou de révoquer certaines habilitations de sécurité du gouvernement fédéral;

- les questions relatives à la *Loi canadienne sur les droits de la personne* qui lui sont renvoyées;

- les rapports ministériels liés à la *Loi sur la citoyenneté* qui recommandent de refuser certaines demandes de citoyenneté.

[4] Le mécanisme de traitement des plaintes de la GRC est décrit au https://www.crcc-ccetp.gc.ca/fr.

02 //

Les cinq premières années de l'OSSNR

Une nouvelle ère de responsabilité en matière de sécurité et de renseignement au Canada

16. La conversation sur les enjeux de sécurité nationale et de renseignement évolue au Canada. Au cours des dernières années, des conflits armés, la pandémie de la COVID-19 et des activités d'organismes de sécurité et de renseignement étrangers et nationaux ont fait la une des nouvelles. Plus récemment, le parlement a débattu le rôle des organismes canadiens de sécurité et de renseignement dans la réaction à la menace de l'ingérence politique étrangère. L'importance d'une surveillance et d'examens rigoureux n'a jamais été aussi évidente et opportune. Alors que la conversation se poursuit, les Canadiens voudront obtenir plus d'information sur le fonctionnement de leurs systèmes de sécurité et de renseignement. L'OSSNR est les yeux et les oreilles de confiance des Canadiens et offre ainsi une transparence qui n'existait pas auparavant.

17. L'OSSNR a pour mandat d'examiner les enjeux et de mener des enquêtes sur les plaintes liées aux activités de sécurité nationale ou de renseignement du Canada. Avant la création de l'OSSNR, certaines activités pouvaient faire l'objet d'un examen, mais il n'existait aucun organisme unique ayant le mandat et le pouvoir d'examiner les activités de l'ensemble du secteur de la sécurité nationale et du renseignement, et certains ministères ne disposaient pas d'un organe d'examen indépendant.

18. Le cadre cloisonné limitait la capacité des prédécesseurs de l'OSSNR, le Comité de surveillance des activités de renseignement de sécurité (CSARS) et le Bureau du commissaire du Centre de la sécurité des télécommunications, de mener des examens et d'enquêter sur les plaintes en raison de leurs mandats restreints. Par exemple, les examens ne permettaient pas de suivre la progression d'un problème dans les divers ministères.

Un mandat unique

19. Le large mandat de l'OSSNR est unique en son genre au sein de la communauté internationale. Il permet de mieux comprendre la façon dont les ministères et les organismes travaillent et interagissent dans le domaine de la sécurité nationale et du renseignement. Par exemple, en 2023, l'OSSNR a entamé un examen de la diffusion du renseignement sur l'ingérence étrangère en mettant l'accent sur le parcours du renseignement à partir des ministères chargés de recueillir les renseignements jusqu'aux consommateurs finaux. Un tel examen était impossible pour les prédécesseurs limités de l'OSSNR.

20. À ce jour, les examens de l'OSSNR ont porté sur 19 ministères et organismes. Le mandat élargi d'enquête sur les plaintes comprend celles soumises contre le SCRS, le CST et, sur renvoi, celles de la CCETP concernant la GRC et la Commission canadienne sur les droits de la personne (CCDP). Le travail de l'OSSNR est au cœur du fonctionnement des activités de sécurité nationale et de renseignement, ce qui permet de formuler des recommandations précises et efficaces.

Établir des processus pour viser l'excellence à partir de zéro

21. L'OSSNR a accordé la priorité à la professionnalisation de la conduite de ses examens en élaborant des politiques et des procédures pour appuyer le processus d'examen. Celles-ci ont été créées alors que l'Office évoluait et se consacrait à l'exécution de son mandat complexe et tout au long de la pandémie de la COVID-19.

22. L'OSSNR a aussi modernisé ses politiques et procédures relatives aux enquêtes sur les plaintes. L'OSSNR a entrepris une importante refonte de son processus d'enquête et a publié de nouvelles *Règles de procédure* pour remplacer le modèle précédent, en vue d'accroître la transparence procédurale pour tous ceux participant au processus de plainte. Lorsque la pandémie de la COVID-19 a rendu impossibles les audiences en personne, l'OSSNR s'est adapté et a présenté d'autres solutions, comme la tenue d'entrevues d'enquête par vidéoconférence, assurant ainsi l'accès des participants.

23. L'OSSNR a mis sur pied une pratique de divulgation proactive et publie ses rapports sur son site Web. L'Office a également entrepris de publier, dans la mesure du possible, les rapports préparés par le CSARS. L'objectif est de rendre les examens de l'OSSNR, ainsi que les conclusions et les recommandations, accessibles au public dès que possible. La divulgation proactive accroît la transparence et enrichit le dialogue sur la sécurité nationale et le renseignement au Canada.

Habiliter les professionnels

24. Le secrétariat compte maintenant près de 100 employés à temps plein. Le plus important atout de l'OSSNR est son personnel, et le secrétariat continue d'attirer des employés possédant une expertise diversifiée en matière de recherche, d'examen, de technologie et de droit. Cette expertise a permis à l'OSSNR de mener divers examens et de créer un modèle d'enquête professionnel pour traiter les plaintes.

25. L'OSSNR s'est efforcé de favoriser une culture unique et continue d'innover dans sa façon de gérer son processus d'examen. Les équipes d'examen sont composées de personnes aux compétences variées qui appuient le besoin d'avoir une expertise juridique et technique. Les équipes sont chargées d'effectuer les examens sous la direction des membres de l'OSSNR et avec l'orientation et le soutien de la direction du secrétariat. Cela permet de mener des examens détaillés et audacieux.

26. De même, le modèle d'enquête sur les plaintes de l'OSSNR est maintenant conçu pour que les membres reçoivent le soutien d'un personnel composé d'experts en matière juridiques, de registres et de recherche. Ce soutien améliore l'efficacité des membres en les appuyant dans leur rôle décisionnel dans le cadre des enquêtes.

Le défi d'un examen plus efficace

27. La mission de l'OSSNR consiste à être les yeux et les oreilles de la population canadienne en jouant le rôle d'organisme de surveillance indépendant chargé d'examiner les activités du gouvernement du Canada en matière de sécurité nationale et de renseignement et d'enquêter sur ces dernières. Pour accomplir sa mission, l'OSSNR doit choisir les examens appropriés et avoir accès aux renseignements requis.

28. La Loi sur l'OSSNR l'oblige à effectuer certains examens annuels, mais elle permet également à l'Office de choisir les sujets à examiner. Ce pouvoir discrétionnaire est fondamental, puisque l'OSSNR doit être en mesure de « suivre le fil » pour s'assurer que les activités qui méritent un examen minutieux sont examinées de façon indépendante. Plus précisément, l'OSSNR a élaboré une matrice de planification et d'examen qui comprend des critères officiels qui aident à cerner les sujets d'examen conformément au mandat et à la mission de l'OSSNR. L'établissement des priorités des examens est fondé sur d'autres facteurs stratégiques, y compris les évaluations de la nature de l'activité et du risque en matière de conformité qu'elle représente, de la nouveauté de l'activité et des technologies qu'elle utilise, ainsi que des ressources, des examens en cours et de l'intérêt public.

29. L'accès à l'information est la pierre angulaire des examens, et l'OSSNR continue d'insister sur ses droits d'accès. Un examen efficace exige des réponses rapides et complètes aux demandes d'information de l'OSSNR, des séances d'information ouvertes et franches, ainsi qu'un respect mutuel. Malgré l'accès inconditionnel accordé à l'Office au titre de la Loi sur l'OSSNR, il n'est pas toujours simple de résoudre les problèmes d'accès. Il y a eu une courbe d'apprentissage, tant pour les entités examinées que pour l'OSSNR, et l'amélioration de la littératie en matière d'examen au sein des ministères et organismes visés par le mandat d'examen de l'OSSNR est une priorité permanente.

Réussites du mandat de l'OSSNR

30. L'incidence du travail de l'OSSNR sur la communauté de sécurité nationale et de renseignement va au-delà des ministères examinés. Récemment, la Cour fédérale s'est servie d'un rapport de l'OSSNR pour éclairer le contexte et l'analyse d'une décision sur une affaire touchant un mandat du SCRS. La Cour a jugé les enjeux cernés par l'OSSNR comme étant importants en ce qui a trait à l'échange de renseignements recueillis dans le cadre de certains mandats.

31. En outre, les ministres responsables des activités de la communauté de la sécurité et du renseignement ont reconnu la valeur d'un examen indépendant et ont renvoyé des enjeux à l'OSSNR. Le premier de ces examens découle d'un jugement de la Cour fédérale. [5] Les ministres de la Sécurité publique et de la Justice ont renvoyé la question à l'OSSNR. Le rapport de l'OSSNR a présenté des conclusions et des recommandations sur la prestation de conseils juridiques par le ministère de la Justice, sur la gestion du processus d'acquisition de mandats par le SCRS et le ministère de la Justice, ainsi que sur des questions culturelles et de gouvernance plus vastes.

32. Depuis 2019, l'OSSNR a effectué 39 examens (13 examens prévus par la loi et 26 examens discrétionnaires)[6]. Parmi ceux-ci, 21 examens concernaient plus d'un ministère. L'OSSNR a également communiqué 17 rapports de conformité aux ministres responsables, comme l'exige l'article 35 de la Loi sur l'OSSNR. Ces rapports sont rédigés lorsque l'Office juge qu'une activité

[5] Il s'agissait d'un jugement exigeant un examen externe exhaustif visant à cerner pleinement les lacunes et les défaillances systémiques, culturelles et en matière de gouvernance qui ont mené le SCRS à mener une activité opérationnelle qui a finalement été considérée comme illégale et un manquement à l'obligation de franchise.

[6] Comprend les examens dont les rapports finaux sont approuvés par les membres de l'OSSNR et envoyés aux ministres concernés. Ne comprend pas les rapports annuels classifiés envoyés au ministre de la Défense nationale et au ministre de la Sécurité publique, ni d'autres activités d'examen.

pourrait ne pas être conforme à la loi.[7] Les enjeux de conformité peuvent comprendre, par exemple, un ministère qui n'a pas respecté un délai prescrit ou une infraction potentielle à la *Charte canadienne des droits et libertés* (« la Charte »). Les rapports de l'OSSNR ont inclus plus de 200 recommandations, allant de modifications précises à des processus à de vastes réformes structurelles. L'OSSNR a également reçu plus de 200 plaintes, ce qui souligne l'importance d'un processus d'enquête indépendant accessible pour traiter les plaintes concernant les activités du SCRS, du CST et la GRC.

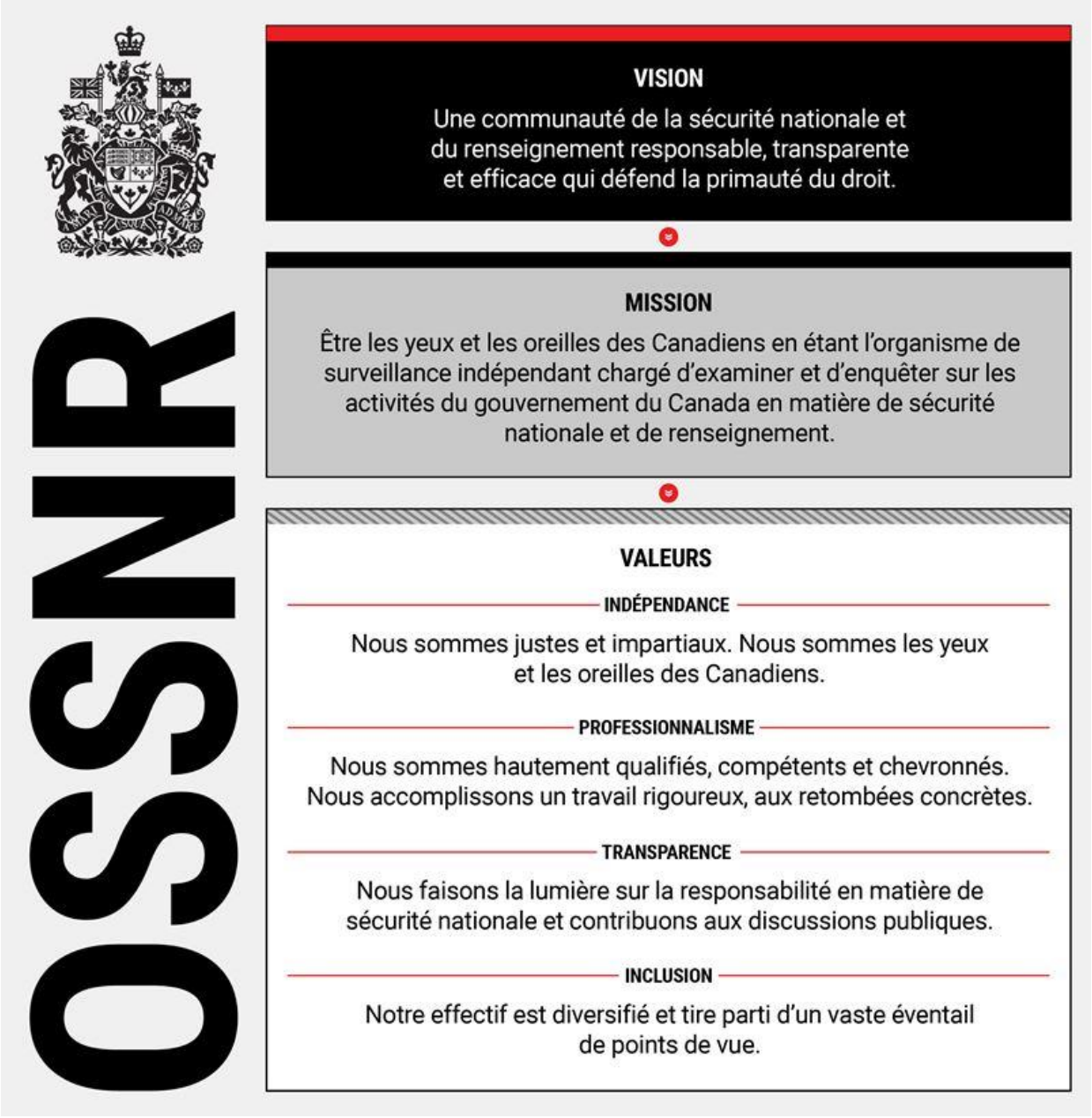
Regard vers l'avenir

33. En ce qui concerne son avenir, l'OSSNR se concentrera également sur son propre fonctionnement, pour s'assurer que sa structure et sa gouvernance sont adaptées à ses besoins. Le prochain examen législatif de la Loi sur l'OSSNR donnera l'occasion d'apporter des améliorations nécessaires.

34. L'OSSNR est extrêmement fier d'avoir contribué à l'examen minutieux et à la transparence des activités de sécurité et de renseignement du Canada au cours de ses cinq premières années. L'OSSNR a joué un rôle essentiel en vue d'assurer la responsabilité impartiale des organisations qui participent aux activités de sécurité et de renseignement du Canada. L'OSSNR envisage son avenir avec enthousiasme et un dévouement renouvelé envers sa mission. Récemment, l'OSSNR a codifié son approche en officialisant sa vision, sa mission et ses valeurs, et bien que ces déclarations officielles soient nouvelles, ce sont les mêmes éléments sous-jacents sur lesquels l'Office se fonde depuis ses débuts.

[7] De plus amples renseignements sur les rapports de l'OSSNR en application de l'article 35 se trouvent à l'adresse suivante : https://nsira-ossnr.gc.ca/fr/examens/policies-and-procedures/application-par-loffice-des-articles-35-et-40-de-la-loi-sur-lossnr/.

Mission, vision et valeurs de l'OSSNR



03 //

Valeur des partenariats élargis

Élargir les partenariats et la coopération à l'international

35. Les partenariats internationaux des prédécesseurs de l'OSSNR étaient principalement établis par l'entremise du Conseil de surveillance et d'examen du renseignement du Groupe des cinq (CSERGC)[8], qui continue d'être une alliance fondamentale pour l'OSSNR. En plus de renforcer les relations héritées de ses prédécesseurs, l'OSSNR a créé de nouveaux partenariats avec des homologues étrangers et a participé activement à des forums internationaux. En 2023 seulement, l'OSSNR a collaboré avec les organisations suivantes et a participé aux événements suivants :

Organisations :

- Inspecteur général du renseignement et de la sécurité de l'Australie (IGIS Australie)
- Inspecteur général du renseignement et de la sécurité de la Nouvelle-Zélande (IGIS Nouvelle-Zélande)
- Inspecteur général de la communauté du renseignement des États-Unis d'Amérique (IC IG É.-U.)
- Bureau du commissaire aux pouvoirs d'enquête du Royaume-Uni (IPCO R.-U.)
- Direction exécutive du Comité contre le terrorisme (DECT) des Nations Unies
- Conseil de surveillance de la vie privée et des libertés civiles des États-Unis (PCLOB É.-U.)
- Commission parlementaire norvégienne de contrôle des services de renseignement et de sécurité (EOS Norvège)
- Conseil danois de surveillance des services de renseignement (TET Danemark)
- Autorité de surveillance indépendante des activités de renseignement de la Suisse (AS-Rens)
- Comité de surveillance parlementaire de l'Allemagne (PKGr)
- Commission néerlandaise de contrôle des services de renseignement et de sécurité (CTIVD Pays-Bas)

Événements et forums :

- Conférence du Conseil de surveillance et d'examen du renseignement du Groupe des cinq
- Forum international de la surveillance du renseignement
- Conférence européenne de la surveillance du renseignement

[8] Le CSERGC comprend des organismes qui ont un mandat de surveillance et d'examen en matière d'activités de sécurité nationale dans leur pays respectif (Canada, Australie, Nouvelle-Zélande, Royaume-Uni et États-Unis).

Leçons tirées et leçons échangées avec les partenaires internationaux

36. La collaboration avec les homologues internationaux et la participation à des discussions multilatérales ont permis à l'OSSNR de tirer parti d'un réseau de partenaires. Le réseau favorise l'échange de renseignements pertinents au sujet de pratiques exemplaires, de méthodologies, d'avancées récentes et d'enjeux communs. L'échange de renseignements et la coopération dans le domaine traditionnellement abstrait et isolé de la surveillance de la sécurité nationale ont élargi les perspectives de l'OSSNR et orienté ses attentes en ce qui concerne les ministères et les organismes surveillés.

37. L'OSSNR a constaté que ses partenaires internationaux ont déjà fait face et, dans certains cas, surmonté bon nombre des défis auxquels l'Office fait face. Il s'agit notamment de défis de nature opérationnelle, comme des tactiques d'acquisition et de vérification de l'information, ainsi que ceux liés au secrétariat de l'OSSNR, comme le recrutement, la formation et le maintien en poste du personnel. L'utilisation des leçons apprises par nos homologues internationaux a accéléré le progrès de l'OSSNR et a appuyé sa réputation croissante à titre d'exemple dans le domaine de la surveillance de la sécurité nationale et du renseignement.

38. Bien que l'OSSNR soit un consommateur vorace de pratiques exemplaires, l'Office est un contributeur tout aussi actif. L'OSSNR a également fait part de ses propres approches, processus et méthodes uniques à la communauté de surveillance, ce qui a parfois amené des organisations partenaires à suivre l'exemple de l'OSSNR et à adopter ses pratiques. Même lorsque l'OSSNR n'est pas confronté à un problème particulier, des partenaires qui reconnaissent la richesse de son expérience et sa réputation pour l'innovation demandent son point de vue et appliquent ses suggestions.

39. Des engagements continus et répétés auprès de partenaires internationaux ont permis à des relations de travail de prendre racine, de s'épanouir et de porter fruit sous forme de discussions régulières et d'échanges occasionnels selon les besoins de dossiers précis. La réduction des obstacles institutionnels a favorisé l'échange d'expertises et une incidence plus directe sur le travail de fond de chaque organisme et a produit des résultats plus tangibles, comme il est décrit dans les exemples ci-dessous.

Exemples de la valeur obtenue grâce aux engagements

<u>Avantages pour l'OSSNR</u>

- Dans le cadre d'une affectation prolongée à l'OSSNR, un expert en communications de l'IPCO du Royaume-Uni a dirigé une évaluation globale de la position actuelle de l'Office

en matière de communications et a joué un rôle important dans l'élaboration d'une nouvelle stratégie de communication. La mise en œuvre de cette stratégie a aidé l'OSSNR à communiquer avec des intervenants nationaux et à tisser des liens avec eux. Les membres et le personnel du secrétariat de l'OSSNR sont très reconnaissants des contributions de l'expert au cours de son passage à l'Office.

- Le TET Danemark et le EOS Norvège ont joué un rôle important dans l'élaboration et la mise en œuvre d'une inspection pour un nouveau système informatique, laquelle a été utilisée pour la première fois dans le cadre de l'examen du cycle de vie de l'information autorisée par mandat du SCRS mené par l'OSSNR. Ils ont également contribué à l'analyse comparative du fonctionnement et du rendement utilisée par l'OSSNR dans ses méthodologies, ses pratiques communes et ses critères d'évaluation.
- L'OSSNR a consulté l'inspecteur général des États-Unis en vue d'améliorer la réceptivité des ministères et organisations examinés à ses recommandations. L'OSSNR a commencé à adopter des pratiques exemplaires pour veiller à ce qu'il y ait un suivi des recommandations formulées.

Contributions de l'OSSNR

- Lors d'un événement organisé par Affaires mondiales Canada (AMC) dans le cadre de la collaboration entre le Canada et la Direction exécutive du Comité contre le terrorisme (DECT) des Nations Unies, l'OSSNR a fait une présentation à la délégation de la DECT dans le but d'expliquer le rôle de l'examen indépendant dans l'évaluation de la légalité des activités canadiennes dans le domaine de la lutte contre le terrorisme. Cette présentation a montré aux évaluateurs internationaux comment le modèle canadien a mis en place des mécanismes indépendants robustes pour l'examen de lutte contre le terrorisme qui touchent les services d'application de la loi et du renseignement.
- La matrice d'examen de l'OSSNR a été communiquée à l'IGIS Nouvelle-Zélande et au TET Danemark, ainsi qu'à de nombreux autres partenaires internationaux. Après leur visite à l'OSSNR, le TET Danemark a mis à jour ses normes en matière de technologies de l'information (TI) pour y inclure des étapes d'assurance de la qualité et a ajouté des facteurs à son cadre d'évaluation des risques.

Une collaboration accrue mène à une meilleure responsabilisation

40. Tout comme les organismes de sécurité et de renseignement coopèrent et échangent régulièrement de l'information avec des partenaires internationaux, les organes qui les supervisent doivent également collaborer. La collaboration entre l'OSSNR et ses homologues

étrangers a produit, et continue de produire, des avantages mutuels pour toutes les parties concernées. Par conséquent, l'OSSNR est devenu une organisation plus compétente, avec une meilleure visibilité dans la communauté transnationale de la sécurité et du renseignement, assurant ainsi une responsabilisation efficace et exhaustive des appareils de sécurité nationale du Canada.

41. Au sein de la communauté canadienne d'examen et de surveillance, l'OSSNR apporte un point de vue distinct et apprécié et remplit un espace auparavant inoccupé dans cet important réseau. Par conséquent, les efforts de l'OSSNR viennent compléter les activités de ses pairs. En 2023, l'OSSNR a rencontré de nombreux agents du Parlement, y compris la vérificatrice générale du Canada, la commissaire à l'intégrité du secteur public et le commissaire à la protection de la vie privée. L'expérience institutionnelle fondée sur de nombreuses décennies et la maturité de ces agents et de leur bureau respectif se sont révélées inestimables pour l'OSSNR. L'échange de pratiques exemplaires a été extrêmement utile, particulièrement dans le perfectionnement de la capacité de communication du secrétariat.

42. Comme prévu dans la Loi sur l'OSSNR, celui-ci collabore avec d'autres organes de surveillance pour résoudre des problèmes d'intérêt mutuel. Par exemple, en 2023, l'OSSNR et le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) ont tous deux mené des examens sur la question de l'ingérence politique étrangère. Tout en maintenant son indépendance, l'OSSNR a coordonné son examen avec le CPSNR afin d'éviter tout dédoublement inutile du travail.

04 //

Examens

4.1 Aperçu

43. En plus de ses examens annuels, l'OSSNR a continué d'effectuer des examens discrétionnaires qu'il jugeait pertinents et appropriés dans le cadre de son mandat. Notamment, l'examen de l'OSSNR sur la diffusion du renseignement ayant trait à l'ingérence politique étrangère exercée par la République populaire de Chine de 2018 à 2023. L'OSSNR a examiné le flux du renseignement au sein du gouvernement, des collecteurs aux consommateurs, y compris les hauts fonctionnaires et les représentants élus. Cela a consisté à examiner attentivement les processus internes pour voir la façon dont les renseignements recueillis ont été communiqués et transmis aux décideurs concernés. L'OSSNR a déterminé qu'il était dans l'intérêt public de publier un rapport sur ce sujet et a rédigé son premier rapport spécial au titre de l'article 40 de la Loi sur l'OSSNR. Le rapport a été déposé devant les deux Chambres du Parlement en mai 2024.

44. Le tableau 1 présente tous les examens en cours en 2023. Cela comprend les examens annuels prévus par la loi, les examens discrétionnaires et les examens annuels des activités du CST et du SCRS. Des résumés généraux du contenu et des résultats des examens terminés avant la fin de l'année civile sont présentés dans les sections suivantes; les conclusions et recommandations complètes se trouvent à l'annexe B. L'OSSNR rend publiques des versions complètes de chaque examen après qu'elles ont été expurgées pour être rendues publiques.

Tableau 1. Activités d'examen de l'OSSNR en 2023

Examen	Ministère(s)/organisation(s)	État*
Rapport annuel au ministre de la Défense nationale sur les activités du CST en 2022	CST	Terminé
Rapport annuel au ministre de la Défense nationale sur les activités du SCRS en 2022	SCRS	Terminé
Examen des communications d'information par les institutions fédérales au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* en 2022	Sécurité publique Canada (SP), CST, SCRS, AMC, GRC, ASFC et Immigration, Réfugiés et Citoyenneté Canada (IRCC)	Terminé

Examen	Ministère(s)/organisation(s)	État*
Examen des solutions réseau du CST et des activités connexes liées à la cybersécurité et à l'assurance de l'information	CST et SPC	Terminé
Examen de l'OSSNR portant sur le régime applicable aux ensembles de données du SCRS	SCRS	Terminé
Examen du programme de gestion des sources humaines du ministère de la Défense nationale et des Forces armées canadiennes	MDN/FAC	Terminé
Examen de la collaboration opérationnelle entre le CST et le SCRS	CST et SCRS	Terminé
Examen du programme des sources humaines confidentielles de l'ASFC	ASFC	Terminé
Examen de la mise en œuvre par les ministères de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* en 2022	ASFA, Agence du revenu du Canada (ARC), CST, SCRS, ministère des Pêches et des Océans (MPO), MDN/FAC, Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), AMC, IRCC, SP, GRC et Transports Canada (TC)	Terminé
Utilisation par le CST du polygraphe dans le processus de filtrage de sécurité	CST et SCT	Terminé
Examen de la diffusion du renseignement ayant trait à l'ingérence politique étrangère exercée par la République populaire de Chine de 2018 à 2023	SCRS, GRC, AMC, CST, SP et Bureau du Conseil Privé (BCP)	Terminé
Examen des mécanismes de responsabilisation de SP et du SCRS	SCRS, AMC, SP, Ministère de la Justice du Canada	Terminé
Examen du cycle de vie de l'information autorisée par mandat du SCRS	SCRS	Terminé
Examen du Programme des sources humaines de la GRC	GRC	Terminé
Examen des communications d'information par les institutions fédérales au titre de *la Loi sur la*	SP, CST, SCRS, AMC, GRC, ASFC et IRCC	En cours

Examen	Ministère(s)/organisation(s)	État*
communication d'information ayant trait à la sécurité du Canada en 2023		
Examen du processus de partage des vulnérabilités du CST	CST, SCRS et GRC	En cours
Examen de la Division de la recherche et de l'analyse (DRA) de l'ARC	ARC	En cours

*État au moment de l'écriture du présent rapport. La mention « terminé » signifie que le rapport d'examen a été approuvé par les membres de l'OSSNR. Certains examens indiqués comme étant « en cours » peuvent avoir été terminés depuis la rédaction du présent rapport et peuvent être accessibles sur le site Web de l'OSSNR.

4.2 Examens du Service canadien du renseignement de sécurité

Aperçu

45. L'OSSNR a le mandat d'examiner toutes les activités du SCRS. La Loi sur L'OSSNR exige que l'Office présente chaque année un rapport sur les activités du SCRS au ministre de la Sécurité publique et de la Protection civile[9]. Ces rapports sont classifiés et comprennent des renseignements relatifs au respect par le SCRS de la loi et des directives ministérielles applicables, ainsi qu'au caractère raisonnable et à la nécessité de l'exercice des pouvoirs du SCRS.

46. En 2023, l'OSSNR a effectué un examen dédié au SCRS en plus de son examen annuel des activités de l'organisation; les deux sont résumés ci-dessous. De plus, le SCRS fait l'objet d'autres examens multiministériels de l'OSSNR, comme l'examen de la collaboration opérationnelle entre le CST et le SCRS, ainsi que les examens annuels prévus par la loi concernant la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, dont les résultats sont décrits à la section 4.5, Examens multiministériels.

[9] Puisque les responsabilités sont maintenant divisées en deux portefeuilles, l'OSSNR présente ses rapports au ministre de la Sécurité publique.

Examen de l'OSSNR portant sur le régime applicable aux ensembles de données du SCRS

47. En juillet 2019, le régime applicable aux ensembles de données est entré en vigueur dans le cadre de la *Loi de 2017 sur la sécurité nationale*, ce qui a donné lieu à la création des articles 11.01 à 11.25 de la *Loi sur le Service canadien du renseignement de sécurité* (Loi sur le SCRS). Le régime permet au SCRS de recueillir et de conserver des ensembles de données contenant des renseignements personnels qui, dans l'immédiat, ne sont pas directement liés à des menaces, mais qui sont susceptibles d'appuyer des enquêtes sur la sécurité nationale.

48. L'OSSNR a examiné la mise en œuvre du régime, y compris les aspects de la gouvernance, de la gestion de l'information, des pratiques de conservation et de la formation. L'OSSNR a relevé des problèmes de conformité qui touchaient à tous les aspects du régime à l'étude. Entre autres, l'OSSNR a constaté que l'application actuelle du régime applicable aux ensembles de données par le SCRS ne se conformait pas au cadre législatif. L'OSSNR a également relevé plusieurs problèmes de conformité quant à la façon dont le SCRS a mis en œuvre le régime, y compris en ce qui concerne la conservation de renseignements personnels de Canadiens et d'étrangers sans les autorisations et approbations requises par la loi.

49. L'examen a permis de conclure que le SCRS n'avait pas mis en œuvre adéquatement son régime applicable aux ensembles de données. Le SCRS n'a pas cherché à clarifier les ambiguïtés juridiques de l'application du régime auprès de la Cour fédérale, même lorsque l'occasion de le faire s'est présentée. Le SCRS a pris différentes positions quant à son application du régime et risque maintenant de limiter ce qui se veut un régime de collecte et de conservation à un mécanisme de conservation seulement. À l'interne, le SCRS n'a pas consacré suffisamment de ressources et de formation pour assurer la conformité au régime. Il est impossible de mettre en œuvre un nouveau régime juridique, peu importe sa pertinence, sans s'engager à fournir les ressources requises et à appuyer la mise en œuvre.

Examen annuel des activités du Service canadien du renseignement de sécurité

50. L'OSSNR a effectué son examen annuel des activités du SCRS, lequel porte sur un vaste éventail d'activités envisagées et entreprises entre le 1er janvier et le 31 décembre 2023. L'examen a mis en évidence les défis en matière de conformité auxquels le SCRS a été confronté, a permis à l'OSSNR de continuer à surveiller les tendances actuelles et a relevé de nouveaux enjeux relatifs à l'exercice des pouvoirs du SCRS. Les renseignements obtenus tout

au long de l'examen, y compris ceux que le SCRS est tenu de fournir à l'OSSNR au titre de la Loi sur le SCRS, ont été utilisés dans le rapport annuel au ministre de la Sécurité publique sur les activités du SCRS, ainsi que pour orienter les examens en cours de l'OSSNR et la planification interne des examens à venir.

Statistiques et données

51. Pour assurer une responsabilisation accrue envers le public, l'OSSNR a demandé au SCRS de publier des statistiques et des données sur les aspects de ses activités liées à la conformité et l'intérêt public. L'OSSNR est d'avis que ces statistiques fourniront au public des informations quant à la portée et à l'étendue des activités du SCRS, et indiqueront l'évolution des activités d'une année à l'autre.

Demandes de mandats

52. L'article 21 de la Loi sur le SCRS autorise le SCRS à demander à un juge de décerner un mandat s'il a des motifs raisonnables de croire que l'utilisation de pouvoirs plus intrusifs est nécessaire pour faire enquête sur une menace particulière envers la sécurité du Canada. Le SCRS peut avoir recours à des mandats, par exemple, pour intercepter des communications, entrer dans un lieu ou obtenir des renseignements, des dossiers ou des documents. Chaque demande de mandat peut viser plusieurs personnes ou demande l'utilisation de plusieurs pouvoirs intrusifs.

Tableau 2 : Demandes de mandats présentées par le SCRS au titre de l'article 21, 2018-2023

Demandes	2018	2019	2020	2021	2022*	2023
Total des demandes soumises au titre de l'article 21	24	24	15	31	28	30
Total des mandats approuvés	24	23	15	31	28	30
Nouveaux mandats	10	9	2	13	6	9
Remplacements	11	12	8	14	14	10
Mandats additionnels	3	2	5	4	8	11

Total des mandats refusés	0	1	0	0	0	0

*Les demandes présentées par le SCRS à la Cour fédérale en 2022 ont donné lieu à l'approbation et à l'émission de 194 autorités judiciaires, y compris 164 mandats et 28 ordonnances d'assistance délivrés au titre des articles 12, 16 et 21 de la Loi sur le SCRS, ainsi que deux autorisations judiciaires émises au titre de l'article 11.13 de la même loi. Chaque demande est soumise à un processus de production et d'examen approfondi qui comprend un examen par un conseiller indépendant du ministère de la Justice et une évaluation par un comité composé de cadres du SCRS, de SP, du CST et de la GRC (le cas échéant) avant que l'approbation ministérielle soit demandée. Un certain nombre de mandats délivrés pendant cette période illustrent l'élaboration de nouvelles autorités et techniques de collecte novatrices, qui ont exigé une collaboration étroite entre les collecteurs, les opérateurs de technologie, les analystes de politique et les conseillers juridiques.

Mesures de réduction de la menace

53. Le SCRS est autorisé à demander un mandat judiciaire pour une MRM s'il croit que certaines mesures intrusives, décrites au paragraphe 21(1.1) de la Loi sur le SCRS, sont nécessaires pour réduire la menace. La Loi sur le SCRS indique clairement que si une MRM proposée limite un droit ou une liberté protégés par la *Charte canadienne des droits et libertés* ou est contraire aux lois canadiennes, un mandat judiciaire autorisant la mesure est nécessaire. À ce jour, le SCRS n'a demandé aucune autorisation judiciaire pour entreprendre des MRM dans le cadre d'un mandat. Les MRM approuvées au cours d'une année peuvent être exécutées au cours des années suivantes. Des motifs opérationnels peuvent également empêcher l'exécution d'une MRM approuvée.

Tableau 3 : Nombre total de mesures de réduction de la menace approuvées et exécutées, 2015-2023

Mesures de réduction de la menace	2015	2016	2017	2018	2019	2020	2021	2022	2023
Approuvées	10	8	15	23	24	11	23	16	14
Exécutées	10	8	13	17	19	8	17	12	19
Avec mandat	0	0	0	0	0	0	0	0	0

Cibles du Service canadien du renseignement de sécurité

54. Le SCRS a pour mandat d'enquêter sur les menaces à la sécurité du Canada, y compris l'espionnage, les activités influencées par l'étranger, la violence politique, religieuse ou

idéologique et la subversion.[10] Des critères permettant au SCRS de mener des enquêtes sur une personne, un groupe ou une entité pour des questions liées à ces menaces sont établis à l'article 12 de la Loi sur le SCRS. Les entités faisant l'objet d'une enquête du SCRS, qu'il s'agisse de personnes ou de groupes, sont appelées des « cibles ».[11]

Tableau 4 : Nombre de cibles du SCRS, 2018–2023

Cibles	2018	2019	2020	2021	2022	2023
Nombre de cibles	430	467	360	352	340	323

Ensembles de données

55. L'analyse de données constitue l'un des principaux outils d'enquête du SCRS. Cet outil lui permet d'établir des liens et de cerner des tendances, ce qui ne serait pas possible avec des méthodes d'enquête traditionnelles. La Loi sur la sécurité nationale de 2017 a accordé au SCRS de nouveaux pouvoirs, notamment un cadre juridique pour la collecte, la conservation et l'utilisation d'ensembles de données par le SCRS. Ce cadre autorise le SCRS à recueillir des ensembles de données (subdivisés en ensembles de données canadiens, étrangers et accessibles au public) qui peuvent aider le SCRS à exercer ses fonctions. Le cadre établit également des mesures de protection des droits et libertés des Canadiens, notamment la protection des renseignements personnels. Ces mesures de protection comprennent des exigences accrues en matière de responsabilisation ministérielle. Le SCRS doit satisfaire à différentes exigences avant de pouvoir utiliser certains types d'ensemble de données.[12]

56. Selon la Loi sur le SCRS, l'OSSNR doit également être tenu au courant de certaines activités liées aux ensembles de données. Des rapports préparés à la suite du traitement d'ensembles de données doivent être fournis à l'OSSNR, sous certaines conditions et dans des délais raisonnables. Même si le SCRS n'est pas tenu d'informer l'OSSNR des autorisations judiciaires ou des approbations ministérielles pour la collecte d'ensembles de données canadiens et étrangers, il a tenu l'OSSNR au courant de ces activités de façon proactive.

---

[10] L'article 2 de la Loi sur le SCRS définit les « menaces à la sécurité nationale ».
[11] Voir le *Rapport sur les événements concernant Maher Arar*, Les faits volume I, note 10.
[12] Modifications apportées à la Loi sur le SCRS – Analytique des données, Document d'information, SCRS (18 juillet 2020).

Tableau 5 : Évaluation et conservation d'ensembles de données accessibles au public, d'ensembles de données canadiens et d'ensembles de données étrangers par le SCRS, 2019–2023

Types d'ensembles de données	2019	2020	2021	2022	2023
Accessibles au public					
Évalués	9	6	4	4	2
Conservés	9	6	2[a]	4	2
Canadiens					
Évalués	0	0	2	0	1
Conservés (approuvés par la Cour fédérale))	0	0	0	2[b]	0
Refusés par la Cour fédérale	0	0	0	0	0
Étrangers					
Évalués	10	0	0	1	2
Conservés (approuvés par le ministre de la Sécurité publique et le commissaire au renseignement)	0	1	1[c]	1	3
Refusés par le ministre	0	0	0	0	0
Refusés par le commissaire au renseignement	0	0	0	0	0

Remarque : les statistiques présentées dans ce tableau sont à jour en date de mai 2024. Les statistiques des rapports annuels précédents ont été mises à jour pour tenir compte des nouvelles données reçues.

[a] En 2021, le SCRS a évalué quatre ensembles de données accessibles au public et en a conservé deux. Parmi les deux autres ensembles de données, il a été constaté que l'un d'entre eux avait été envoyé aux fins d'évaluation trop tard, alors il a été supprimé sans qu'aucune information ne soit conservée. Il a été déterminé que l'ensemble de données restant était de nature administrative, ce qui fait en sorte qu'il n'était pas visé par l'article 11 de la Loi sur le SCRS.

[b] Les ensembles de données recueillis et évalués en 2021 ont reçu une autorisation judiciaire et ont donc été conservés en 2022.

[c] En 2019, le SCRS a demandé l'autorisation ministérielle de conserver dix ensembles de données étrangers. Bien qu'aucun ensemble de données étranger n'ait été évalué en 2020 ou 2021, un ensemble de données

étranger a été conservé après autorisation ministérielle (par le directeur désigné) et ratification par le commissaire au renseignement, à la suite d'une demande présentée en 2019.

Cadre de justification

57. Le cadre de justification du SCRS établit une justification limitée qui autorise ses employés et les personnes agissant sous leur direction à mener des activités qui constitueraient par ailleurs des infractions aux lois canadiennes. Le cadre de justification du SCRS est inspiré des protections dont bénéficient déjà les services canadiens d'application de la loi.[13] Le cadre de justification apporte au SCRS et à la population canadienne la clarté nécessaire quant à ce que le SCRS peut faire légalement dans le cadre de ses activités. Il reconnaît qu'il est dans l'intérêt public de veiller à ce que les employés du SCRS puissent s'acquitter efficacement de leurs fonctions de collecte de renseignements, notamment par la commission d'actes et d'omissions qui seraient par ailleurs illégaux, dans l'intérêt du public et conformément à la primauté du droit. Les types d'actes et d'omissions par ailleurs illégaux qui sont autorisés par le cadre de justification sont déterminés par le ministre et approuvés par le commissaire au renseignement. Il existe des limites quant aux activités qui peuvent être réalisées, et le cadre de justification ne permet pas de commettre un acte ou une omission qui porterait atteinte à un droit ou à une liberté garantis par la Charte.

58. Selon l'article 20.1de la Loi sur le SCRS, les employés doivent être désignés par le ministre de la Sécurité publique et de la Protection civile pour être visés par le cadre de justification lorsqu'ils commettent un acte ou une omission par ailleurs illégal ou en ordonnent la commission. Les employés désignés sont des employés du SCRS qui ont besoin du cadre de justification pour exécuter leurs fonctions. Les employés désignés sont justifiés de commettre eux-mêmes un acte ou une omission (commissions par les employés) et ils peuvent ordonner à une autre personne de commettre un acte ou une omission (directives de commettre) dans le cadre de leurs fonctions.

Tableau 6 : Autorisations, commissions et directives en vertu du cadre de justification du SCRS, 2019–2023

	2019	2020	2021	2022	2023
Autorisations	49	147	178	172	172

[13] Voir https://www.canada.ca/fr/service-renseignement-securite/nouvelles/2020/06/modifications-apportees-a-la-loi-sur-le-scrs--cadre-de-justification.html.

Commissions par les employés	1	39	51	61	47
Directives de commettre	15	84	116	131	116
Désignations en situation d'urgence	0	0	0	0	0

Remarque : les statistiques présentées dans ce tableau sont à jour en date de mai 2024. Les statistiques des rapports annuels précédents ont été mises à jour pour tenir compte des nouvelles données reçues.

Conformité

59. L'unité du programme de conformité opérationnelle interne du SCRS dirige et gère la conformité globale au sein du SCRS. L'objectif de cette unité consiste à promouvoir une culture de conformité au sein du SCRS en dirigeant une approche pour signaler et évaluer les incidents potentiels de non-conformité, et à fournir aux employés des conseils et des directives en temps opportun sur les politiques et procédures internes. Ce programme constitue le centre de traitement de tous les cas de non-conformité liés aux activités opérationnelles.

60. L'OSSNR continuera de surveiller de près les cas de non-conformités canadiennes et à la Charte, et collaborera avec le SCRS pour améliorer la transparence quant à ces activités.

Tableau 7 : Nombre total d'incidents de non-conformité traités par le SCRS, 2019–2023

Incidents	2019	2020	2021	2022	2023
Incidents de non-conformité traités	53	99	85	59	79
Incidents administratifs		53	64	42	48
Incidents opérationnels[a]	40[b]	19[b]	21	17	31
Lois canadiennes	Non disponible	Non disponible	1	2	4
Charte	Non disponible	Non disponible	6	5	15
Conditions de mandats	Non disponible	Non disponible	6	3	11
Gouvernance du SCRS	Non disponible	Non disponible	8	15	27

[a] Pour 2021, chaque incident de non-conformité opérationnel a été comptabilisé en fonction de l'échelon de non-conformité (c.-à-d. qu'un incident de non-conformité à la Charte et à la gouvernance du SCRS n'est comptabilisé que dans la catégorie Charte). Pour 2022 et 2023, chaque incident est comptabilisé dans toutes les catégories dans lesquelles il y a eu non-conformité. Ainsi, la somme des incidents de non-conformité opérationnels dans les différentes catégories est plus élevée que le nombre total d'incidents de ce type.

[b] Le nombre total d'incidents de non-conformité n'a pas été ventilé en 2019 et en 2020. Ce nombre représente le nombre d'incidents de non-conformité comme celles de la Loi sur le SCRS, de la Charte, des conditions des mandats ou des procédures et politiques internes du SCRS.

4.3 Examens visant le Centre de la sécurité des télécommunications

Aperçu

61. L'OSSNR a pour mandat d'examiner toute activité menée par le Centre de la sécurité des télécommunications (CST). L'OSSNR doit également présenter au ministre de la Défense nationale un rapport annuel sur les activités du CST, portant notamment sur le respect par le

CST des lois et des directives ministérielles applicables ainsi que sur l'évaluation par l'OSSNR du caractère raisonnable et de la nécessité de l'exercice des pouvoirs du CST.

62. En 2023, l'OSSNR a effectué deux examens visant le CST et a entrepris un examen annuel des activités du CST, tous sont résumés ci-dessous. De plus, le CST fait l'objet d'autres examens multiministériels de l'OSSNR, comme l'examen de la collaboration opérationnelle entre le CST et le SCRS et les examens annuels obligatoires de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* (voir section 4.5).

Examen de l'utilisation par le CST du polygraphe pour le filtrage de sécurité

63. L'examen par l'OSSNR de l'utilisation par le CST du polygraphe pour le filtrage de sécurité a révélé que les politiques et les procédures en place au CST ne traitaient pas adéquatement les questions de protection de la vie privée. Plus précisément, l'utilisation par le CST des renseignements personnels recueillis lors d'examens polygraphiques à des fins de dotation pourrait avoir dépassé le consentement accordé et ne pas se conformer à l'article 7 de la *Loi sur la protection des renseignements personnels*.

64. L'OSSNR a également constaté des problèmes quant à la façon dont le CST se servait du programme polygraphique, y compris des questions inutilement répétitives et agressives posées par les examinateurs, un contrôle de la qualité insuffisant des examens et des enjeux de conservation liés aux enregistrements audiovisuels. De plus, la façon dont le CST utilisait les résultats des examens polygraphiques pour éclairer la prise de décisions relatives au filtrage de sécurité pourrait causer de l'incertitude quant à la possibilité de contester les refus d'habilitations de sécurité au titre de la Loi sur l'OSSNR. En général, le CST s'est trop fié aux résultats des examens polygraphiques pour prendre des décisions relatives à des cas de filtrage de sécurité. Dans son ensemble, l'utilisation par le CST du polygraphe dans le processus de filtrage de sécurité a soulevé d'importantes préoccupations liées à la Charte.

65. L'OSSNR a également examiné le rôle du SCT dans l'établissement de la Norme sur le filtrage de sécurité (« la Norme »), qui régit l'utilisation du polygraphe pour le filtrage de sécurité par le gouvernement du Canada. L'OSSNR a conclu que le SCT n'avait pas tenu compte adéquatement des répercussions de l'utilisation du polygraphe en ce qui concerne la protection de la vie privée ou la Charte. Le SCT n'a pas non plus mis en œuvre des mesures de protection suffisantes dans la Norme pour remédier à ces répercussions.

66. Par conséquent, l'OSSNR a recommandé que le CST et le SCT s'attaquent d'urgence aux problèmes fondamentaux liés à la légalité, au caractère raisonnable et à la nécessité de l'utilisation du polygraphe pour le filtrage de sécurité. Si ces problèmes ne peuvent pas être réglés, l'OSSNR recommande que le SCT retire le polygraphe de la Norme et que le CST cesse de l'utiliser pour le filtrage de sécurité.

Examen des solutions réseau du CST et des activités connexes liées à la cybersécurité et à l'assurance de l'information

67. Depuis l'entrée en vigueur de la Loi sur le CST en 2019, les activités de cybersécurité et d'assurance de l'information (CSAI) du CST ont pris de l'ampleur et de l'importance. Le CST obtient et analyse de vastes quantités de renseignements en vue de cerner et de prévenir les menaces à la cybersécurité. Il s'agit d'une activité essentielle qui touche néanmoins d'importants intérêts en matière de protection de la vie privée, un équilibre que l'OSSNR a cherché à comprendre.

68. Il s'agissait du premier examen par l'OSSNR des activités de CSAI du CST, ainsi que son premier examen de Services partagés Canada (SPC). Les deux ministères mènent de concert des activités de CSAI, car SPC est le responsable du système de la plupart des réseaux du gouvernement du Canada.

69. L'OSSNR a conclu que le CST exploite un écosystème complet et intégré de systèmes, d'outils et de capacités de cybersécurité pour se protéger contre les cybermenaces et dont la conception intègre des mesures visant à protéger la vie privée des Canadiens et des personnes au Canada.

70. L'OSSNR a formulé des conclusions et des recommandations pour deux domaines de préoccupation :

- Les communications du CST au ministre de la Défense nationale au sujet de son programme de CSAI ne décrivaient pas complètement ses activités en pratique. L'OSSNR a formulé des recommandations pour aider le CST à améliorer sa transparence à cet égard.

- Le CST a acquis des renseignements de sources qui, dans certains cas, pourraient mettre en jeu des intérêts canadiens en matière de protection de la vie privée. Bien que ces renseignements soient manifestement utiles en matière de cybersécurité, ils n'ont pas été acquis dans le cadre d'autorisations ministérielles, en partie en raison d'une

incompatibilité entre des paragraphes de la Loi sur le CST. L'OSSNR a recommandé diverses mesures pour remédier à cette acquisition.

71. L'OSSNR a obtenu des connaissances de base sur les activités de CSAI du CST au moyen de son examen, ce qui permettra d'orienter ses activités futures.

Examen annuel des activités du Centre de la sécurité des télécommunications

72. L'OSSNR a mené le deuxième examen annuel des activités du CST. L'examen de 2023 visait à cerner les défis liés à la conformité, des tendances générales et les nouveaux problèmes en utilisant les renseignements que le CST est tenu par la loi de fournir à l'OSSNR, ainsi que de l'information additionnelle. En plus de contribuer au rapport annuel de l'OSSNR au ministre de la Défense nationale sur les activités du CST, l'examen a également permis de cerner des aspects qui méritent de faire l'objet de nouveaux examens par l'OSSNR et d'en apprendre davantage sur les activités du CST.

Statistiques et données

73. Pour accroître la responsabilisation et la transparence, l'OSSNR a demandé au CST de lui fournir des statistiques et des données sur les aspects de ses activités liées à l'intérêt public et à la conformité. L'OSSNR est d'avis que ces statistiques fourniront au public de l'information importante quant à la portée et à l'étendue des activités du CST, et indiqueront l'évolution des activités d'une année à l'autre.

Autorisations ministérielles et arrêtés ministériels

74. Les autorisations ministérielles sont délivrées au CST par le ministre de la Défense nationale. Ces autorisations appuient les activités précises liées au renseignement étranger ou à la cybersécurité, ou des cyberopérations défensives ou actives menées par le CST conformément aux volets de son mandat. Les autorisations sont délivrées lorsque ces activités pourraient autrement contrevenir à une loi du Parlement ou compromettre l'attente raisonnable en matière de respect de la vie privée d'un Canadien ou d'une personne se trouvant au Canada.

Tableau 8 : Autorisations ministérielles délivrées, 2019–2023

Type d'autorisation ministérielle	Article habilitant de la Loi sur le CST	Délivrées en 2019	Délivrées en 2020	Délivrées en 2021	Délivrées en 2022	Délivrées en 2023
Renseignement étranger	26(1)	3	3	3	3	3
Cybersécurité – infrastructures fédérales et non fédérales	27(1) et 27(2)	2	1	2	3	3
Cyberopérations défensives	29(1)	1	1	1	1	1
Cyberopérations actives	30(1)	1	1	2	3	3

Remarque : Le tableau présente les autorisations ministérielles qui ont été délivrées au cours des années civiles données et ne reflètent pas nécessairement les autorisations ministérielles qui étaient en vigueur à un moment donné. Par exemple, si une autorisation ministérielle a été délivrée à la fin de 2022 et est demeurée en vigueur pendant une partie de 2023, elle est comptée uniquement comme une autorisation ministérielle de 2022.

75. Les arrêtés ministériels sont délivrés par le ministre pour 1) désigner comme étant importantes pour le gouvernement fédéral de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information [article 21(1) de la Loi sur le CST]; ou 2) désigner des destinataires de l'information qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada, c'est-à-dire de l'information nominative sur un Canadien [articles 45 et 44(1) de la Loi sur le CST].

Tableau 9 : Arrêtés ministériels en vigueur en 2023

Nom de l'arrêté ministériel [traduction]	Article habilitant de la Loi sur le CST
Désignation des destinataires de l'information nominative sur un Canadien utilisée, analysée ou conservée au titre d'une autorisation touchant le renseignement étranger	43
Désignation des destinataires de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada qui a été acquise, utilisée ou analysée dans le cadre des volets du mandat du CST touchant la cybersécurité et l'assurance de l'information	44
Désignation de l'information électronique et des infrastructures d'importance pour le gouvernement du Canada	21
Désignation de l'information électronique et des infrastructures de l'Ukraine comme étant d'importance pour le gouvernement du Canada	21
Désignation de l'information électronique et des infrastructures de la Lettonie comme étant d'importance pour le gouvernement du Canada	21

Remarque : Les arrêtés ministériels demeurent en vigueur jusqu'à ce qu'ils soient annulés par le ministre.

Rapports sur le renseignement étranger

76. Conformément à l'article 16 de la Loi sur le CST, ce dernier a pour mandat d'acquérir de l'information à partir de l'infrastructure mondiale de l'information. Au sens de la Loi sur le CST, l'infrastructure mondiale de l'information est ainsi définie : « [v]ise notamment les émissions électromagnétiques et tout équipement produisant de telles émissions, les systèmes de communication, les systèmes et réseaux des technologies de l'information, ainsi que les données et les renseignements techniques qu'ils transportent, qui s'y trouvent ou qui les concernent. » Le CST utilise, analyse et diffuse l'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement fédéral en matière de renseignement.

Tableau 10 : Nombre de rapports sur le renseignement étranger produits, 2019–2023

Rapports sur le renseignement étranger du CST	2020 (#)	2021 (#)	2022 (#)	2023 (#)
Nombre de rapports produits	Non disponible	3050	3185	3184
Nombre de ministères et organismes	>25	28	26	28
Nombre de clients précis au sein des ministères et organismes	>2 100	1627	1761	2049

Remarque : L'OSSNR n'a pas demandé au CST de statistiques concernant les rapports sur le renseignement étranger pour son rapport public annuel de 2019. En 2020, des statistiques ont été demandées, mais les statistiques fournies étaient de nature générale en raison de la classification des données à l'époque, et le CST a indiqué que la publication de détails supplémentaires porterait atteinte à la sécurité nationale.

Information qui se rapporte à un Canadien ou à une personne au Canada

77. L'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada (IRCPC) constitue de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada qui pourrait être recueillie incidemment par le CST lorsqu'il mène des activités liées au renseignement étranger ou à la cybersécurité au titre d'une autorisation ministérielle. La collecte fortuite renvoie à de l'information qui n'était pas délibérément recherchée par le CST et au fait que l'activité qui a permis l'acquisition de cette information ne visait pas un Canadien ou une personne se trouvant au Canada. Selon la politique du CST, l'IRCPC constitue toute information reconnue comme se rapportant à un Canadien ou à une personne se trouvant au Canada, peu importe si cette information peut être utilisée pour identifier un Canadien ou une personne se trouvant au Canada ou non.

78. L'OSSNR a demandé au CST de publier des statistiques ou des données sur la régularité avec laquelle de l'IRCPC ou de l'information recueillie au Canada est incluse dans les rapports sur les produits finaux du CST. Le CST a répondu que [traduction] « cette information demeure classifiée et ne peut pas être publiée ».

Information nominative sur un Canadien

79. Il est interdit au CST de cibler des Canadiens ou des personnes se trouvant au Canada dans le cadre de ses activités. Toutefois, en raison des méthodes de collecte du CST, de telles

informations peuvent parfois être recueillies incidemment. Lorsque ces informations recueillies incidemment sont utilisées dans un rapport sur le renseignement étranger du CST, toute partie susceptible d'identifier un Canadien ou une personne se trouvant au Canada est supprimée afin de protéger la vie privée des personnes en question. Le CST peut communiquer l'information nominative sur un Canadien (INC) non supprimée à des destinataires désignés lorsqu'ils disposent d'un pouvoir juridique et d'une justification opérationnelle de la recevoir et lorsque l'information est essentielle aux affaires internationales, à la défense ou à la sécurité (y compris la cybersécurité).

Tableau 11 : Nombre de demandes de communication d'INC, 2021–2023

Type de demande	2021 (#)	2022 (#)	2023 (#)
Demandes du gouvernement du Canada	741	657	1 087
Demandes du Groupe des cinq	90	62	142
Demandes d'organismes ne faisant pas partie du Groupe des cinq	0	0	0
Total	831	719	1 229

80. En 2023, sur les 1 229 demandes reçues, le CST a indiqué avoir rejeté 281 demandes. À la fin de l'année, 40 demandes étaient toujours en cours de traitement.

81. L'OSSNR a également demandé au CST de publier le nombre de cas où de l'INC a été supprimée de rapports sur la cybersécurité ou le renseignement étranger du CST. Le CST a répondu que [traduction] « la communication du nombre de cas où de l'INC a été supprimée de rapports sur le renseignement du CST porterait atteinte aux capacités du CST et ne peut pas être publiée. »

Incidents liés à la protection des renseignements personnels et erreurs de procédure

82. Un incident lié à la protection des renseignements personnels se produit lorsque les renseignements personnels d'un Canadien, ou d'une personne au Canada, sont compromis d'une manière qui va à l'encontre des politiques du CST ou qui n'est pas prévue par celles-ci. Le CST assure le suivi de ces incidents au moyen de son dossier des incidents liés à la

protection des renseignements personnels,[14] et, pour les incidents liés à la protection des renseignements personnels attribuables à un partenaire secondaire ou à un partenaire national, de son dossier des incidents liés à la protection des renseignements personnels de seconde partie.

Tableau 12 : Nombre d'incidents liés à la protection des renseignements personnels saisis par le CST, 2021–2023

Type d'incident	2021 (#)	2022 (#)	2023 (#)
Incidents liés à la protection des renseignements personnels	96	114	107
Incidents liés à la protection des renseignements personnels attribuables à des secondes parties	33	23	37
Incidents non liés à la protection des renseignements personnels	Non disponible	Non disponible	28

Remarque : L'OSSNR n'a pas demandé au CST de statistiques concernant les rapports sur les incidents non liés à la protection des renseignements personnels pour ses rapports publics annuels de 2021 et de 2022.

Tableau 13 : Nombre d'incidents liés à la protection des renseignements personnels survenus dans le cadre du volet relatif au renseignement étranger du mandat du CST signalés en 2023

Type d'incident	2023 (#)
Incidents liés à la protection des renseignements personnels	70
Incidents liés à la protection des renseignements personnels attribuables à des secondes parties	37

[14] Depuis le quatrième trimestre de l'exercice 2021-2022, le CST a cessé de faire la distinction entre le dossier des incidents liés à la protection des renseignements personnels et le dossier des incidents liés à la protection des renseignements personnels de seconde partie, car les incidents de chaque type correspondent à la même définition du CST d'un incident lié à la protection de la vie privée. Les erreurs de procédure sont maintenant signalées dans le dossier des incidents liés à la protection des renseignements personnels.

Incidents non liés à la protection des renseignements personnels	16

Tableau 14 : Nombre d'incidents liés à la protection des renseignements personnels survenus dans le cadre du volet cybersécurité et assurance de l'information du mandat du CST signalés en 2023

Type d'incident	2023
Incidents liés à la protection des renseignements personnels	37
Incidents non liés à la protection des renseignements personnels	12

Cybersécurité et assurance de l'information

83. Conformément à l'article 17 de la Loi sur le CST, le CST a pour mandat de fournir des avis, des conseils et des services afin d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales, de même que celles des entités non fédérales désignées par le ministre comme étant d'importance pour le gouvernement fédéral.

84. Le Centre canadien pour la cybersécurité (CCC) est l'autorité canadienne unifiée en matière de cybersécurité. Le CCC, qui fait partie du CST, offre une orientation, des services et une formation spécialisés, tout en travaillant en collaboration avec les intervenants des secteurs privé et public. Le CCC traite les incidents survenus au sein du gouvernement et des institutions désignées, notamment les types d'incidents qui comprennent ce qui suit :

- les activités de reconnaissance menées par des auteurs de menace dotés de techniques sophistiquées;
- les incidents d'hameçonnage, soit les courriels contenant des maliciels;
- les accès non autorisés à des environnements de technologie de l'information (TI) organisationnels;
- les attaques imminentes par rançongiciel;
- les exploits du jour zéro (exploitation de vulnérabilités critiques dans des logiciels n'ayant pas fait l'objet de correctifs).

Tableau 15 : Nombre de dossiers de cyberincident ouverts par le CST, 2022 et 2023

Type de cyberincident	2022	2023
Institutions fédérales	1 070	977
Infrastructures essentielles	1575	1756
À l'échelle internationale	Non disponible	82
Total	2 645	2 815

Remarque : L'OSSNR n'a pas demandé au CST de statistiques concernant les rapports sur les incidents internationaux pour son rapport public annuel de 2022.

Cyberopérations actives et défensives

85. Conformément à l'article 18 de la Loi sur le CST, le CST a pour mandat de mener des cyberopérations défensives (COD) afin d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales de même que celles des entités non fédérales désignées par le ministre comme étant d'importance pour le gouvernement fédéral contre les cyberattaques hostiles.

86. Conformément à l'article 19 de la Loi sur le CST, le CST a pour mandat de mener des cyberopérations actives (COA) contre des étrangers, des États, des organismes ou des groupes terroristes étrangers dans la mesure où elles se rapportent aux affaires internationales, à la défense ou à la sécurité.

87. L'OSSNR a demandé au CST de publier le nombre de COD et de COA approuvées et le nombre de COD et de COA menées en 2023. Le CST a répondu que [traduction] « cette information demeure classifiée et ne peut pas être publiée ».

Assistance technique et opérationnelle

88. Dans le cadre du volet du mandat du CST touchant l'assistance technique et opérationnelle, le CST reçoit des demandes d'assistance d'organismes canadiens chargés de l'application de la

loi et de la sécurité de même que de la part du ministère de la Défense nationale et des Forces armées canadiennes.[15]

Tableau 16 : Nombre de demandes d'assistance que le CST a reçues et auxquelles il a donné suite, 2020–2023

Action	2020	2021	2022	2023
Approuvées	23	32	59	48
Non approuvées	1	3	0	0
En cours d'examen	Non disponible	Non disponible	0	2
Annulées	Non disponible	Non disponible	1	0
Refusées	Non disponible	Non disponible	2	1
Nombre total de demandes reçues	**24**	**35**	**62**	**53**

Remarque : Pour 2020 et 2021, le CST n'a pu fournir que le nombre de demandes reçues et auxquelles il a donné suite. Le CST a toutefois indiqué qu'il a depuis amélioré son système de suivi interne des demandes d'assistance. Pour 2022, le CST était désormais en mesure de fournir le nombre de demandes d'assistance approuvées, refusées ou annulées.

4.4 Examens d'autres ministères

Aperçu

89. Outre les examens visant le SCRS et le CST mentionnés ci-dessus, l'OSSNR a réalisé les examens suivants auprès de ministères et organismes en 2023 :

- un examen de l'Agence des services frontaliers du Canada;

[15] L'OSSNR a demandé au CST de fournir la ventilation des demandes d'assistance par ministère demandeur, mais cette information n'a pas pu être communiquée aux fins de publication en raison de sa classification.

- un examen du ministère de la Défense nationale et des Forces armées canadiennes;
- les examens annuels par l'OSSNR de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, auxquels participent davantage de ministères et d'organismes qui font partie de l'appareil de la sécurité nationale et du renseignement du Canada.

Agence des services frontaliers du Canada

Examen du programme des sources humaines confidentielles de l'ASFC

90. L'examen s'est concentré sur les cadres juridiques et politiques qui régissent le programme des sources humaines confidentielles (SHC) de l'ASFC. L'examen comportait trois domaines d'intérêt : la gestion et l'évaluation du risque; la gestion du devoir de diligence de l'ASFC à l'égard de ses sources; et le caractère suffisant de la direction et de la responsabilité ministérielle en ce qui concerne le programme. Ensemble, ces domaines appuient la capacité de l'ASFC de mener ses activités de gestion des sources humaines de façon légale et éthique et avec une responsabilisation appropriée.

91. L'examen a démontré que le programme des SHC, en tant qu'outil d'enquête utilisé pour appuyer le mandat de l'ASFC, repose sur un cadre juridique adéquat. Cependant, l'examen a révélé certaines lacunes dans le cadre régissant le programme, particulièrement en ce qui concerne la façon dont l'ASFC gère les risques associés à l'utilisation de sources humaines qui n'ont pas de statut au Canada. L'examen contient de nombreuses conclusions liées aux pratiques de gestion du risque de l'ASFC.

92. Dans deux cas, l'examen de l'OSSNR a permis de conclure que les activités de l'ASFC pourraient ne pas respecter la loi. Dans le premier cas, l'examen a permis de constater, au moyen d'une étude de cas détaillée, que l'ASFC aurait enfreint deux fois la loi visant le privilège de l'informateur en divulguant de façon inappropriée des renseignements qui auraient pu identifier la source humaine. Dans ce cas-ci et dans un autre, l'OSSNR a conclu que l'ASFC n'avait pas informé le ministre de la Sécurité publique d'une activité d'une source humaine qui aurait pu avoir une incidence sur la sécurité d'une personne, comme l'exigent les Instructions du ministre sur la surveillance et les sources humaines confidentielles. Cela constitue une infraction au paragraphe 12(2) de la *Loi sur l'Agence des services frontaliers du Canada* (Loi sur l'ASFC).

93. L'OSSNR a formulé six recommandations dans le cadre de cet examen. Ces recommandations visent à améliorer la gouvernance du programme des SHC en vue de veiller à ce que l'ASFC soit attentive au bien-être de ses sources humaines dans l'ensemble des activités. Elles illustrent également l'attention continue que l'OSSNR porte au principe de la responsabilisation ministérielle. Dans l'ensemble, les conclusions et les recommandations de l'OSSNR témoignent du niveau de maturité du programme de l'ASFC : bien qu'il soit en œuvre depuis près de 40 ans, l'introduction des politiques propres aux sources humaines est assez récente. L'examen met aussi en évidence les efforts récents de l'ASFC pour améliorer son programme.

Ministère de la Défense nationale et les Forces armées canadiennes

Examen du Programme de gestion des sources humaines du MDN et des FAC

94. Cet examen visait à déterminer si le MDN et les FAC dirigent leurs activités de gestion des sources humaines de façon légale et éthique et avec une responsabilisation appropriée.

95. L'OSSNR a conclu que le cadre stratégique du MDN et des FAC permet la réalisation d'activités de gestion des sources humaines qui pourraient ne pas respecter la loi. Les risques touchent particulièrement les sources associées à des groupes terroristes. L'OSSNR a recommandé que le Parlement adopte un cadre de justification qui autoriserait le MDN et les FAC et leurs sources à commettre des actes par ailleurs illégaux à l'extérieur du Canada, lorsque ceux-ci servent raisonnablement à recueillir des renseignements relatifs à la défense.

96. L'OSSNR a conclu que les cadres d'évaluation du risque du MDN et des FAC ne fournissent pas aux commandants les renseignements exacts, cohérents et objectifs dont ils ont besoin pour évaluer les risques associés à la communication avec des sources particulières. L'OSSNR a recommandé que ces cadres soient révisées pour s'assurer que tous les facteurs de risque applicables sont pris en considération.

97. L'OSSNR a constaté des lacunes dans la gestion du devoir de diligence du MDN et des FAC à l'égard de leurs sources. Les processus de protection n'étaient pas toujours bien employés; le processus de traitement des plaintes était sous-développé; et les risques aux agents n'étaient pas toujours suffisamment évalués. Des mesures visant à régler ces lacunes doivent être clairement indiquées dans les documents de gouvernance.

98. L'OSSNR a conclu que le ministre de la Défense nationale n'est pas suffisamment au fait des activités de gestion des sources humaines pour remplir ses responsabilités ministérielles. Le

ministre devrait être au courant des questions juridiques, politiques et de gouvernance qui peuvent avoir une incidence sur les activités de gestion des sources humaines.

99. L'OSSNR a également constaté que d'autres directives ministérielles sont requises pour appuyer la gouvernance du Programme de gestion des sources humaines du MDN et des FAC. L'OSSNR a recommandé que le ministre fournisse des directives ministérielles au MDN et aux FAC dans le but de guider la réalisation légale et éthique d'activités de gestion des sources humaines.

4.5 Examens multiministériels

Examen de la collaboration opérationnelle entre le CST et le SCRS

100. Le CST et le SCRS sont deux piliers de la collecte de renseignements au Canada, ce qui signifie qu'une collaboration efficace entre ces organismes est essentielle à la sécurité nationale. Cependant, il existe une tension entre le mandat du SCRS, qui autorise la collecte et l'échange de renseignements sur des Canadiens, et l'interdiction fondamentale pour le CST de diriger ses activités auprès de Canadiens. Il s'agit du premier examen qui a été en mesure d'accéder à l'information des deux organismes pour étudier cette tension.

101. L'OSSNR a examiné un échantillon des activités opérationnelles collaboratives et de l'échange de renseignements du CST et du SCRS, ainsi que la collaboration entre le SCRS et le CST en ce qui concerne le mandat de mesure de réduction de la menace (MRM) du SCRS. Cet examen a satisfait à l'exigence annuelle d'examiner un aspect des MRM du SCRS énoncée au paragraphe 8(2) de la Loi sur l'OSSNR.

102. En ce qui a trait à la collaboration opérationnelle, y compris le mandat de MRM du SCRS, l'OSSNR a constaté un échange de renseignements insuffisants et un manque de planification proactive. Il a également été conclu que le CST n'a pas adéquatement tenu compte du risque de cibler des Canadiens dans son travail avec le SCRS en vue de l'atténuer. L'OSSNR a recommandé certaines modifications aux procédures pour améliorer le flux de l'information, la consultation, la transparence et la responsabilité.

103. En ce qui concerne l'échange de renseignements, l'OSSNR a conclu que les processus existants entre les organismes présentaient des lacunes en matière d'orientation et de responsabilité et posaient le risque pour le CST de cibler des Canadiens, risque qui s'est matérialisé dans certains cas. L'OSSNR a recommandé aux deux organismes d'établir des politiques, des procédures et de la formation pour les analystes. En outre, l'OSSNR a

recommandé au SCRS de cesser de présenter des demandes visant des Canadiens au CST et de réfléchir aux renseignements relatifs à des Canadiens que l'organisme échange avec le CST. L'OSSNR a également recommandé au CST de réévaluer la façon dont l'information sur les Canadiens est recueillie, conservée et communiquée dans certains scénarios et de n'utiliser que les renseignements sur les étrangers tirés des rapports du SCRS.

104. Dans l'examen, l'OSSNR a relevé deux cas de non-respect de la loi. Les deux cas concernaient des activités du CST qui ciblaient des Canadiens dans le cadre de son mandat relatif au renseignement étranger.

Examen des communications d'information par des institutions fédérales au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* en 2022

105. Cet examen présente un aperçu de l'application de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) en 2022. Ce faisant, l'examen permet de documenter le volume et la nature des communications d'information faites en 2022 en vertu de la LCISC, d'évaluer la conformité à la LCISC et de faire ressortir les tendances de son utilisation au sein des institutions du gouvernement du Canada au fil du temps.

106. En 2022, quatre institutions fédérales ont effectué un total de 173 communications d'information à cinq institutions. L'OSSNR a conclu que les institutions se sont conformées aux exigences de la LCISC en matière de communication et de conservation des dossiers dans la majorité des communications. Les cas de non-conformité liés au paragraphe 9(3) concernaient la rapidité de l'envoi des documents à l'OSSNR; les cas liés au paragraphe 5.1(1) concernaient la rapidité de la destruction ou du retour de renseignements personnels; et ceux liés au paragraphe 5(2) concernaient la fourniture d'une déclaration sur l'exactitude et la fiabilité. Ces cas ne font pas état de lacunes systémiques quant à l'application de la LCISC par les institutions du gouvernement du Canada.

107. L'OSSNR a également établi des conclusions concernant des pratiques qui laissent place à l'amélioration, bien qu'elles soient conformes à la LCISC. Les recommandations connexes de l'OSSNR visaient à améliorer la normalisation dans l'ensemble du gouvernement du Canada d'une manière qui respecte les pratiques exemplaires démontrées par les institutions, ainsi que les principes directeurs de la LCISC.

108. Dans l'ensemble, l'OSSNR a observé des améliorations quant au rendement des institutions examinées comparativement aux résultats des rapports des années précédentes et au cours

de l'examen. Ces améliorations comprennent des mesures correctives prises par les institutions examinées en réponse aux demandes d'information de l'OSSNR dans le cadre de l'examen.

Examen de la mise en œuvre par les ministères de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* pour 2022

109. Cet examen a évalué la conformité des ministères à la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* (LCMTIEE) et la mise en œuvre des directives associées à la LCMTIEE au cours de l'année civile 2022. Dans ce contexte, l'examen a porté sur le thème de la réalisation des évaluations du risque des ministères, notamment la façon dont leurs méthodes peuvent entraîner une sous-évaluation du niveau de risque associé à une communication d'information.

110. Les conclusions et recommandations de l'OSSNR dans le rapport indiquent que la mise en œuvre des directives par les ministères a progressé et stagné à la fois. L'OSSNR a constaté des efforts de collaboration interministérielle pour normaliser certaines pratiques à l'échelle du gouvernement du Canada. Bien que ces efforts indiquent une amélioration par rapport aux approches antérieures, ils ne satisfont pas aux exigences du cadre relatif à l'échange au sein du gouvernement de renseignements étrangers prévues par la LCMTIEE. De plus, l'OSSNR a observé certaines pratiques qui pourraient amener les ministères à sous-évaluer systématiquement les risques associés aux échanges de renseignements envisagés. Une telle sous-évaluation peut ensuite donner lieu à des échanges de renseignements qui ne respectent pas les interdictions énoncées dans les directives.

111. L'OSSNR a formulé cinq recommandations dans le cadre de cet examen. Dans l'ensemble, ces recommandations permettraient de veiller à ce que les cadres relatifs à la LCMTIEE des ministères appuient une normalisation correspondant à celle visée par la LCMTIEE et les directives connexes, et à ce que ces cadres soient conçus pour favoriser la conformité aux directives.

05 //

Enquêtes sur les plaintes

5.1 Aperçu

112. L'OSSNR a le mandat d'enquêter sur les plaintes du public liées à la sécurité nationale. Les enquêtes sur les plaintes de l'OSSNR sont menées avec uniformité, équité et rapidité. Le mandat de l'OSSNR en matière de plaintes du public permet de veiller à ce que les organisations de sécurité nationale et de renseignement du Canada soient imputables envers le public canadien.

113. L'OSSNR s'est engagé à établir des normes de service pour l'examen des plaintes, avec pour objectif de mener à bien 90 % des enquêtes dans le respect des normes. Ces normes de service, qui sont en vigueur depuis le 1er avril 2023, établissent des délais internes pour certaines étapes de l'enquête pour chaque type de plainte, dans des circonstances normales. L'OSSNR est fier d'annoncer que, pour la période du 1er avril au 31 décembre 2023, 100 % des normes de service ont été respectées dans tous les dossiers d'enquête assujettis à ces normes.

114. Tout en prenant compte des intérêts du plaignant et des impératifs de sécurité de l'organisation, l'OSSNR a mis en place un processus de vérification indépendant auprès du CST pour les nouvelles plaintes déposées au titre de l'article 17 de la Loi sur l'OSSNR. Plus précisément, à la réception d'une plainte, l'OSSNR doit évaluer si celle-ci relève de son mandat, en fonction des conditions énoncées dans la Loi sur l'OSSNR. En ce qui concerne les plaintes contre le CST, ainsi que celles contre le SCRS et la GRC, l'OSSNR doit être convaincu que la plainte contre l'organisation défenderesse porte sur une activité menée par l'organisation et qu'elle n'est pas frivole, vexatoire ou sans objet. Le nouveau processus de vérification indépendant aide l'OSSNR à déterminer s'il a la compétence d'enquêter sur les plaintes déposées contre le CST.

115. L'OSSNR a élaboré un nouvel outil de suivi interne pour assurer une gestion efficace des dossiers de plaintes.

116. L'OSSNR a déjà affirmé que son site Web serait amélioré dans le but de favoriser l'accessibilité aux enquêtes sur les plaintes. Au cours de la refonte de son site Web public à l'automne 2023, l'OSSNR a modifié ses formulaires de plaintes pour s'assurer qu'ils répondent aux critères

d'accessibilité et aux exigences de conformité des Règles pour l'accessibilité des contenus Web (WCAG) 2.0.

117. En 2023, l'OSSNR a terminé la dernière phase d'une étude menée conjointement avec la Commission civile d'examen et de traitement des plaintes relatives à la GRC (CCETP) concernant la collecte des données fondées sur la race et d'autres renseignements démographiques. L'étude vise à évaluer la viabilité de la collecte de données démographiques et fondées sur l'identité dans le cadre des initiatives de lutte contre le racisme continues du gouvernement du Canada.

118. Dans le cadre de l'étude, des entrevues ont été menées auprès de membres de la communauté qui connaissent l'OSSNR, la CCETP et les organisations que celles-ci examinent. En fin de compte, l'étude a permis de constater que la collecte de données fondées sur la race est faisable.

119. L'étude comprenait également des recommandations relatives à la collecte de données fondées sur la race, portant notamment sur :

- la collecte auprès de plaignants de données fondées sur la race et la façon de recueillir ces données;
- la collecte d'autres données biographiques des plaignants;
- la collecte de données fondées sur la race concernant le personnel de services de police et d'organisations de renseignement;
- l'analyse des données recueillies;
- la fourniture des données recueillies aux intervenants intéressés, au grand public, ou aux deux;
- l'élaboration d'un plan d'analyse de données avancé.

120. L'OSSNR accueille favorablement les observations obtenues dans le cadre de l'étude conjointe et examinera attentivement les recommandations pour déterminer comment elles pourraient être mises en œuvre. La collecte de données fondées sur la race et d'autres renseignements démographiques dans le secteur de la sécurité nationale et du renseignement est un domaine nouveau. L'examen documentaire de l'étude a mis en évidence que ce type de collecte de données démographiques et fondées sur la race n'a jamais été réalisé auparavant dans le domaine canadien de la sécurité nationale et du renseignement ou par l'un des partenaires internationaux du Canada. L'OSSNR et la CCETP continueront de collaborer à cette importante initiative en déterminant des stratégies de mise en œuvre potentielles.

5.2 Initiatives en cours

121. En 2023, l'OSSNR a commencé à réviser ses *Règles de procédure* en vue de peaufiner les procédures régissant ses enquêtes sur les plaintes. La révision se poursuivra en 2024 avec l'appui du secrétariat pour s'assurer que l'OSSNR respecte les obligations prévues dans le *Plan sur l'accessibilité*.

122. Une partie des modifications apportées aux procédures de l'OSSNR en 2024 consistera à examiner la déclaration de confidentialité inscrite sur les formulaires de plainte afin d'assurer une transparence accrue quant à la façon dont les renseignements soumis à l'OSSNR par les plaignants seront utilisés dans les enquêtes.

5.3 Résumés des enquêtes

Rapports finaux émis*

**Afin de dépersonnaliser les présents résumés d'enquêtes, le masculin est utilisé pour faire référence aux individus ayant déposé une plainte, quel que soit leur genre.*

Enquête sur des allégations contre le SCRS (dossier de l'OSSNR 07-403-45)

123. Le plaignant a allégué que des agents du SCRS avaient interagi avec lui à plusieurs reprises et a affirmé que ces interactions consistaient en des arrestations et des détentions illégales; que les agents l'avaient intimidé illégalement en prétendant qu'ils allaient l'expulser à Guantanamo Bay; et que le SCRS avait appliqué incorrectement la *Loi sur la protection des renseignements personnels* en refusant de fournir des documents que le plaignant prétend avoir été contraint de signer lors d'une des interactions susmentionnées.

124. Après avoir examiné tous les éléments de preuve présentés par les parties et les renseignements disponibles, l'OSSNR a constaté que le plaignant n'avait jamais interagi avec le SCRS. L'OSSNR a conclu qu'aucune des allégations ne pouvait être corroborée.

Allégations contre le SCRS par rapport à des difficultés de voyage, du harcèlement et de la discrimination (dossier de l'OSSNR 07-403-23)

125. Le plaignant a allégué que, à la suite d'un séjour à l'étranger, il a éprouvé des difficultés lors de voyages internationaux, difficultés qu'il croyait être attribuables au SCRS et aux renseignements que le SCRS échange avec les gouvernements de pays étrangers. Le plaignant

a affirmé que le SCRS l'avait inscrit à une « liste noire » comme membre de l'État islamique en Irak et en Syrie. Il a ajouté que le SCRS l'avait harcelé et avait fait preuve de discrimination à son égard en raison de sa race, de son origine ethnique et de sa religion.

126. Au moment du voyage du plaignant, certains pays servaient régulièrement de destinations intermédiaires pour les voyageurs extrémistes d'Amérique du Nord et d'Europe qui souhaitaient se rendre à des territoires contrôlés par l'État islamique.

127. Le SCRS a interrogé la famille du plaignant pour obtenir des renseignements sur le plaignant, ses croyances et ses intentions possibles. Le plaignant a considéré l'interaction comme un interrogatoire inapproprié des membres de sa famille.

128. Après examen de tous les éléments de preuve, l'OSSNR a conclu que les activités du SCRS dans cette affaire étaient légitimes et raisonnables. Le SCRS avait effectivement entrepris des mesures d'enquête, mais rien n'indique que le SCRS avait inscrit le plaignant à une « liste noire » ou que des renseignements sur lui avaient été communiqués de façon inappropriée. De même, l'allégation selon laquelle le SCRS était responsable des difficultés de voyage du plaignant a été jugée non fondée. Les difficultés de voyage du plaignant peuvent être attribuables à des autorités étrangères, ce qui va au-delà de la portée de la compétence de l'OSSNR.

129. L'OSSNR a conclu que le SCRS avait mené une entrevue avec un parent du plaignant à sa résidence, en présence d'autres membres de sa famille, au cours de laquelle le parent a participé volontairement et a exprimé sa volonté d'offrir de l'aide supplémentaire au besoin. L'OSSNR a jugé que le fondement de l'entrevue était raisonnable et n'a pas trouvé de preuve de comportement inapproprié, d'intimidation, d'acte répréhensible ou de harcèlement.

130. L'OSSNR n'a pas trouvé de fondement de preuve en appui aux allégations de harcèlement et de discrimination fondée sur la race, l'origine ethnique ou la religion de la part du SCRS envers le plaignant.

131. Les allégations du plaignant ont été jugées non fondées.

Allégations contre le SCRS concernant des activités criminelles menées par un agent du SCRS (dossier de l'OSSNR 07-403-39)

132. Le plaignant a allégué qu'un agent du SCRS avait envahi son domicile et déclaré qu'il était un agent du renseignement en service. Selon le plaignant, l'agent du SCRS l'avait agressé

physiquement, l'avait enregistré sur vidéo pendant qu'il se déshabillait et avait menacé de le tuer. Le plaignant a également allégué que le SCRS tente de les faire taire.

133. Après examen de tous les éléments de preuve, il est devenu apparent que le comportement du plaignant l'a porté à l'attention du SCRS. Celui-ci a d'abord communiqué avec le SCRS pour soumettre des plaintes contre une personne. Le SCRS a reçu et examiné les allégations, puis a donné suite aux plaintes afin de déterminer si la personne nommée par le plaignant était affiliée au SCRS. À la suite d'un examen des documents soumis par le SCRS, l'OSSNR a déterminé que la personne visée par les plaintes du plaignant n'était pas un employé du SCRS et n'avait aucun lien avec l'organisation.

134. De plus, l'OSSNR a conclu que dans le cadre des activités du SCRS menées par rapport à la plainte, le SCRS n'a recueilli que peu de renseignements sur le plaignant. L'OSSNR a conclu que la collecte des renseignements personnels du plaignant était justifiée par le mandat du SCRS.

135. L'OSSNR a conclu que les activités du SCRS liées au plaignant étaient légitimes et raisonnables dans les circonstances.

Allégations contre le SCRS concernant une entrevue de filtrage de sécurité pour la citoyenneté (dossier de l'OSSNR 07-403-65)

136. Le plaignant avait présenté une demande de citoyenneté canadienne et a ensuite été tenu de se présenter à une entrevue avec le SCRS. Le plaignant s'est rendu à l'entrevue avec son avocat. Le plaignant a allégué que les agents du SCRS responsables de l'entrevue :

- ont refusé que le plaignant et son avocat enregistrent et prennent des notes lors de l'entrevue;
- ont enfreint des recommandations antérieures du CSARS en n'enregistrant pas l'entrevue;
- ont interagi avec l'avocat du plaignant de manière intimidante et n'ont pas permis à l'avocat d'intervenir ou d'interrompre;
- n'ont pas fourni un service d'interprétation adéquat;
- ont manqué de sensibilité culturelle pendant l'entrevue, ont utilisé des tactiques d'entrevue inappropriées, ont choisi des points de discussion qui ont créé une tension inutile et ont mal agi.

137. Après examen de tous les éléments de preuve, l'OSSNR a conclu que les agents du SCRS ont commis une erreur en interdisant au plaignant et à son avocat de prendre des notes qu'ils pourraient conserver après l'entrevue. Le SCRS a admis que cette pratique n'était plus en place. L'OSSNR a recommandé au SCRS de modifier sa politique de gouvernance pour indiquer clairement que la personne interviewée et son représentant peuvent prendre et conserver des notes lors d'entrevues.

138. L'OSSNR a fait remarquer que, depuis 2000, de nombreux rapports et décisions du CSARS ont recommandé que le SCRS enregistre les entrevues de filtrage de sécurité liées à l'immigration. Cependant, le SCRS n'enregistrait pas systématiquement ces entrevues au moment de l'entrevue du plaignant. Le SCRS a indiqué que l'organisation entreprenait actuellement des efforts pour exiger l'enregistrement de toutes les entrevues d'immigration dans ses procédures écrites. L'OSSNR a recommandé au SCRS d'enregistrer de façon proactive les entrevues relatives à l'immigration et à la citoyenneté et de conserver les enregistrements au moins jusqu'à ce qu'une décision soit prise par IRCC selon les conseils du SCRS. Si le SCRS arrive à une conclusion négative, l'enregistrement devrait être conservé jusqu'à ce que le statut d'immigration soit déterminé, ainsi que pendant la période de tout appel de cette décision.

139. Puisque le plaignant n'a pas été en mesure de conserver les notes prises pendant l'entrevue et que celle-ci n'a pas été enregistrée, l'OSSNR n'a pas pu tirer de conclusion sur la plupart des déclarations inappropriées que l'agent du SCRS aurait faites. Toutefois, une déclaration en particulier, un idiome anglais que l'agent du SCRS a reconnu avoir dit a été jugé inutile et contre-productif, car elle risquait d'accroître les tensions lors de l'entrevue et n'avait peut-être pas de traduction littérale raisonnable dans la langue parlée par le plaignant.

140. Le SCRS a indiqué, et l'OSSNR a convenu, que l'avocat d'une personne interviewée joue un rôle dans le processus d'entrevue, mais ne le dirige pas. L'avocat d'une personne interviewée n'est pas tenu au silence, mais ne doit pas non plus agir de manière à nuire à la capacité du SCRS d'exécuter son mandat. Par conséquent, il n'est pas permis à l'avocat de diriger les témoins ou de jouer un rôle intrusif dans l'interrogation. Cependant, l'OSSNR a souligné que l'avocat peut soulever des préoccupations sur l'interprétation ou suggérer des questions de clarification. Ces préoccupations doivent être soulevées pendant une pause ou d'une autre manière organisée qui ne perturbe pas l'entrevue. L'OSSNR a donc recommandé que le SCRS énonce, dans sa procédure opérationnelle, le rôle de l'avocat (ou d'autres tiers) comme précisé ci-dessus et communique à l'avance ces attentes aux personnes qui participent à une entrevue.

141. Finalement, pour corriger les erreurs commises, l'OSSNR a recommandé que le SCRS convoque une deuxième entrevue pour le plaignant, avec des agents et un interprète différents. Étant donné les irrégularités de la première entrevue et l'inquiétude subséquente qu'elle ait contenu des faits inexacts, l'OSSNR a également recommandé au SCRS de ne pas tenir compte des résultats de la première entrevue dans son évaluation et ses conseils à l'intention d'IRCC.

Allégations contre la GRC pour défaut de remettre des objets saisis (dossier de l'OSSNR 07-407-08)

142. Le plaignant a déposé une plainte contre la GRC alléguant que l'organisation avait omis de lui remettre des biens saisis de son bureau, à la suite d'une enquête de la GRC sur un complot terroriste. Le plaignant a également allégué que la GRC avait endommagé ses biens.

143. Après examen des faits et du calendrier de l'enquête de la GRC qui a mené à la saisie des biens du plaignant, l'OSSNR a conclu que les biens étaient dûment détenus, conformément aux dispositions du *Code criminel* et à la politique de la GRC.

144. De plus, l'OSSNR a conclu qu'aucune preuve ne permettrait de conclure que les biens du plaignant avaient été endommagés par la GRC pendant et après la saisie.

145. Les allégations du plaignant ont été jugées non fondées.

Allégation selon laquelle la GRC a omis d'enquêter sur des menaces contre le plaignant et sa famille faites par un gouvernement étranger (dossier de l'OSSNR 07-407-04)

146. Le plaignant est arrivé au Canada à titre de réfugié fuyant des persécutions violentes. À la suite d'un litige contre son ancien employeur, qui était lié au gouvernement d'un État étranger, le plaignant a allégué avoir été victime de menaces de mort de la part de l'ancien employeur et de représentants du gouvernement du pays d'où il s'était enfui. Le plaignant croyait que ces menaces étaient crédibles, puisqu'elles étaient souvent accompagnées de détails précis, comme les vêtements portés par le plaignant lors d'une certaine sortie et l'endroit où il était allé. Le plaignant croyait que les représentants du gouvernement susmentionné travaillant à l'ambassade du pays au Canada participaient à la surveillance du plaignant et de sa famille, y compris de ses enfants lorsqu'ils étaient à l'école.

147. Le plaignant a allégué que la GRC n'avait pas mené une enquête complète sur les incidents liés à des menaces, dont des menaces de mort, proférées contre le plaignant et sa famille, et

que les décisions de la GRC avaient été influencées de façon inappropriée par des représentants étrangers.

148. Les éléments de preuve fournis par la GRC ont démontré que l'organisation avait pris les mesures nécessaires pour examiner les renseignements donnés par le plaignant, mais qu'il n'y avait pas suffisamment de motifs pour que la GRC poursuive son enquête sur l'aspect de l'influence étrangère des menaces. Toutefois, le service de police local était le service de police compétent en ce qui concerne l'enquête sur le harcèlement criminel, les menaces et les préoccupations en matière de sécurité liées aux déclarations du plaignant. La GRC a informé le service de police local que les renseignements recueillis par la GRC lui seraient remis et a demandé d'être avisée si le service de police trouvait une personne au Canada qui travaille au nom d'un gouvernement étranger pour menacer ou intimider le plaignant. L'OSSNR a conclu que l'enquête initiale de la GRC était raisonnablement approfondie et que sa décision finale constituait un exercice justifiable du pouvoir discrétionnaire de la police.

149. De plus, aucune preuve permettant d'appuyer l'allégation du plaignant selon laquelle la décision de la GRC de mettre fin à son enquête avait été influencée de façon inappropriée par des étrangers n'a été présentée à l'OSSNR.

150. Les allégations du plaignant ont été jugées non fondées.

Allégations contre la GRC concernant le traitement de membres d'une famille dans le cadre d'une opération tactique (dossier de l'OSSNR 07-407-05)

151. La GRC a arrêté le plaignant à son domicile en raison d'accusations liées au terrorisme. Au cours de l'opération, les membres de la famille du plaignant ont été menottés. Le plaignant est d'avis que cela était inapproprié et que les agents de la GRC n'avaient pas mis en pratique leur formation de sensibilisation aux réalités culturelles.

152. L'OSSNR a conclu :

- que les agents qui sont intervenus au domicile du plaignant et dont le comportement a donné lieu à la plainte étaient des membres d'autres services de police, et non pas de la GRC;
- qu'étant donné que la police avait à l'époque des motifs raisonnables de croire que des armes dangereuses et entreposées de façon non sécuritaire auraient pu se trouver sur les lieux, le fait de menotter les membres de la famille du plaignant n'était pas arbitraire. Cependant, l'utilisation des menottes n'était plus appropriée dès que les agents avaient

sécurisé les lieux. Par conséquent, les membres de la famille ont été détenus arbitrairement, au sens de l'article 9 de la Charte;

- que, puisque la formation de sensibilisation culturelle fournie par la GRC aux enquêteurs participant à l'opération a abordé les points essentiels, la GRC n'a commis aucun acte ou n'a rien omis qui puisse soulever le risque de comportement insensible à la culture.

153. L'OSSNR a déterminé que, bien que la GRC ait assumé un rôle de supervision générale dans l'exécution de l'opération, elle dépendait du professionnalisme d'autres services de police pour la planification et l'exécution d'une fouille dynamique. Étant donné que le comportement des autres policiers qui ont participé à la fouille ne peut pas être attribué à la GRC, l'OSSNR n'a établi aucune constatation ou recommandation pour la GRC.

Autres résultats

Allégations concernant le rôle du SCRS dans les retards de l'évaluation de la sécurité relative à des demandes d'immigration ou de citoyenneté (dossiers de l'OSSNR 07-403-81, 07-403-87, 07-403-100)

154. Les plaignants ont déposé des plaintes contre le SCRS alléguant que celui-ci a causé un retard important dans la soumission d'évaluations de sécurité liées à leurs demandes d'immigration ou de citoyenneté. Au cours des enquêtes, l'OSSNR a demandé si le SCRS pouvait fournir des mises à jour sur sa participation aux processus visés. Le SCRS a fourni des lettres à l'OSSNR qui peuvent être communiquées aux plaignants pour les informer que le SCRS avait terminé son évaluation du processus de filtrage de sécurité. Comme les allégations des plaignants concernaient principalement les retards dans le filtrage de sécurité, les affaires ont été réglées à l'amiable, conformément à la règle 10.10 des *Règles de procédure* de l'OSSNR et les dossiers ont été fermés.

Allégations contre le CST concernant la discrimination d'un candidat à un emploi (dossier de l'OSSNR 07-406-07)

155. Le plaignant a déposé une plainte au titre de l'article 17 par rapport à sa demande d'emploi auprès du CST. Plus précisément, le plaignant a terminé un contrat d'étudiant au CST et a reçu une offre verbale pour un autre contrat, mais le CST a décidé de ne pas renouveler l'emploi du plaignant. Celui-ci a allégué que la décision du CST était fondée sur son origine ethnique. Même si le chef du CST a reçu une lettre de plainte du plaignant, le CST a affirmé à l'OSSNR que la lettre constituait le premier avis de la plainte et a demandé à ce que l'affaire soit mise en suspens (en attente). Après avoir mené une enquête interne sur les allégations du plaignant

(indépendamment du processus de traitement des plaintes de l'OSSNR), le CST et le plaignant ont entamé des discussions en vue d'un règlement. En fin de compte, les parties se sont entendues et en ont avisé l'OSSNR. La plainte a été réglée à l'amiable, conformément à la règle 10 des *Règles de procédure* de l'OSSNR, avant que l'OSSNR rende une décision quant à sa compétence pour enquête sur le dossier.

Allégations contre la GRC pour défaut d'enquêter sur une plainte (dossier de l'OSSNR 07-407-10)

156. La plainte a été renvoyée à l'OSSNR par le CCETP, conformément au paragraphe 45.53(4.1) de la Loi sur la GRC. Dans la plainte, il est allégué que la GRC n'a pas mené d'enquête sur des personnes qui auraient fait partie d'une milice. L'OSSNR a tenté de communiquer avec le plaignant à maintes reprises pour entreprendre son enquête. L'OSSNR a conclu que des tentatives raisonnables avaient été faites pour communiquer avec le plaignant et que toutes les options avaient été épuisées. Par conséquent, l'OSSNR a donné les motifs de l'abandon de la plainte, conformément aux *Règles de procédure* de l'OSSNR. Le dossier d'enquête sur la plainte a été fermé.

5.4 Statistiques concernant les enquêtes sur les plaintes

157. Les activités d'enquête se sont poursuivies à des niveaux importants en 2023 (voir l'annexe C). L'OSSNR a conclu plusieurs enquêtes et a émis sept rapports finaux. De plus, quatre dossiers ont été résolus à l'amiable, conformément à la règle 10 des *Règles de procédure* de l'OSSNR.

158. En 2023, l'OSSNR a observé une augmentation des plaintes contre le SCRS, dans le cadre de l'article 16 de la Loi sur l'OSSNR, alléguant des retards dans le processus de filtrage de sécurité de demandes d'immigration ou de citoyenneté. Notamment, au titre des articles 14 et 15 de la Loi sur le SCRS, le SCRS fournit des conseils en matière de sécurité à IRCC et à l'ASFC pour orienter les décisions visant à déterminer si les demandeurs de citoyenneté ou d'immigration représentent une menace pour la sécurité du Canada. Bien que le SCRS s'engage à exécuter son mandat de filtrage de sécurité en temps rapidement, il n'y a pas de délai normal établi. Au cours de l'année civile 2023, sur les six plaintes dans le cadre desquelles l'OSSNR a exercé sa compétence au titre de l'article 16 de la Loi sur l'OSSNR, cinq portaient sur des allégations de retards attribués par les plaignants aux activités de filtrage de sécurité du SCRS.

06 //

Conclusion

159. Les enquêtes et les examens exhaustifs menés par l'OSSNR en 2023 soulignent le dévouement de l'Office à l'égard de la transparence et de la responsabilisation. Les efforts ont permis de fournir des recommandations constructives visant à améliorer les pratiques opérationnelles et les cadres stratégiques des acteurs principaux de la sécurité nationale et du renseignement au Canada.

160. L'OSSNR reconnaît la nature persistante et changeante des menaces à la sécurité, qui nécessite des approches adaptatives et proactives de la part des organismes canadiens de sécurité et de renseignement. De même, l'OSSNR s'engage à améliorer continuellement ses méthodologies, à adopter les progrès technologiques et à renforcer ses capacités d'analyse pour suivre le rythme d'un monde en constant évolution. L'OSSNR continuera de collaborer avec les partenaires d'examen nationaux et internationaux du domaine de la sécurité et du renseignement en vue d'améliorer ses pratiques et de permettre au public de mieux comprendre son travail et la valeur qu'il apporte.

161. L'OSSNR est motivé par son rôle en tant qu'organisme de confiance des Canadiens au sein du domaine autrement fermé de la sécurité nationale et du renseignement, ce qui lui confère la fonction essentielle d'accroître la transparence et la responsabilisation. La vision, la mission et les valeurs de l'OSSNR illustrent cet engagement et guideront le travail de l'OSSNR vers l'avenir.

07 //

Annexes

Annexe A : Abréviations

Abréviation	Nom complet
AMC	Affaires mondiales Canada
ARC	Agence du revenu du Canada
ARVP	Attente raisonnable en matière de droit à la vie privée
ASFC	Agence des services frontaliers du Canada
AS-Rens	Autorité de surveillance indépendante des activités de renseignement de la
BCP	Bureau du Conseil Privé
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada
CCC	Centre canadien pour la cybersécurité
CCDP	Commission canadienne des droits de la personne
CCETP	Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada
COA	Cyberopérations actives
COD	Cyberopérations défensives
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement
CSAI	Cybersécurité et assurance de l'information
CSARS	Comité de surveillance des activités de renseignement de sécurité
CSERGC	Conseil de surveillance et d'examen du renseignement du Groupe des cinq
CST	Centre de la sécurité des télécommunications
CTIVD Pays-Bas	Commission néerlandaise de contrôle des services de renseignement et de sécurité

DECT	Direction exécutive du Comité contre le terrorisme des Nations Unies
DRA	Division de la recherche et de l'analyse
EOS Norvège	Commission parlementaire norvégienne de contrôle des services de renseignement et de sécurité
FAC	Forces armées canadiennes
GRC	Gendarmerie royale du Canada
HUMINT	Renseignement humain
IC IG É.-U.	Inspecteur général de la communauté du renseignement des États-Unis d'Amérique
IGIS Australie	Inspecteur général du renseignement et de la sécurité de l'Australie
IGIS Nouvelle-Zélande	Inspecteur général du renseignement et de la sécurité de la Nouvelle-Zélande
INC	Information nominative sur un Canadien
IPCO R.-U.	Bureau du commissaire aux pouvoirs d'enquête du Royaume-Uni
IRCC	Immigration, Réfugiés et Citoyenneté Canada
IRCPC	Information qui se rapporte à des Canadiens ou à des personnes au Canada
la Norme	Norme sur le filtrage de sécurité
LCISC	Loi sur la communication d'information ayant trait à la sécurité du Canada
LCMTIEE	Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères
MND	Ministère de la Défense nationale
MPO	Ministère des Pêches et des Océans
MRM	Mesure de réduction de la menace
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement
PCLOB É.-U.	Conseil de surveillance de la vie privée et des libertés civiles des États-Unis
PKGr	Comité de surveillance parlementaire de l'Allemagne
SCRS	Service canadien du renseignement de sécurité

SCT	Secrétariat du Conseil du Trésor du Canada
SHC	(Programme) des sources humaines confidentielles
SP	Sécurité publique Canada
SPC	Services partagés Canada
SR	Solutions réseau
TC	Transports Canada
TET Danemark	Conseil danois de surveillance des services de renseignement
TI	Technologie de l'information

Annexe B : Conclusions et recommandations formulées dans le cadre d'examens

La présente annexe dresse une liste complète des conclusions et des recommandations découlant des examens de l'OSSNR achevés en 2023. Dans certains cas, le texte original a été expurgé et remplacé par un résumé désigné par [*résumé*]. Une fois caviardés, les examens complets et les réponses du gouvernement aux recommandations disponibles de l'OSSNR sont publiées sur son site Web.

Examen du Service canadien du renseignement de sécurité (SCRS)

Examen de l'OSSNR portant sur le régime applicable aux ensembles de données du SCRS[16]

Conclusions de l'OSSNR

1. L'OSSNR conclut que la façon dont le SCRS applique le régime des ensembles de données n'est pas conforme aux termes énoncés dans le cadre législatif.

2. L'OSSNR conclut que l'approche suivie par le SCRS quant aux informations collectées à partir des ensembles de données au titre de l'article 12 pose le risque de créer un mécanisme de collecte parallèle qui pourrait affaiblir le seuil minimal prescrit à l'article 12 tout en se privant d'un régime de surveillance externe apte à protéger les renseignements personnels dans le contexte du régime des ensembles de données.

3. L'OSSNR conclut que le SCRS n'a pas avisé pleinement la Cour quant à son interprétation et à son application du régime des ensembles de données. Le SCRS aurait dû demander à la Cour de fournir des éclaircissements concernant ce qu'elle considère précisément comme des conduites permissibles avant d'invoquer le régime des ensembles de données.

4. L'OSSNR conclut que lorsqu'il a procédé à des interrogations en situation d'urgence, le SCRS a conservé de l'information ne correspondant pas au critère minimal de la mesure « strictement nécessaire » énoncé à l'article 12.

[16] Voir l'intégralité de l'examen expurgée : https://nsira-ossnr.gc.ca/fr/examens/examens-en-cours-et-termines/examens-termines/examen-de-lossnr-portant-sur-le-regime-applicable-aux-ensembles-de-donnees/

5. L'OSSNR conclut que le défaut de délais explicitement cités dans les dispositions de l'article 11.17 qui régissent les ensembles de données étrangers fait en sorte que des ensembles de données sont conservés pendant plusieurs années dans l'attente d'une prise de décision par le Ministre ou la personne désignée (le directeur du SCRS).

6. L'OSSNR conclut que le SCRS court le risque de collecter de l'information qui est accessible au public, mais à l'égard de laquelle il pourrait y avoir une attente raisonnable en matière de protection de la vie privée.

7. L'OSSNR conclut que les politiques du SCRS qui régissent la collecte et la conservation des ensembles de données canadiens et étrangers ne correspondent pas à la façon dont le SCRS interprète actuellement l'application du régime des ensembles de données.

8. L'OSSNR conclut que le SCRS ne dispose d'aucune politique qui régisse le traitement de l'information éphémère. De plus, la [**expurgé**] qui est actuellement en place ne fournit pas suffisamment d'instructions aux employés, ce qui pourrait faire en sorte que le SCRS conserve de l'information qui, par ailleurs, serait assujettie au régime des ensembles de données.

9. L'OSSNR conclut que les pratiques du SCRS en matière de gestion de l'information ont été responsables d'un certain nombre d'incidents de conformité et qu'elles donnent actuellement lieu à la création de copies d'ensembles de données dans les systèmes du Service.

10. L'OSSNR conclut qu'au mois d'août 2023, le SCRS n'avait pas respecté les dispositions de la Loi sur le SCRS concernant les ensembles de données dans la mesure où il avait conservé des informations canadiennes tirées d'ensembles de données étrangers et des informations étrangères assimilables un ensemble de données.

11. L'OSSNR conclut que le SCRS ne s'était pas conformé aux dispositions de la Loi sur le SCRS s'appliquant aux ensembles de données, dans la mesure où il a conservé des informations canadiennes et y a fait référence jusqu'à tout récemment, en 2022. Cette information aurait dû être détruite dès l'entrée en vigueur de la LSN (2017), en juillet 2019.

12. L'OSSNR conclut que le SCRS n'a pas procédé à un balayage complet de ses systèmes qui aurait permis de relever l'information assujettie au régime des ensembles de données et de la traiter conformément aux prescriptions en vigueur.

13. L'OSSNR conclut que la formation obligatoire qui permet aux employés désignés de devenir aptes à évaluer, à interroger et à exploiter les ensembles de données au titre de l'art. 11.01 contient de l'information claire sur les exigences en matière de collecte et de conservation.

14. L’OSSNR conclut que le personnel opérationnel du SCRS, y compris le personnel travaillant principalement à la collecte de volumes massifs d’information, n’a pas reçu de formation qui soit adéquate et qui leur permette de reconnaître les circonstances où l’information collectée pourrait être assujettie au régime des ensembles de données.

15. L’OSSNR conclut que le SCRS n’a pas priorisé l’affectation de ressources à l’unité technique responsable de l’évaluation, de l’interrogation et de l’exploitation des ensembles de données canadiens et étrangers.

16. L’OSSNR conclut que le SCRS n’a pas affecté suffisamment de ressources à l’amélioration de ses systèmes techniques ou à la conception de nouveaux systèmes qui soient équipés pour prendre en charge l’utilisation de volumes massifs de données.

17. L’OSSNR conclut que le SCRS a collecté de l’information ayant trait à des activités qui, faute de motifs raisonnables, ne pouvaient pas être soupçonnées de constituer une menace pour la sécurité du Canada. De plus, la collecte, l’analyse et la conservation de cette information n’étaient pas strictement nécessaires.

Recommandations de l'OSSNR
Recommandation 1 : L'OSSNR recommande que dans la prochaine demande d'autorisation judiciaire visant un ensemble de données canadien, le SCRS indique à la Cour comment il compte concrètement appliquer le régime des ensembles de données et comment l'information concernée sera utilisée en attente de la décision de la conserver au titre du régime des ensembles de données.
Recommandation 2 : L'OSSNR recommande que le SCRS détruise immédiatement tout document contenant les noms conservés pour motif de situation urgente, dans la mesure où ces documents ne répondent pas au critère minimum de la mesure strictement nécessaire.
Recommandation 3 : L'OSSNR recommande que le législateur légifère sur un délai prescrit pour l'autorisation d'un ensemble de données étranger par le Ministre ou la personne désignée.
Recommandation 4 : L'OSSNR recommande que le SCRS analyse de près et documente toute attente raisonnable en matière de protection de la vie privée, lorsqu'il s'agit d'évaluer les ensembles de données accessibles au public.
Recommandation 5 : L'OSSNR recommande que le SCRS élabore : • des lignes directrices concernant la mise en application de la section 6 de la consigne provisoire [**expurgé**] qui feront état de la façon dont ladite consigne sera conciliée avec la période d'évaluation de 90 jours prévue par le régime des ensembles de données; • une politique régissant le traitement de l'information éphémère.
Recommandation 6 : L'OSSNR recommande que le SCRS cesse de créer des copies de l'information déclarée dans le système opérationnel.
Recommandation 7 : L'OSSNR recommande que le SCRS détruise immédiatement l'information de tout ensemble de données canadien ou étranger qu'il n'est pas strictement nécessaire de conserver. Cette information ne cadre plus dans la période d'évaluation juridiquement établie à 90 jours. Il n'est donc plus possible de la conserver au titre du régime des ensembles de données.
Recommandation 8 : L'OSSNR recommande que le SCRS procède à un balayage complet de ses registres opérationnels et organisationnels dans le but de relever et de détruire toute information non conforme.
Recommandation 9 : L'OSSNR recommande que le SCRS prépare et offre des ateliers axés sur des scénarios, qui serviront à former le personnel quant à la façon dont le SCRS applique actuellement le régime des ensembles de données. Ces ateliers permettraient de faire appel aux experts, le cas échéant.
Recommandation 10 : L'OSSNR recommande que le SCRS priorise l'affectation de ressources à l'unité technique responsable de l'évaluation, de l'interrogation et de l'exploitation des ensembles de données canadiens et étrangers.

Recommandation 11 : L'OSSNR recommande que le SCRS priorise l'amélioration des systèmes techniques en place ou l'élaboration de nouveaux systèmes qui rendent possible l'utilisation des données de masses qu'il est permis d'exploiter.

Recommandation 12 : L'OSSNR recommande que le SCRS détruise immédiatement l'ensemble de données – celui qui est cité dans l'étude de cas – qu'il a collecté au titre de l'article 12, dans la mesure où cet ensemble ne répond pas aux critères minimaux prescrits par la loi. En effet, l'information ne cadre plus dans la période d'évaluation juridiquement établie à 90 jours. Il n'est donc plus possible de la conserver au titre du régime des ensembles de données.

Recommandation 13 : L'OSSNR recommande que le SCRS soumette une copie intégrale non expurgée du présent rapport à la Cour fédérale.

Examens du Centre de la sécurité des télécommunications Canada

Examen de l'utilisation par le CST du polygraphe pour le filtrage de sécurité

Conclusions de l'OSSNR

1. L'OSSNR a conclu que la gouvernance du CST en matière d'utilisation des tests polygraphiques à des fins de filtrage de sécurité s'avère inadéquate s'agissant des questions liées à la protection des renseignements personnels.

2. L'OSSNR a conclu que le CST n'a pas mené d'évaluation des facteurs relatifs à la vie privée à l'égard de son utilisation des tests polygraphiques aux fins du filtrage de sécurité.

3. L'OSSNR a conclu que le CST pourrait avoir omis de vérifier si l'information collectée pendant les tests polygraphiques était directement liée ou nécessaire à l'évaluation de la criminalité d'un particulier ou de sa loyauté envers le Canada, comme l'exigent *Loi sur la protection des renseignements personnels* et la Directive sur les pratiques relatives à la protection de la vie privée.

4. L'OSSNR a conclu que les examinateurs en polygraphie avaient utilisé une approche au cas par cas lorsqu'il s'est agi d'évaluer les renseignements à caractère médical qui ont été collectés pendant les tests polygraphiques.

5. L'OSSNR a conclu que le CST ne se serait possiblement pas conformé aux dispositions de l'article 7 de la *Loi sur la protection des renseignements personnels* en utilisant, sans le consentement des sujets, des renseignements collectés pendant les tests polygraphiques pour prendre des décisions sur le plan de l'aptitude et de l'embauche.

6. L'OSSNR a conclu que le CST fournit aux sujets de l'information qui tend à surestimer le niveau de fiabilité et de validité des tests polygraphiques, et ce, avant d'obtenir le consentement desdits sujets.

7. L'OSSNR a conclu qu'en certaines circonstances, la façon dont le CST a réalisé ses tests polygraphiques comportait le risque d'inciter les sujets à inventer de l'information pour se disculper à la suite d'une évaluation polygraphique qui leur avait été défavorable.

8. L'OSSNR a relevé des cas où les modalités de contrôle de la qualité que le CST appliquait aux tests polygraphiques n'étaient pas toujours conformes à la politique du CST.

9. L'OSSNR a conclu qu'environ 20 % des dossiers de sécurité faisant partie de l'échantillon examiné ne contenaient aucun enregistrement audiovisuel des tests polygraphiques.

10. L'OSSNR a conclu que dans tous les cas où, dès lors que les résultats de tests polygraphiques indiquaient une occurrence de tromperie ou s'avéraient non concluants, la pratique du CST consistait à réaliser plusieurs tests polygraphiques au lieu d'entamer un processus de dissipation des doutes, comme le propose la Norme.

11. L'OSSNR a conclu que le test polygraphe jouissait d'une importance excessive dans la prise de décisions faisant suite au filtrage de sécurité. Par conséquent, d'autres activités de filtrage de sécurité moins intrusives n'on été utilisées que très peu, voire pas du tout.

12. L'OSSNR a conclu que, de fait, le test polygraphique a été déterminant dans les décisions prises par le CST au terme des processus de filtrage de sécurité.

13. L'OSSNR a conclu qu'au terme du processus de filtrage de sécurité, la prise de décision par le CST pourrait ne pas être conforme aux exigences de la Norme sur le filtrage de sécurité pour ce qui concerne la tenue des dossiers.

14. L'OSSNR a conclu que la façon dont le CST utilise les tests polygraphiques lorsqu'il s'agit de prendre une décision au terme du processus de filtrage de sécurité ne garantit aucunement la possibilité de contester les refus d'accorder la cote de sécurité, ce qui contrevient aux stipulations de la Loi sur l'OSSNR et de la Norme.

15. L'OSSNR a conclu que le SCT n'a pas adéquatement prise en compte la protection des renseignements personnels et les dispositions de la Charte lorsqu'il a intégré les tests polygraphiques en tant qu'activité de filtrage de sécurité prévue par la Norme sur le filtrage de sécurité.

16. L'OSSNR a conclu que la Norme sur le filtrage de sécurité ne tient pas suffisamment compte des dispositions de la Charte ou du principe de protection des renseignements personnels lorsqu'il s'agit du recours aux tests polygraphiques.

17. L'OSSNR a conclu que tel qu'elle est décrite dans le présent rapport d'examen, la façon dont le gouvernement du Canada utilise actuellement les tests polygraphiques en tant qu'outil de filtrage de sécurité pourrait poser de sérieux problème quant à la conformité aux dispositions de la *Charte canadienne des droits et libertés*.

Recommandations de l'OSSNR
Recommandation 1 : L'OSSNR recommande que le Conseil du Trésor du Canada résolve dans les plus brefs délais les problèmes soulevés dans le cadre du présent examen relativement à la légalité, au caractère raisonnable et à la nécessité des tests polygraphiques dans le contexte du filtrage de sécurité ou ben qu'il supprime les tests polygraphiques de la Norme sur le filtrage de sécurité,
Recommandation 2 : L'OSSNR recommande que le CST résolve dans les plus brefs délais les problèmes soulevés dans le cadre du présent examen, pour ce qui a trait notamment à l'application de la Charte et de la *Loi sur la protection des renseignements personnels*, ou bien qu'il cesse de faire passer des tests polygraphiques dans le contexte du filtrage de sécurité.

Examen des solutions réseau du CST et des activités connexes liées à la cybersécurité et à l'assurance de l'information

Conclusions de l'OSSNR

1. L'OSSNR a conclu que le CST exploite un écosystème complet et intégré de systèmes, d'outils et de capacités de cybersécurité pour se protéger contre les cybermenaces et dont la conception intègre des mesures visant à protéger la vie privée des Canadiens et des personnes au Canada.

2. L'OSSNR a conclu que le CST traite tous les renseignements sur les solutions réseau (SR) comme de l'information qui se rapporte à un Canadien ou à une personne au Canada (IRCPC) et applique des mesures visant à protéger tous les renseignements acquis par l'entremise de SR.

3. L'OSSNR a conclu que les renseignements acquis par l'entremise de SR comprendront toujours, par leur nature, de l'IRCPC et de l'information pour laquelle il existe une attente raisonnable en matière de protection de la vie privée (ARVP) sur un Canadien ou une personne

au Canada. Cela n'a pas été communiqué de façon transparente dans les demandes correspondantes au ministre.

4. L'OSSNR a conclu qu'en raison d'un manque de précision dans son lien avec SPC, le CST n'a pas obtenu le consentement de responsables de systèmes pour ses activités de cybersécurité et d'assurance de l'information (CSAI) de la façon décrite au ministre.

5. L'OSSNR a conclu que SPC n'était pas pleinement au courant de ses responsabilités à titre de responsable du système, comme décrit dans les demandes du CST au ministre.

6. L'OSSNR a conclu que, malgré l'existence d'un protocole d'entente entre le CST et SPC, les organisations n'avaient pas clarifié la mise en œuvre des engagements convenus concernant les activités de SR sur les réseaux exploités par SPC.

7. L'OSSNR a conclu que le CST n'a pas expliqué au ministre pourquoi le consentement aux activités de cybersécurité du CST ne pouvait pas être raisonnablement obtenu auprès des utilisateurs des systèmes du gouvernement du Canada.

8. L'OSSNR a conclu que l'application restreinte par le CST du paragraphe 22(4) de la Loi sur le CST présente des risques juridiques et relatifs à la responsabilité et a entraîné l'acquisition par le CST de renseignements qui pourraient contrevenir à une ARVP d'un Canadien ou d'une personne au Canada. Ces renseignements provenaient d'une source acquise en dehors du régime des autorisations ministérielles.

9. L'OSSNR a conclu qu'une incompatibilité entre les paragraphes 27(1) et 22(4) de la Loi sur le CST empêche le CST d'acquérir certains renseignements de sources [*type précis*], comme [*source précise*], lorsque ces renseignements contreviennent à une ARVP d'un Canadien ou d'une personne au Canada. Certains de ces renseignements amélioreraient la capacité du CST à exécuter son mandat en matière de CSAI.

Recommandations de l'OSSNR

Recommandation 1 : L'OSSNR recommande au CST d'expliquer clairement dans ses demandes au ministre :

- que les solutions réseau permettent d'acquérir de l'IRCPC, y compris des renseignements qui contreviennent à une ARVP de Canadiens et de personnes au Canada;
- que le CST utilise, analyse et conserve ensuite ces renseignements aux fins d'activités de cybersécurité et d'assurance de l'information.

Recommandations de l'OSSNR
Recommandation 2 : L'OSSNR recommande que le CST renouvelle son protocole d'entente avec SPC pour s'assurer que le CST et SPC respectent leurs engagements respectifs, y compris tout engagement que le CST prend à l'égard du ministre concernant le rôle de SPC d'informer les responsables de systèmes à propos du programme de SR.
Recommandation 3 : L'OSSNR recommande que le CST mette à jour le protocole d'entente avec tous ses partenaires de cybersécurité afin de s'assurer que ceux-ci consentent aux activités de cybersécurité du CST et que ces ententes respectent les autorités de gouvernance contemporaines. Le CST doit continuer d'effectuer de telles mises à jour comme pratique normalisée à mesure que les autorités évoluent.
Recommandation 4 : L'OSSNR recommande au CST d'expliquer au ministre comment le consentement aux activités de cybersécurité du CST est obtenu auprès des utilisateurs des systèmes du gouvernement du Canada ou d'expliquer pourquoi ce consentement ne peut pas raisonnablement être obtenu.
Recommandation 5 : L'OSSNR recommande que le CST réexamine si les limites de l'acquisition par le CST de renseignements provenant d'une infrastructure Internet mondiale (conformément au paragraphe 22(4) de la Loi sur le CST) s'appliquent aux renseignements provenant de sources [*source précise*]. L'examen devrait comprendre une évaluation de la possibilité de recourir à l'article 8 de la *Charte canadienne des droits et libertés*, ainsi que des cas où des sources [*source précise*] pourraient contenir des renseignements qui contreviennent à une ARVP d'un Canadien ou d'une personne au Canada.
Recommandation 6 : L'OSSNR recommande que, pour poursuivre ses activités d'acquisition nécessaires à des fins de cybersécurité et d'assurance de l'information (CSAI), le CST évalue si ses sources actuelles d'information de CSAI – qui sont acquises en dehors du cadre d'une autorisation – contreviennent à une ARVP d'un Canadien ou d'une personne au Canada. Cette évaluation doit être répétée au besoin pour s'assurer que de tels renseignements ne sont pas obtenus sans une autorisation ministérielle valide.
Recommandation 7 : L'OSSNR recommande que l'article 27 de la Loi sur le CST soit modifié pour permettre au ministre d'autoriser le CST à acquérir des renseignements qui sont nécessaires à ses activités de CSAI (mais qui pourraient contenir des renseignements qui contreviennent à une ARVP d'un Canadien ou d'une personne au Canada ou à une loi fédérale) provenant de sources autres que les infrastructures et systèmes d'information fédéraux d'importance pour le gouvernement du Canada.

Examen de l'Agence des services frontaliers du Canada

Examen du programme des sources humaines confidentielles de l'ASFC

Conclusions de l'OSSNR

1. L'OSSNR a conclu que la politique de l'ASFC ne nécessite aucune approbation documentée ou évaluation des risques liés à l'utilisation d'une SHC après le processus d'inscription.

2. L'OSSNR a conclu qu'il y avait des documents incomplets associés à la période de préinscription, de sorte que le programme des SHC ne puisse pas surveiller l'ensemble des activités du programme.

3. L'OSSNR a conclu que les politiques et pratiques de l'ASFC relatives à l'obtention d'un consentement éclairé ne permettent pas d'assurer que ce consentement est obtenu systématiquement, avant que les personnes ne courent le risque de fournir des renseignements confidentiels à l'ASFC.

4. L'OSSNR a conclu que les mesures visant à atténuer les risques liés aux SHC n'étaient pas souvent existantes ou mises en œuvre.

5. L'OSSNR a conclu que l'ASFC pourrait avoir enfreint le droit relatif au privilège de l'indicateur à deux reprises.

6. L'OSSNR a conclu que les agents d'exécution dans les bureaux intérieurs ont recueilli des renseignements et promis la confidentialité, mais l'ont fait sans avoir suivi la formation requise au titre de la politique applicable visant à expliquer clairement les conséquences d'accorder la confidentialité.

7. L'OSSNR a conclu que l'approche en matière de gestion du risque décrite dans la nouvelle série de politiques de l'ASFC ne s'harmonise pas entièrement avec les principes des instructions du ministre.

8. L'OSSNR a conclu que les renseignements que l'ASFC fournira au ministre, conformément aux instructions, ne suffisent pas à communiquer l'envergure et la portée du programme SHC.

9. L'OSSNR a conclu que, dans deux cas, l'ASFC n'a pas respecté le paragraphe 12(2) de la Loi sur l'ASFC, car elle n'a pas respecté l'exigence des instructions du ministre voulant que l'ASFC

informe le ministre lorsqu'une activité de SHC « est susceptible d'avoir des répercussions néfastes importantes, comme menacer la sécurité d'une personne ».

Recommandations de l'OSSNR
Recommandation 1 : L'OSSR recommande que l'ASFC modifie sa politique afin d'exiger une évaluation des risques documentée et une approbation officielle pour utiliser une SHC pendant la période de préinscription.
Recommandation 2 : L'OSSNR recommande que l'ASFC exige que la liste de vérification de l'entrevue soit remplie au plus tard lorsque la promesse de confidentialité est faite.
Recommandation 3 : L'OSSNR recommande que l'ASFC fournisse des directives sur la façon d'obtenir un consentement éclairé adapté aux circonstances personnelles de la SHC.
Recommandation 4 : L'OSSNR recommande que l'ASFC mette en place des directives précises sur la façon d'atténuer l'ensemble des risques pour les SHC et de veiller à ce que ces mesures d'atténuation soient mises en œuvre.
Recommandation 5 : L'OSSNR recommande à l'ASFC d'élargir sa définition de source humaine confidentielle active pour que les rapports aux ministres s'appliquent à l'ensemble du PSHC.
Recommandation 6 : L'OSSNR recommande que l'ASFC avise immédiatement le ministre des deux cas ciblés dans le présent examen et dans lesquels la sécurité d'une personne est en cause.

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

Examen du Programme de gestion des sources humaines du MDN et des FAC

Conclusions de l'OSSNR

1. L'OSSNR a conclu que le cadre stratégique du MDN et des FAC permet la réalisation d'activités de gestion des sources humaines qui pourraient enfreindre la loi.

2. L'OSSNR a conclu que les politiques du MDN et des FAC ne sont pas suffisamment précises en ce qui a trait à la détection et à l'atténuation des risques de mauvais traitement engendrés par les activités de gestion des sources humaines.

3. L'OSSNR a conclu que le cadre d'évaluation des risques relatifs aux activités de gestion des sources humaines du MDN et des FAC est inadéquat. Les évaluations du risque actuelles ne fournissent pas des renseignements suffisants ou fiables aux décideurs, car :

    - ils sont trop subjectifs;
    - ils ne présentent pas clairement les risques atténués et non atténués;
    - ils confondent les risques;
    - ils concernent principalement les considérations de certains risques aux dépens des autres.

4. L'OSSNR a constaté des lacunes dans la délégation du devoir de diligence du MDN et des FAC du début à la fin du contact avec la source humaine. Ces lacunes comprennent :

    - un processus de protection qui n'est pas employé correctement pour certaines sources;
    - un processus de traitement des plaintes des sources sous-élaboré;
    - des évaluations insuffisantes du risque posé aux agents.

5. L'OSSNR a conclu que le ministre de la Défense nationale n'est pas adéquatement tenu au courant pour s'acquitter des responsabilités ministérielles relatives aux activités de gestion des sources humaines.

6. L'OSSNR a conclu que d'autres directives ministérielles sont requises pour appuyer la gouvernance du Programme de gestion des sources humaines du MDN et des FAC.

Recommandations de l'OSSNR
Recommandation 1 : L'OSSNR recommande que le Parlement adopte un cadre de justification qui autoriserait le MDN et les FAC et leurs sources à commettre des actes ou des omissions par ailleurs illégaux à l'extérieur du Canada, lorsque ceux-ci servent raisonnablement à recueillir des renseignements relatifs à la défense.
Recommandation 2 : L'OSSNR recommande que le MDN et les FAC élaborent une gouvernance stratégique pour outiller adéquatement les équipes de renseignement humain (HUMINT) sur le terrain pour qu'elles puissent mener leurs activités de gestion des sources humaines conformément à la loi. La gouvernance doit comprendre, au moins : • une attention accrue visant à déterminer si des personnes sont impliquées dans des activités terroristes; • des contrôles de gouvernance pour accroître la responsabilisation et la réactivité; • un changement aux politiques en vue de n'accepter que les renseignements dont la provenance est légale et plausible;

Recommandations de l'OSSNR

- l'élaboration d'une formation pour aider les membres à appuyer les membres des FAC dans la gestion des sources humaines, tout en atténuant les risques juridiques;
- un examen des activités en ce qui a trait à leur conformité aux obligations juridiques étrangères du Canada.

Recommandation 3 : L'OSSNR recommande que le MDN et les FAC adoptent une approche permettant d'évaluer si les échanges avec des sources humaines créent un risque sérieux de mauvais traitement qui est propre à la gestion des sources humaines, qui est globale en ce qui concerne les obligations relatives aux lois sur les droits de la personne et humanitaires internationales et qui est officialisée dans les politiques et les procédures.

Recommandation 4 : L'OSSNR recommande que le MDN et les FAC élaborent un cadre d'évaluation des risques propre à la gestion des sources humaines et comprenant une orientation doctrinale adéquate quant à l'évaluation des sources humaines, y compris la prise en compte de tous les facteurs de risque pertinents.

Tous les membres du MDN et des FAC qui participent au processus d'évaluation des risques (y compris les membres des équipes HUMINT sur le terrain, les commandants, le personnel du renseignement et les conseillers juridiques et politiques) doivent être formés sur le nouveau cadre d'évaluation des risques et l'orientation afin d'assurer l'uniformité entre les équipes et les déploiements.

Recommandation 5 : L'OSSNR recommande que le MDN et les FAC adoptent, en consultation avec d'autres ministères au besoin, des mesures additionnelles visant à assurer le bien-être et la protection des sources humaines. Ces mesures doivent être clairement mises en œuvre dans les documents de gouvernance (directives, ordonnances, procédures, etc.) et doivent aborder, au minimum, les problèmes décrits dans la conclusion 3.

Recommandation 6 : L'OSSNR recommande que le MDN et les FAC, en consultation avec le ministre de la Défense nationale, améliorent le contenu des rapports semestriels au ministre afin d'y inclure, au moins, les enjeux juridiques, politiques et de gouvernance qui pourraient avoir une incidence sur les activités de gestion des sources humaines.

Recommandation 7 : L'OSSNR recommande que, en ce qui concerne les activités de gestion des sources humaines, le MDN et les FAC créent des dossiers écrits officiels des avis et des séances d'information au ministre de la Défense nationale, ainsi que des dossiers de décision visant à améliorer la responsabilisation mutuelle.

Recommandation 8 : L'OSSNR recommande que le ministre de la Défense nationale donne au MDN et aux FAC une directive ministérielle sur la gestion des sources humaines qui comprend, au moins :

- des principes fondamentaux orientant la réalisation légale et éthique d'activités de gestion des sources humaines;
- les types de risques qui devraient être évalués et le moment où ces risques doivent être communiqués aux fins de consultations au niveau ministériel;

Recommandations de l'OSSNR
• les attentes relatives à la gestion des sources humaines; • une directive concernant le contenu et la fréquence de la reddition de compte.

Examens multiministériels

Examen de la collaboration opérationnelle entre le CST et le SCRS

Conclusions de l'OSSNR

1. L'OSSNR a conclu que le CST ne communique pas régulièrement ses plans opérationnels et ses évaluations des risques connexes au SCRS lorsqu'il exerce ses activités sous les pouvoirs du SCRS. Par conséquent, le SCRS pourrait ne pas être en mesure d'évaluer pleinement les activités du CST pour en assurer la conformité.

2. L'OSSNR a conclu que la collaboration opérationnelle étroite a créé les conditions appropriées pour que le SCRS puisse surveiller les activités d'aide du CST afin d'en assurer la conformité aux conditions du mandat.

3. L'OSSNR a conclu que le SCRS n'avait pas présenté une demande d'aide à jour au CST en temps opportun lorsqu'il cherchait de nouveaux pouvoirs conférés par mandat.

4. L'OSSNR a conclu que le CST et le SCRS n'ont pas mené d'enquête, d'évaluation ou de suivi d'un incident de conformité en collaboration.

5. L'OSSNR a conclu que le CST et le SCRS n'ont pas mis en œuvre un cadre opérationnel efficace pour leurs activités de collecte. Cela a mené à deux cas de non-conformité aux directives de la Cour fédérale.

6. L'OSSNR a conclu que le CST et le SCRS ont trouvé une occasion efficace de collaborer dans le cadre de leurs mandats respectifs et de mener une opération qui s'est avérée avantageuse tant pour le Canada que pour ses alliés.

7. L'OSSNR a conclu que, bien que le cadre opérationnel du SCRS soit suffisant, le cadre opérationnel du CST n'évaluait pas les risques juridiques et politiques propres aux opérations.

8. L'OSSNR a conclu que le CST et le SCRS n'avaient pas rédigé de conditions d'engagement conjointes, de plan opérationnel conjoint ou d'évaluations des risques conjointes.

9. L'OSSNR a conclu que l'évaluation du caractère étranger du CST ne tenait pas compte du risque accru de cibler des Canadiens dans le cadre de la collaboration avec le SCRS.

10. L'OSSNR a conclu que le CST et le SCRS ne disposent pas de politiques, de procédures et de mécanismes de reddition de comptes pour régir les messages d'information du SCRS ainsi que les demandes et les mesures connexes.

11. L'OSSNR a conclu que l'utilisation par le SCRS de messages d'information pour échanger de l'information et faire des demandes au sujet de Canadiens crée un risque élevé de non-conformité pour le CST.

12. L'OSSNR a conclu que l'application par le CST des dispositions relatives à la collecte accidentelle pourrait ne pas être appropriée dans les situations où le CST sait qu'une source potentielle de renseignements étrangers du SCRS a un lien avec le Canada et où il sait qu'il est probable de recueillir des renseignements sur des Canadiens dans la poursuite de la source.

13. L'OSSNR a conclu que le CST ne s'était pas conformé aux dispositions du paragraphe 22(1) de la Loi sur le CST lorsqu'il a [*examiné le contenu*] d'un dispositif appartenant à un Canadien, laquelle avait été acquise par l'intermédiaire d'un message contenant des pistes fournies par le SCRS.

14. L'OSSNR a conclu que le CST ne s'était pas conformé au paragraphe 22(1) de la Loi sur le CST ou à l'alinéa 273.64(2)a) de la *Loi sur la défense nationale* lorsqu'il a utilisé [*un certain nombre de*] rapports spéciaux à des fins de renseignement étranger.

15. L'OSSNR a conclu que le CST n'utilise pas systématiquement son outil d'entité protégée pour empêcher le ciblage des renseignements d'identification de Canadiens qu'il reçoit du SCRS.

16. L'OSSNR a conclu que, même si le SCRS effectue une consultation initiale, il ne poursuit pas régulièrement des consultations additionnelles avec le CST pendant les activités de mesure de réduction des menaces qui pourraient chevaucher les activités du CST.

17. L'OSSNR a conclu que le CST n'a pas avisé le SCRS en temps opportun d'un incident de conformité relatif à une cyperopération active, qui était lié à une mesure de réduction des menaces du SCRS.

18. L'OSSNR a conclu que le CST n'a pas coopéré efficacement avec le SCRS, ce qui a donné lieu à une occasion manquée de faire progresser les objectifs canadiens en matière de renseignement grâce à une collaboration nationale.

Recommandations de l'OSSNR
Recommandation 1 : L'OSSNR recommande que le CST communique ses plans opérationnels et ses évaluations des risques connexes au SCRS avant de travailler sous les pouvoirs du SCRS.
Recommandation 2 : L'OSSNR recommande que, lorsque le SCRS communique avec le CST pour obtenir de l'aide dans l'exécution des pouvoirs justifiés, un employé du SCRS participe à la vérification de la conformité aux activités de collecte du CST jusqu'à la fin de la demande d'aide.
Recommandation 3 : L'OSSNR recommande que le SCRS élabore un processus pour veiller à ce que les demandes d'aide nécessaires soient soumises au CST en temps opportun après l'obtention des pouvoirs conférés par mandat.
Recommandation 4 : L'OSSNR recommande, lorsqu'il s'agit d'une demande d'aide, le SCRS et le CST élaborent un cadre d'enquête conjointe sur les incidents de non-conformité potentiels.
Recommandation 5 : L'OSSNR recommande que le SCRS s'assure que les rôles et les responsabilités sont clairement convenus avant de permettre aux partenaires d'exécuter des mandats. S'il y a lieu, ces ententes devraient être communiquées à la Cour fédérale.
Recommandation 6 : L'OSSNR recommande que le SCRS s'assure qu'il participe directement à toutes les communications de fond avec tout partenaire qui exécute activement ses pouvoirs conférés par mandat.
Recommandation 7 : L'OSSNR recommande que le SCRS communique les paragraphes 32 à 41 du présent examen, ainsi que les recommandations connexes, à la Cour fédérale.
Recommandation 8 : L'OSSNR recommande que, lorsque le CST participe à des opérations conjointes avec le SCRS, il effectue des évaluations des risques pour chaque activité opérationnelle. Ces évaluations devraient particulièrement tenir compte du risque de cibler des Canadiens et mettre en œuvre des mesures proactives pour atténuer ce risque.
Recommandation 9 : L'OSSNR recommande que, lorsqu'ils participent à des opérations conjointes, le CST et le SCRS élaborent conjointement ou échangent des conditions d'engagement, des plans opérationnels et des évaluations des risques.
Recommandation 10 : L'OSSNR recommande que le CST effectue des évaluations du caractère étranger du CST qui tiennent compte du risque accru de cibler des Canadiens dans le cadre de la collaboration avec le SCRS.

Recommandations de l'OSSNR
Recommandation 11 : L'OSSNR recommande au SCRS de cesser de présenter des demandes d'action ou d'obtention d'autres renseignements au CST concernant des Canadiens ou des personnes au Canada par l'entremise de messages d'information du SCRS.
Recommandation 12 : L'OSSNR recommande que le SCRS élabore des politiques, des procédures et une formation pour les analystes afin de normaliser la divulgation des messages d'information du SCRS au CST.
Recommandation 13 : L'OSSNR recommande que le CST élabore des politiques, des procédures et une formation des analystes afin de normaliser l'utilisation des messages d'information du SCRS.
Recommandation 14 : L'OSSNR recommande que le CST élabore un régime pour la collecte et la conservation de renseignements canadiens et la production de rapports au SCRS sur les renseignements canadiens qu'il découvre dans le cadre d'activités légitimes de renseignement étranger lorsqu'il acquiert une connaissance approfondie de l'information canadienne.
Recommandation 15 : L'OSSNR recommande que le CST mette à jour ses politiques afin d'interdire l'analyse de renseignements relatifs à un Canadien ou à une personne au Canada dans le but de cerner des renseignements étrangers.
Recommandation 16 : L'OSSNR recommande que, si le SCRS décide de divulguer des rapports exceptionnels au CST, il extraie les renseignements étrangers pertinents aux fins de divulgation plutôt que d'envoyer le rapport complet.
Recommandation 17 : L'OSSNR recommande que le CST cesse d'utiliser des rapports spéciaux complets du SCRS dans le cadre de son mandat en matière de renseignement étranger.
Recommandation 18 : L'OSSNR recommande que le CST impose une exigence de toujours appliquer l'outil d'entité protégée à tous les renseignements d'identification de Canadiens.
Recommandation 19 : L'OSSNR recommande que le SCRS entreprenne une collaboration régulière avec le CST pendant la mise en œuvre de ses mesures de réduction de la menace lorsque le risque de chevauchement opérationnel existe.
Recommandation 20 : L'OSSNR recommande que le CST communique les détails des incidents de non-conformité potentiels au SCRS lorsqu'il peut y avoir un chevauchement avec une mesure de réduction des menaces du SCRS.

Examen des communications d'information par les institutions fédérales au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* en 2022[17]

Conclusions de l'OSSNR

1. L'OSSNR a conclu que le CST, le SCRS, AMC et IRCC font régulièrement usage de la LCISC d'une manière qui justifie la conclusion d'ententes de communication d'information, comme l'encourage l'alinéa 4c) de la LCISC.

2. L'OSSNR a conclu que l'ASFC, le MDN/FAC et IRCC ont contrevenu au paragraphe 9(3) de la LCISC, car ils ne lui ont pas fourni tous les documents produits en vertu des paragraphes 9(1) et 9(2) dans les délais prescrits par la Loi.

3. L'OSSNR a conclu une amélioration des résultats en matière de conformité dans les cas où les ministères ont préparé des tableaux sommaires des communications présentant un aperçu des documents, conformément aux paragraphes 9(1) et 9(2) de la LCISC. Ces tableaux présentaient les caractéristiques suivantes :

    - une ligne pour chaque communication faite ou reçue;
    - des colonnes explicitement liées à chacun des alinéas de l'article 9;
    - des colonnes supplémentaires pour saisir des détails administratifs pertinents tels que le fait de savoir si la communication a été demandée ou faite de façon proactive, la date de la demande (le cas échéant) et tout numéro de référence de dossier applicable.

4. L'OSSNR a conclu que toutes les institutions fédérales se sont conformées à leur obligation de préparer et de conserver des documents qui contiennent les renseignements prescrits par les paragraphes 9(1) et 9(2) de la LCISC.

5. L'OSSNR a conclu que plus de la moitié des descriptions fournies par l'ASFC et IRCC au titre de l'alinéa 9(1)e) de la LCISC ne faisaient pas explicitement état de leur certitude que la communication avait été autorisée en vertu de l'alinéa 5(1)b), c'est à dire qu'elle satisfaisait au critère de proportionnalité.

---

[17] Voir l'intégralité de l'examen expurgée : https://nsira-ossnr.gc.ca/fr/publications/operations-du-secretariat/examen-des-communications-dinformation-par-les-institutions-federales-au-titre-de-la-loi-sur-la-communication-dinformation-ayant-trait-a-la-securite-du-canada-en-2022/

6. L'OSSNR a conclu, dans l'échantillon des communications à l'étude, que les institutions qui communiquent de l'information ont montré qu'elles ont satisfait aux critères de contribution et de proportionnalité, conformément au paragraphe 5(1) de la LCISC.

7. L'OSSNR a conclu qu'AMC s'était assuré du respect du critère de contribution de l'alinéa 5(1)a) de la LCISC sur la base d'une mauvaise compréhension du mandat de sécurité nationale du destinataire dans deux cas.

8. L'OSSNR a conclu, dans l'échantillon des communications à l'étude, que l'ASFC et AMC (dans une et deux communications, respectivement) n'avaient pas respecté l'exigence prévue au paragraphe 5(2) de la LCISC, qui consiste à fournir une déclaration concernant l'exactitude et la fiabilité.

9. L'OSSNR a conclu, en ce qui concerne les autres communications faisant partie de l'échantillon, qu'AMC, IRCC et la GRC incluaient leurs déclarations concernant l'exactitude et la fiabilité dans le corps des communications, tandis que l'ASFC fournissait ses déclarations dans les lettres d'accompagnement des communications.

10. L'OSSNR a conclu que le MDN/FAC a détruit des renseignements personnels au titre du paragraphe 5.1(1) de la LCISC, mais n'a pas respecté l'exigence selon laquelle cela doit être fait « dès que possible après leur réception ».

11. L'OSSNR a constaté des retards, en relation d'au moins 20 % des communications (n=34), entre le moment où une communication a été autorisée et le moment où la personne désignée par le responsable de l'institution destinataire l'a reçue.

Recommandations de l'OSSNR
Recommandation 1 : L'OSSNR recommande que des ententes de communication d'information soient utilisées pour régir les communications régulières faites au titre de la LCISC entre AMC et le SCRS, entre IRCC et le SCRS et entre IRCC et le CST.
Recommandation 2 : L'OSSNR recommande à toutes les institutions fédérales de préparer un aperçu des documents afin de s'assurer de répondre aux exigences des paragraphes 9(1) et 9(2) de la LCISC et de le lui faire parvenir accompagné d'une copie de la communication proprement dite et, s'il y a lieu, d'une copie de la demande.
Recommandation 3 : L'OSSNR recommande que les institutions qui communiquent de l'information tiennent compte explicitement des exigences des alinéas 5(1)a) et 5(1)b) dans les documents qu'elles préparent au titre de l'alinéa 9(1)e) de la LCISC.

Recommandations de l'OSSNR
Recommandation 4 : L'OSSNR recommande aux institutions fédérales qui envisagent d'avoir recours à des communications proactives en vertu de la LCISC de contacter l'institution destinataire avant de procéder afin d'éclairer leurs évaluations au titre du paragraphe 5(1).
Recommandation 5 : L'OSSNR recommande à toutes les institutions qui communiquent de l'information d'inclure les déclarations concernant l'exactitude et la fiabilité dans le document où se trouve l'information communiquée.
Recommandation 6 : L'OSSNR recommande aux institutions fédérales de revoir leurs processus administratifs pour l'envoi et la réception de communications d'information au titre de la LCISC, en plus de modifier leurs pratiques qui entraînent des retards.

Examen de 2022 portant sur la mise en œuvre par les ministères de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*

Conclusions de l'OSSNR

1. L'OSSNR a conclu que tous les ministères, à l'exception du MPO, en ce qui concerne le paragraphe 7(1), se conformaient aux exigences de déclaration énoncées dans la LCMTIEE.

2. L'OSSNR a conclu que tous les ministères avaient des cadres pour régir leur mise en œuvre de la LCMTIEE et de ses orientations connexes d'ici la fin de 2022.

3. L'OSSNR a constaté que la plupart des ministères ont continuellement peaufiné leurs cadres liés à la LCMTIEE en se fondant sur des lacunes cernées à l'interne, des recommandations de l'OSSNR et des efforts de coordination à l'échelle de la communauté.

4. L'OSSNR a conclu que le cadre de gouvernance de la LCMTIEE de Transports Canada (TC) ne comprenait pas les politiques et les procédures relatives à :

    a) le renvoi des cas à l'administrateur général; ou

    b) l'évaluation des risques de l'échange de renseignements avec des entités étrangères.

5. L'OSSNR a conclu que tous les ministères, à l'exception du MPO, d'AMC, de SP et de TC, ont utilisé des évaluations des risques des pays ou des entités pour éclairer leur évaluation du risque substantiel de mauvais traitements et du renvoi de cas.

6. L'OSSNR a conclu que les évaluations des risques des ministères par pays ne concordaient pas entre elles.

7. L'OSSNR a conclu que la réalisation simultanée d'évaluations indépendantes des risques liés aux droits de la personne dans différents ministères a produit un dédoublement important des efforts dans l'ensemble du gouvernement du Canada et a créé le risque de produire des résultats divergents.

8. L'OSSNR a conclu, pour la quatrième année consécutive, qu'aucun ministère n'a renvoyé des cas à ses administrateurs généraux aux fins de décision.

9. L'OSSNR a conclu que certaines activités d'échange à risque élevé ont été interrompues avant le renvoi visant à cerner des mesures d'atténuation possibles.

10. L'OSSNR a conclu que certains cadres de gouvernance de la LCMTIEE et certaines méthodes d'évaluation des risques des ministères comprenaient des caractéristiques qui pourraient systématiquement sous-évaluer le niveau de risque associé à une transaction. Ces caractéristiques comprennent :

    - différentes applications du seuil de risque sérieux de mauvais traitement;
    - l'intégration de mesures d'atténuation dans les évaluations de base des risques, menant à la surestimation de leur incidence;
    - un manque de vérifications et de contrepoids dans le processus d'évaluation des risques.

Recommandations de l'OSSNR
Recommandation 1 : L'OSSNR recommande à TC de mettre à jour son cadre de gouvernance de la LCMTIEE afin d'y inclure les politiques et les procédures pour : a) le renvoi des cas à l'administrateur général; b) l'évaluation des risques de l'échange de renseignements avec des entités étrangères.
Recommandation 2 : L'OSSNR recommande que le gouvernement du Canada désigne un organisme chargé d'élaborer : a) un ensemble harmonisé d'évaluations de la situation des droits de la personne dans les pays étrangers, qui inclut pour chaque pays le niveau de classification normalisé des « risques de mauvais traitements »; b) des évaluations normalisées des risques de mauvais traitements liés à l'échange de renseignements avec des entités étrangères, dans la mesure où plusieurs ministères traitent avec les mêmes entités au sein d'un pays donné. Examen 2019-06 de l'OSSNR.

Recommandations de l'OSSNR
Recommandation 3 : L'OSSNR recommande aux ministères d'appliquer le seuil de « risque sérieux » d'une manière conforme à la définition adoptée à l'échelle du gouvernement; et que les ministères dont les cadres stratégiques plus larges ne comprennent pas encore cette définition (ASFC, ARC, IRCC et TC) fassent les mises à jour requises.
Recommandation 4 : L'OSSNR recommande que les évaluations ministérielles du risque sérieux de mauvais traitements soient fondées sur les dossiers des pays en matière de droits de la personne; et que les considérations subséquentes quant à l'entité soient fondées sur le respect validé, actuel et cohérent des mises en garde et garanties, plutôt que sur l'absence de renseignements dérogatoires propres sur cette entité ou d'autres considérations bilatérales.
Recommandation 5 : L'OSSNR recommande que tous les cadres de gouvernance de la LCMTIEE intègrent des vérifications et des contrepoids à plusieurs niveaux dans l'évaluation des risques et le renvoi de cas qui pourraient comporter un risque sérieux de mauvais traitements.

Annexe C : Statistiques concernant les enquêtes sur les plaintes

Du 1er janvier au 31 décembre 2023

DEMANDES DE TRAITEMENT DE PLAINTE REÇUES		135
Nombre de nouvelles plaintes déposées		**26**
Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (Loi sur l'OSSNR), article 16, plaintes visant le Service canadien du renseignement de sécurité (SCRS)		18
Loi sur l'OSSNR, article 17, plaintes visant le Centre de la sécurité des télécommunications (CST)		5
Loi sur l'OSSNR, article 18, habilitations de sécurité		3
Loi sur l'OSSNR, article 19, plaintes renvoyées par la Gendarmerie royale du Canada (GRC)		0
Loi sur l'OSSNR, article 19, *Loi sur la citoyenneté*		0
Loi sur l'OSSNR, article 45, renvois par la Commission canadienne des droits de la personne (CCDP)		0
Décision sur la compétence d'enquêter		**8**
	Acceptée	Rejetée
Loi sur l'OSSNR, article 16, plaintes visant le SCRS	6	17
Loi sur l'OSSNR, article 17, plaintes visant le CST	1	4
Loi sur l'OSSNR, article 18, habilitations de sécurité	0	1
Loi sur l'OSSNR, article 19, plaintes renvoyées par la GRC	1	0
Total	8	22
Enquêtes actives au 31 décembre 2023		**17**
Loi sur l'OSSNR, article 16, plaintes visant le SCRS		8
Loi sur l'OSSNR, article 17, plaintes visant le CST		1
Loi sur l'OSSNR, article 18, habilitations de sécurité		4

Loi sur l'OSSNR, article 19, plaintes renvoyées par la GRC	3
Loi sur l'OSSNR, article 19, poursuite de l'enquête (plaintes renvoyées par la GRC) [a]	1
Résolutions à l'amiable en cours en date du 31 décembre 2023	**1**
Loi sur l'OSSNR, article 16, plaintes visant le SCRS	0
Loi sur l'OSSNR, article 17, plaintes visant le CST	0
Loi sur l'OSSNR, article 18, habilitations de sécurité	1
Loi sur l'OSSNR, article 19, plaintes renvoyées par la GRC	0
Nombre total d'enquêtes closes	**12**

	Abandonnée	Rapport final	Réglée à l'amiable	Retirée
Loi sur l'OSSNR, article 16, plaintes visant le SCRS	0	4	3	0
Loi sur l'OSSNR, article 17, plaintes visant le CST	0	0	1	0
Loi sur l'OSSNR, article 18, habilitations de sécurité	0	0	0	0
Loi sur l'OSSNR, article 19, plaintes renvoyées par la GRC	1	3	0	0
Loi sur l'OSSNR, article 45, renvois par la CCDP	0	0	0	0
Total	1	7	4	0

[a] Le premier rapport final a été produit en 2022. L'enquête concerne une question non résolue.