



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

National Security and
Intelligence Review
Agency



OSSNR

L'organisme d'examen indépendant du Canada pour
toutes les activités en matière de sécurité nationale et de
renseignement

Rapport annuel 2019

Canada 

© Sa Majesté la Reine du chef du Canada, représentée par l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, 2020.

ISSN 2563-5786

N° de catalogue : PS106-9F-PDF

Le 20 novembre 2020

Le très honorable Justin Trudeau, C.P., député
Premier ministre du Canada
Bureau du premier ministre et 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, j'ai le plaisir de vous présenter notre premier 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 pendant 2019, ainsi que nos conclusions et nos recommandations. Conformément aux dispositions transitoires 12(1) et 12(2) de la *Loi de 2017 sur la sécurité nationale*, ce rapport comprend également des renseignements que nos prédécesseurs, le Comité de surveillance des activités de renseignement de sécurité et le Bureau du commissaire du Centre de la sécurité des télécommunications, n'avaient pas encore rendus publics.

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 la consultation des administrateurs généraux concernés afin de s'assurer qu'il ne contient pas des informations dont la communication porterait atteinte à la sécurité nationale ou à la défense nationale ou aux relations internationales ou des informations protégées par le secret professionnel de l'avocat ou du notaire ou par le privilège relatif au litige.

Je vous prie d'agréer, Monsieur le Premier ministre, l'assurance de ma très haute considération

A handwritten signature in blue ink, consisting of a stylized 'I' followed by a horizontal line and a large, sweeping flourish that extends to the left.

L'honorable Ian Holloway, Ph. D., C.P., C.D., c.r.

Président suppléant

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



OSSNR

L'organisme d'examen indépendant du Canada pour toutes les
activités en matière de sécurité nationale et de renseignement

Rapport annuel 2019

Table des matières

Message du Comité	ii
Résumé	v
Introduction	14
Partie 1 : Création d'une institution	16
Examen	16
Enquêtes sur les plaintes	17
Valeurs de l'OSSNR	18
Partie 2 : Examen	20
Section I — Le continuum de l'information	20
Section II — Collecte	22
Section III — Protection	35
Partie IV — Échange d'information	42
Section V — Actions	51
Partie 3 : Plaintes	58
Section I — Mandat de l'OSSNR en matière d'enquête sur les plaintes	58
Section II — Synopsis des tendances et des principaux thèmes	60
Section III — Protection des dénonciateurs	61
Section IV — Priorités pour l'année à venir	62
Partie 4 : Engagement et transparence	64
Section I — Engagement	66
Section II — Transparence	67
Conclusion	68
Annexe A : Résumés des examens de l'OSSNR terminés pendant la période de rapport	69
Annexe B : Résumés des examens non publiés du CSARS et du BCCST jusqu'en juillet 2019	80
Annexe C : Résumés des enquêtes sur les plaintes	85
Annexe D : Tableau statistique des plaintes	90
Annexe E : Organisation, réalisations et priorités de l'OSSNR	92
Annexe F : Liste des abréviations	95
Notes de fin de document	96



Message du Comité

Nous sommes fiers de présenter le premier rapport annuel de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) pour les travaux entrepris en 2019. Notre loi habilitante exige que nous présentions chaque année au Parlement un rapport sur nos activités au cours de l'année civile précédente, y compris tout examen qui n'a pas encore été rendu public par nos prédécesseurs, le Comité de surveillance des activités de renseignement de sécurité et le Bureau du commissaire du Centre de la sécurité des télécommunications. Ce faisant, notre rapport traite de nos activités dans un cadre qui tient compte de l'approche complexe, multiagences et interdépendante qu'adopte le Canada en matière de sécurité nationale.

Nous sommes en premier lieu un organisme rétrospectif, c'est-à-dire que nous examinons généralement les activités qui ont déjà eu lieu et que nous tirons des conclusions quant à leur conformité à la loi et aux instructions ministérielles. Nous examinons également le caractère raisonnable et la nécessité pour un ministère d'exercer ses pouvoirs. Nous sommes très conscients de la nécessité pour les parlementaires et tous les Canadiens d'avoir accès à nos conclusions en temps opportun. L'OSSNR est déterminé à publier les examens caviardés dès que possible après leur envoi au ministre concerné. Nous espérons que notre rapport annuel sera un mécanisme de réflexion sur les tendances et les thèmes plus généraux qui touchent l'ensemble de notre travail. Nous croyons fermement que cette approche fait partie intégrante de notre mandat et qu'elle est appuyée par l'engagement du gouvernement pour une plus grande transparence en matière de sécurité nationale.

L'ouverture signifie également approfondir le dialogue avec les Canadiens sur la sécurité nationale. Nous nous sommes exposés à un ensemble diversifié de points de vue pour nous assurer que notre plan d'examen reflète les préoccupations et les priorités de tous les Canadiens. Cela est particulièrement important dans le contexte des mouvements antiracistes qui se manifestent partout dans le monde. Nous espérons que notre engagement auprès de diverses communautés aidera notre organisation à déterminer la meilleure façon de contribuer à la lutte contre le racisme et la discrimination dans le domaine de la sécurité nationale et du renseignement. La mobilisation des experts canadiens, des communautés culturelles et de la société civile a déjà commencé comme nous renforçons notre présence dans les médias sociaux et notre capacité d'organiser des vidéoconférences et des réunions en personne. Nous avons rencontré plusieurs intervenants à Ottawa, à Victoria, à Toronto et à Calgary, et d'autres activités sont prévues au cours de l'année à venir. À l'échelle internationale, nous travaillons et partageons nos expériences avec des organismes d'examen parallèles en tant que membre du Conseil de surveillance

et d'examen du renseignement du Groupe des cinq, qui est composé de nos partenaires en Australie, en Nouvelle-Zélande, au Royaume-Uni et aux États-Unis.

Nous sommes conscients de la nécessité d'éviter les chevauchements avec d'autres organismes d'examen et de faire le meilleur usage possible des ressources en place au sein de la communauté de la sécurité nationale pour faciliter notre travail. On comprend que, pour de nombreux ministères et organismes, l'examen externe est une nouvelle entreprise, et ils auront besoin de temps pour s'adapter. Nous sommes très heureux du niveau de coopération et de soutien que nous constatons. Nous avons élaboré et partagé notre plan d'examen triennal qui, nous l'espérons, clarifiera nos priorités de travail et donnera aux organisations que nous examinerons le temps de s'adapter et de se préparer. Notre loi est sans équivoque en ce qui concerne l'accès à l'information; nous avons le droit d'avoir accès en temps opportun à tout ce qui est en la possession ou sous le contrôle d'un ministère en lien avec nos examens (à l'exception seulement des documents confidentiels du Cabinet). Cet accès est essentiel pour l'intégrité de notre travail. Nos rapports publics feront donc état de toute lacune à cet égard. Afin d'éviter les chevauchements et d'améliorer le système de responsabilisation en matière de sécurité nationale du Canada, nous sommes déterminés à collaborer avec d'autres organismes de surveillance et d'examen, y compris le Bureau du commissaire au renseignement, le Comité des parlementaires sur la sécurité nationale et le renseignement, le Commissariat à la protection de la vie privée du Canada (CPVP), la Commission civile d'examen et de traitement des plaintes relatives à la GRC et le Bureau du vérificateur général du Canada.¹

L'OSSNR regroupe également sous un même toit les enquêtes sur les plaintes liées à la sécurité nationale qui sont déposées par des membres du public. Nous avons le mandat d'enquêter sur les plaintes relatives aux activités du Service canadien du renseignement de sécurité, à celles du Centre de la sécurité des télécommunications et des activités liées à la sécurité nationale de la Gendarmerie royale du Canada. De plus, nous pouvons enquêter sur les plaintes d'une personne dont l'habilitation de sécurité est refusée ou révoquée, ainsi que sur les affaires portées à son attention par la Commission canadienne des droits de la personne² et sur certaines questions relevant de la *Loi sur la citoyenneté*. Nous sommes convaincus que ce regroupement des enquêtes sur les plaintes aidera à faire en sorte que le traitement des griefs liés à la sécurité nationale des Canadiens soit plus uniforme, de meilleure qualité et le plus rapide possible. Nous nous pencherons particulièrement, au cours de la prochaine année, sur l'amélioration de l'efficacité du processus de traitement des plaintes.

Nous manquerions à notre devoir si nous ne tenions pas compte de l'environnement unique et difficile auquel nous sommes tous confrontés en ce moment. La pandémie de la COVID-19 a eu des conséquences profondes dans le monde que nous commençons peut-être à peine à comprendre. Pendant la majeure partie de 2020, le personnel de l'OSSNR a travaillé à domicile, avec un accès minimal au bureau et, par conséquent, aux documents classifiés physiques et électroniques qui doivent être conservés dans un espace sécurisé. Nous sommes très fiers du travail extraordinaire de notre personnel, qui a maintenu son élan pendant cette période difficile et qui continue de mettre en place des mesures pour améliorer notre adaptabilité organisationnelle. Nous nous attendons également à ce que les organisations sur lesquelles portent nos examens et nos enquêtes sur les plaintes, qui elles aussi doivent s'adapter à une situation en constante évolution, continuent d'affecter du personnel à ces fonctions essentielles et continuent de considérer comme une priorité l'obligation de rendre des comptes liée à la sécurité nationale.

Pour le moment, nous tenons à exprimer notre gratitude à trois membres de l'OSSNR dont le mandat a pris fin cette année : l'honorable Pierre Blais, l'honorable L. Yves Fortier et Murray Rankin, le premier président de l'OSSNR. Leur collégialité et leur leadership en période de transition ont été grandement appréciés, et leur contribution à la responsabilisation en matière de sécurité nationale au Canada continue d'être profondément ressentie.

Nous sommes honorés d'avoir été choisi en tant que premiers membres de l'OSSNR. Nous sommes déterminés à présenter des conclusions et des recommandations significatives sur la mesure dans laquelle la communauté de la sécurité nationale du Canada se conforme à la loi, ainsi que sur la nécessité et le caractère raisonnable de ses actions. Nous avons hâte de relever le défi qui nous attend dans cet environnement de plus en plus complexe.

L'honorable Ian Holloway, Ph. D., C.P., C.D., c.r. (président suppléant)

L'honorable Marie Deschamps, C.C.

Professeur Craig Forcese

L'honorable Marie-Lucie Morin, C.P., C.M.

L'honorable Pierre Blais, C.P. (membre jusqu'en mai 2020)

L'honorable L. Yves Fortier, C.P., C.C., O.Q., c.r. (membre jusqu'en octobre 2020)

Murray Rankin, c.r., (membre et président jusqu'en septembre 2020)



Résumé

- Les renseignements relatifs à la transition du Comité de surveillance des activités de renseignement de sécurité (CSARS) à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), les jalons organisationnels, les valeurs et les objectifs organisationnels et d'autres éléments pertinents sont brièvement décrits dans l'introduction et sont complétés par des documents plus détaillés dans diverses annexes ainsi que sur le site Web de l'OSSNR³.
- Les constatations et les thèmes abordés dans le présent rapport reflètent le travail de l'OSSNR au cours des premiers mois de notre mandat, à compter de juillet 2019. Elles s'appuient également sur le travail effectué par le CSARS et le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST), y compris les examens que ces organisations n'avaient pas encore publiés avant l'établissement de l'OSSNR. Des résumés de ces examens se trouvent aux annexes A et B. Nous abordons les constatations et les thèmes du présent rapport en fonction du « continuum d'information », c'est-à-dire la collecte, la protection, l'échange et l'action.
- L'un des principaux défis que doivent relever les ministères et organismes au Canada consiste à s'assurer que leur utilisation des nouvelles technologies est conforme aux lois sur la protection des renseignements personnels et respecte les droits des Canadiens en vertu de la *Charte canadienne des droits et libertés* (la Charte). L'OSSNR est au courant de cas où un organisme a utilisé la technologie d'une manière qui dépassait les autorisations légales. L'un des premiers examens de l'OSSNR portait notamment sur l'utilisation des données de géolocalisation accessibles au public par le Service canadien du renseignement de sécurité (SCRS). L'OSSNR a conclu que l'utilisation sans mandat de ces données par le SCRS risquait de contrevenir à l'article 8 de la Charte, qui protège contre les fouilles, les perquisitions et les saisies abusives. L'OSSNR a présenté un rapport en vertu de l'article 35 de la Loi sur l'OSSNR au ministre de la Sécurité publique et de la Protection civile au sujet de l'activité illégale possible⁴.
- Le rapport donne un aperçu de certains problèmes de longue date du SCRS quant à leurs manquements face à l'obligation de franchise envers la Cour fédérale, notamment en ce qui concerne ses activités liées aux sources humaines⁵. Plus précisément, le SCRS n'a pas informé la Cour que les demandes de mandat du SCRS étaient fondées sur du renseignement qui avait

probablement été recueilli par des moyens illégaux. La Cour a également observé des lacunes en ce qui concerne le rôle du ministère de la Justice dans la situation. En réponse, le gouvernement a renvoyé la question à l'OSSNR aux fins d'examen en vertu de l'alinéa 8(1)c) de la Loi sur l'OSSNR. Au cours de la prochaine année, l'OSSNR consacrera d'importantes ressources à un examen découlant de cette décision de la Cour fédérale.

- L'OSSNR a accordé la priorité à la protection (c.-à-d. la façon dont le gouvernement protège les personnes, l'information et les biens) comme thème annuel d'examen. Au cours de notre première année d'existence, l'OSSNR a effectué un examen des mesures de protection du SCRS et en a entrepris un autre au sein du ministère de la Défense nationale (MDN). À noter, nos observations en ce qui a trait au polygraphe (ou « détecteur de mensonges ») dans le cadre du processus d'attribution des autorisations de sécurité, mettent en évidence un certain nombre de lacunes, dont les suivantes :
 - Le SCRS n'a pas été en mesure de démontrer la compétence des examinateurs, qui ne sont pas médecins, pour poser des questions d'ordre médical aux candidats.
 - Les résultats ou les répercussions des examens polygraphiques étaient inéquitables, selon que le candidat venait de l'extérieur du SCRS ou qu'il était déjà un employé.
- Cette conclusion soulève des questions plus vastes. Bien que la Norme sur le filtrage de sécurité du Secrétariat du Conseil du Trésor (SCT), créée en 2014, mentionne l'utilisation du polygraphe comme outil approprié pour évaluer les candidats qui demandent une habilitation de sécurité approfondie de niveau « Très secret », le SCT n'a pas été en mesure de fournir de justification stratégique de l'utilisation de cet outil. L'OSSNR a porté un certain nombre de lacunes à l'attention du SCT. La norme fait actuellement l'objet d'un examen interne au SCT, et nous sommes en attente des résultats.
- L'OSSNR a fait plusieurs constatations et recommandations au Centre de la sécurité des télécommunications (CST) pour améliorer ses pratiques de documentation, d'atténuation et de protection de la vie privée en ce qui a trait au dossier des incidents liés à la protection des renseignements personnels.
- En 2019, l'OSSNR a réalisé notre premier examen interorganismes. Il s'agissait d'une évaluation de la mise en œuvre des instructions ministérielles sur l'échange

d'information avec des entités étrangères de 2017 par l'Agence des services frontaliers du Canada, le CST, le SCRS, le MDN, Affaires mondiales Canada et la Gendarmerie royale du Canada. L'OSSNR a constaté que la réussite de la mise en œuvre des instructions ministérielles variait beaucoup parmi les six ministères et organismes. Certains ministères ou organismes, comme le SCRS et le CST, avaient adopté des procédures relativement avancées pour mettre en œuvre les instructions, mais l'examen a permis de relever quelques lacunes. Certains ministères et organismes ont de la difficulté à concrétiser ces instructions. D'autres ont de la difficulté à établir des mécanismes décisionnels indépendants de la première ligne opérationnelle dans les cas où il existe un risque de mauvais traitement. L'application non uniforme du critère relatif au « risque sérieux de mauvais traitement » entre les ministères est une lacune principale relevée par l'OSSNR dans son examen. D'après les instructions de 2017 et leurs versions suivantes, l'échange d'information est interdit lorsqu'il existe un risque sérieux de mauvais traitement d'une personne par une entité étrangère. La façon dont les ministères et organismes évaluent ce critère fera l'objet de travaux futurs.

- En 2020-2021, l'OSSNR modernise le processus de traitement des *plaintes*. Notre objectif ne changera pas les faits d'assurer une enquête juste et efficace, et le règlement des plaintes. Deux priorités guideront la modernisation, soit l'accès à la justice pour les plaignants non représentés et le besoin d'un plus large éventail d'outils pour simplifier le règlement des plaintes.
- Dans une correspondance antérieure adressée au procureur général, l'OSSNR a relevé des lacunes législatives liées à la protection des dénonciateurs au sein de la communauté de la sécurité nationale du Canada et les répercussions négatives correspondantes découlant de ces lacunes⁶. Entre-temps, l'OSSNR mettra en œuvre des procédures internes pour répondre aux préoccupations soulevées par les membres de l'appareil de la sécurité et du renseignement.
- En 2019, l'OSSNR a lancé une série de consultations publiques afin de mieux faire connaître notre nouvelle organisation, d'élargir notre réseau et d'approfondir notre compréhension des préoccupations des Canadiens concernant les activités de sécurité nationale et de renseignement. Au cours de la prochaine année, l'OSSNR a l'intention de poursuivre notre programme de sensibilisation et d'engagement, en mettant l'accent sur quatre domaines clés, soit : développer notre réseau pour aider à régler les problèmes liés aux technologies nouvelles et émergentes (y compris l'intelligence artificielle); élargir notre dialogue avec les intervenants pour éclairer les futures priorités d'examen de l'OSSNR; établir de nouvelles relations avec les groupes communautaires, dans le but de démystifier

le processus d'enquête sur les plaintes; et intensifier les efforts de recrutement pour veiller à ce que l'OSSNR continue de se doter d'un effectif d'élite aux compétences et aux expériences variées.

- Afin de favoriser la transparence, l'OSSNR a également l'intention de caviarder et de publier de façon proactive nos rapports futurs à mesure qu'ils sont approuvés au cours de l'année, plutôt que d'attendre la publication de notre rapport annuel pour divulguer nos constatations et nos recommandations. L'organisation collabore avec les ministères et les organismes pour veiller à ce que cette nouvelle approche soit aussi rapide et efficace que possible, qu'elle protège les renseignements essentiels en matière de sécurité nationale et de renseignement, et donne au public le plus d'information possible sur les résultats des examens de l'OSSNR.

Introduction



L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR)⁷ a débuté ses opérations le 12 juillet 2019 dans le cadre de la transformation du cadre de responsabilisation en matière de sécurité nationale du Canada. Par conséquent, ce premier rapport annuel ne couvre qu'une période de six mois, de juillet à la fin de l'année civile 2019⁸. Au cours de cette période et jusqu'en 2020, l'OSSNR a déployé beaucoup d'efforts pour assurer une transition réussie du Comité de surveillance des activités de renseignement de sécurité (CSARS)⁹ à une organisation plus vaste ayant un mandat beaucoup plus important.

- 
- A vertical photograph on the left side of the page shows a person wearing a white lab coat. Their hands are visible, and they appear to be working at a desk. A calculator is partially visible in the lower left corner of the image. The lighting is warm and focused on the person's hands.
2. Étant donné que le site Web de l'OSSNR fournit des renseignements détaillés sur son mandat, les types d'examens entrepris, le processus et le cycle de vie d'un examen et le processus d'enquête sur les plaintes, le présent rapport ne traite pas de ces sujets.
 3. Il met plutôt l'accent sur le travail initial de l'OSSNR en ce qui concerne ses examens, ses enquêtes sur les plaintes, ainsi que ses efforts d'engagement du public et de transparence. L'accent mis sur l'analyse des récentes constatations et tendances dans l'examen s'appuie sur des examens du CSARS et du Bureau du commissaire du Centre de la sécurité des télécommunications¹⁰ qui n'ont pas encore été publiés et qui remontent à 2018 et 2019, respectivement, ainsi que sur les examens de l'OSSNR effectués au cours des premiers mois de fonctionnement. Des résumés de ces rapports individuels sont disponibles aux annexes A et B.
 4. La partie 1 décrit nos valeurs organisationnelles et l'approche adoptée par l'OSSNR pour mettre en place une nouvelle institution.
 5. La partie 2 fournit une analyse détaillée des thèmes sur lesquels portent bon nombre de ces examens, en établissant des liens et en mettant en place une plateforme pour les futurs travaux.
 6. La partie 3 traite de nos enquêtes sur les plaintes et aborde brièvement des thèmes de 2019 et des priorités pour l'année à venir, en mettant l'accent sur la modernisation du processus d'enquête sur les plaintes afin de le rendre plus rapide et accessible. Des résumés et des statistiques relatifs aux enquêtes sur les plaintes sont disponibles aux annexes C et D.
 7. La partie 4 décrit les efforts de l'OSSNR et sa vision en matière d'engagement et de transparence, qui sont des priorités clés pour l'organisation.
 8. Les principales réalisations et les priorités continues en ce qui concerne les services ministériels de l'OSSNR, y compris les mesures prises pour s'adapter à un mandat élargi, sont décrites en détail à l'annexe E.¹¹
 9. Il s'agit du premier rapport annuel de l'OSSNR, et il est structuré de façon à ce qu'il soit utile et intéressant pour le lecteur, tout en servant sa fonction première, à savoir apporter une contribution importante au dialogue des Canadiens sur les questions de sécurité nationale et de renseignement. Les commentaires sur la façon de le rendre aussi utile et accessible que possible pour atteindre cet objectif sont les bienvenus.

Création d'une institution

10. La création de l'OSSNR, à la suite de la proclamation de la *Loi de 2017 sur la sécurité nationale*, a représenté une étape importante dans le développement de la responsabilisation en matière de sécurité nationale et de renseignement au Canada. Au cours des deux dernières décennies, les opérations de sécurité nationale et de renseignement sont devenues de plus en plus interreliées au sein du gouvernement du Canada. Cela a fait en sorte qu'un certain nombre de ministères et d'organismes qui ne faisaient pas traditionnellement partie de l'appareil de la sécurité et du renseignement jouent maintenant des rôles clés dans ce domaine. Toutefois, les pouvoirs des organismes d'examen n'ont pas évolué au même rythme que le paysage de la sécurité nationale et du renseignement, et leur capacité d'examiner les organismes et d'apporter des contributions est demeurée compartimentée.
11. La création de l'OSSNR comble une lacune de longue date dans l'architecture de sécurité nationale du Canada et renforce considérablement le cadre de responsabilisation en matière de sécurité nationale. L'OSSNR a pris en charge les mandats de ses prédécesseurs pour examiner les opérations du Service canadien du renseignement de sécurité (SCRS) et du Centre de la sécurité des télécommunications (CST), respectivement, mais nous avons aussi un mandat supplémentaire et nouveau, soit celui d'examiner toute activité du gouvernement fédéral liée à la sécurité nationale ou au renseignement. En plus de ce mandat élargi, l'OSSNR a un accès sans entrave aux renseignements classifiés en la possession ou sous le contrôle de tout ministère ou organisme (à l'exception des documents confidentiels du Cabinet). Cela permet à l'OSSNR de délaisser l'approche compartimentée précédente de l'examen et de la responsabilisation et de la remplacer par un examen interorganismes horizontal et approfondi. Ainsi, le Canada dispose maintenant de l'un des systèmes d'examen indépendant de la sécurité nationale les plus complets au monde.
12. Depuis juillet 2019, le Secrétariat de l'OSSNR s'est efforcé d'assurer une transition réussie et efficace vers une organisation beaucoup plus grande ayant un mandat beaucoup plus vaste. Il a notamment mis l'accent sur les éléments suivants : l'obtention de nouveaux locaux; la dotation efficace et le perfectionnement des connaissances; l'établissement de relations de travail solides avec les ministères et les organismes, ainsi qu'avec d'autres organismes d'examen canadiens; et le respect de nos exigences en matière de rapports obligatoires. L'OSSNR a absorbé des effectifs du Comité de surveillance des activités de renseignement de sécurité (CSARS), qui avaient une expertise en matière d'examen et d'enquête sur les plaintes liées au SCRS. Des efforts soutenus visant à recruter du personnel et à accroître les connaissances de l'appareil élargi de la sécurité et du renseignement se poursuivront au cours de l'année à venir.

Examen

13. Au cours des premiers mois de notre mandat, l'OSSNR a élaboré un plan d'examen triennal. Ce plan aidera à élaborer une approche systématique pour décider ce qu'il faut examiner et comment établir les priorités. En plus d'aider à orienter les décisions

relatives à l'affectation des ressources et à la dotation à moyen terme, le plan d'examen fournit des précisions aux ministères et organismes visés et prévient le chevauchement avec d'autres organismes d'examen.

14. Une partie du défi inhérent au mandat de l'OSSNR consiste à percevoir différemment la façon d'organiser et de mener des examens. Le mandat interorganismes permet de planifier et d'entreprendre des examens horizontaux auxquels participent plusieurs ministères et organismes dès le départ. De même, l'OSSNR travaille également de façon horizontale à l'interne, pour inclure plus systématiquement des experts juridiques et techniques dans les examens, afin que les considérations dans ces domaines soient intégrées aux examens dès le départ.
15. Dans le cadre de ce plan, l'examen approfondi du SCRS et du CST demeure une priorité organisationnelle. L'OSSNR acquiert également des connaissances de base sur les activités de sécurité nationale et de renseignement menées dans les institutions du gouvernement fédéral qui n'ont traditionnellement pas fait l'objet d'un examen. Par une série d'examens de plus en plus complexes et approfondis qu'il mènera au cours des prochaines années, l'OSSNR cherchera à broser un tableau complet et détaillé des activités, des programmes ou des principaux thèmes de l'appareil de la sécurité nationale et du renseignement.
16. Quand il procède à des examens, qu'il s'agisse d'exercices simples d'établissement de la portée ou de projets plus complexes, l'OSSNR tient compte d'un certain nombre d'éléments pour formuler des conclusions, des constatations et des recommandations. Il s'agit notamment de la légalité, du respect des directives et des politiques, du caractère raisonnable, de la nécessité et du caractère proportionnel des activités de sécurité et de renseignement. Ces considérations permettent à l'OSSNR de s'assurer que les Canadiens sont confiants que les activités de sécurité nationale et de renseignement entreprises par le gouvernement du Canada font l'objet d'un examen et d'une évaluation approfondis.

Enquêtes sur les plaintes

17. En plus de son mandat d'examen, l'OSSNR a la responsabilité d'enquêter sur les plaintes liées à la sécurité nationale. Cela comprend les plaintes du public concernant les mesures prises par le SCRS et le CST, les plaintes liées à la sécurité nationale concernant la Gendarmerie royale du Canada (GRC)¹² et les plaintes liées aux habilitations de sécurité révoquées ou refusées.
18. L'OSSNR reconnaît que le cadre d'enquête sur les plaintes hérité du CSARS était beaucoup trop lent et trop complexe. Une analyse du nombre de plaintes déposées chaque année et du nombre de plaintes qui ne correspondent pas au mandat d'enquête de l'OSSNR révèle également un manque évident de connaissances concernant le rôle de l'OSSNR à cet égard. Pour ces raisons, l'OSSNR a entrepris de réformer le processus de traitement des plaintes, notamment en augmentant l'accès, la rapidité et la responsabilisation.

Valeurs de l'OSSNR

- 19.** L'OSSNR a hérité d'un certain nombre de valeurs, de pratiques et d'une expertise des organismes d'examen qui l'ont précédé. Néanmoins, l'OSSNR est déterminé à entreprendre ses travaux d'une nouvelle façon, qui met l'accent sur la sensibilisation, la mobilisation et la transparence. À ce titre, l'OSSNR a entrepris un vaste programme de mobilisation de la société civile, des groupes communautaires, des universitaires et d'autres intervenants, fondé sur un certain nombre d'objectifs, notamment :
- éclairer le plan d'examen de l'OSSNR;
 - mieux faire connaître le processus d'enquête sur les plaintes et le démystifier;
 - mettre à profit et créer des communautés d'intérêts sur des questions clés (par exemple, sur l'intelligence artificielle);
 - recruter des Canadiens talentueux.
- 20.** La nouvelle organisation veut rompre avec les pratiques antérieures qui prévoyaient la publication des constatations et des recommandations qu'une fois par année. Pour accroître la transparence, l'OSSNR s'engage à diffuser les versions non classifiées des examens, caviardées et traduites, à mesure qu'elles sont disponibles. En mettant ses examens à la disposition du public, l'OSSNR espère accroître la transparence et la responsabilisation, et ouvrir la porte à des discussions et à des débats approfondis dans la sphère publique. Par conséquent, une priorité est de rédiger des rapports qui évitent les renseignements classifiés parce que l'intention est de les publier; cette approche de « communication écrite » facilitera le processus de caviardage, au besoin, et assurera une diffusion plus rapide et efficace de l'information.¹³
- 21.** L'OSSNR s'engage à :
- Faire preuve d'ouverture et de transparence, afin de mieux communiquer avec les Canadiens;
 - Viser l'excellence des méthodes pour assurer la qualité de notre travail;
 - Procéder à une réflexion prospective et à faire preuve d'innovation, y compris la façon dont nous tenons compte des répercussions des nouvelles technologies et d'un environnement de sécurité nationale en constante évolution.
- 22.** Pour atteindre nos nombreux objectifs complexes, l'OSSNR compte sur un effectif qualifié et expérimenté. Au fur et à mesure que l'organisation prendra de l'expansion, l'OSSNR continuera de recruter des candidats talentueux qui reflètent la nature diversifiée et inclusive du Canada.
- 23.** L'OSSNR comprend que la santé et le bien-être de l'organisation sont essentiels à la réussite. L'organisation souhaite être un employeur de choix qui favorise et offre un milieu de travail sain. Bien que la pandémie de la COVID-19 ait soulevé des défis sans précédent, l'OSSNR continue de se concentrer sur l'adaptation aux changements radicaux causés par la pandémie. Veiller à la santé physique et mentale et au bien-être de notre personnel demeure une pierre angulaire de la stratégie de l'organisation tandis que nous élaborons des façons créatives de maintenir l'efficacité et l'efficience tout en travaillant de façon non centralisée.

-
- 24.** En plus de maintenir une expertise variée au sein de l'organisation, l'OSSNR a mis l'accent sur l'établissement d'un réseau de partenariat solide pour aider à définir nos priorités de recherche et à réaliser notre mandat. L'OSSNR a travaillé avec d'autres organisations au sein du système canadien d'examen et de responsabilisation dans son ensemble, comme le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)¹⁴ et le Commissariat à la protection de la vie privée du Canada (CPVP)¹⁵, sur des questions d'intérêt commun afin de maximiser l'efficacité et l'efficience des organismes d'examen en matière de sécurité nationale, tout en limitant le dédoublement des efforts.
- 25.** L'OSSNR a fait beaucoup de progrès dans tous les aspects de notre mandat au cours des premiers mois de fonctionnement en 2019. De nombreux projets ambitieux sont en cours pour l'année à venir, et s'inscrivent dans la mise en place d'une institution apte à assumer un rôle important et constructif dans le système canadien de responsabilisation en matière de sécurité nationale.

Examen

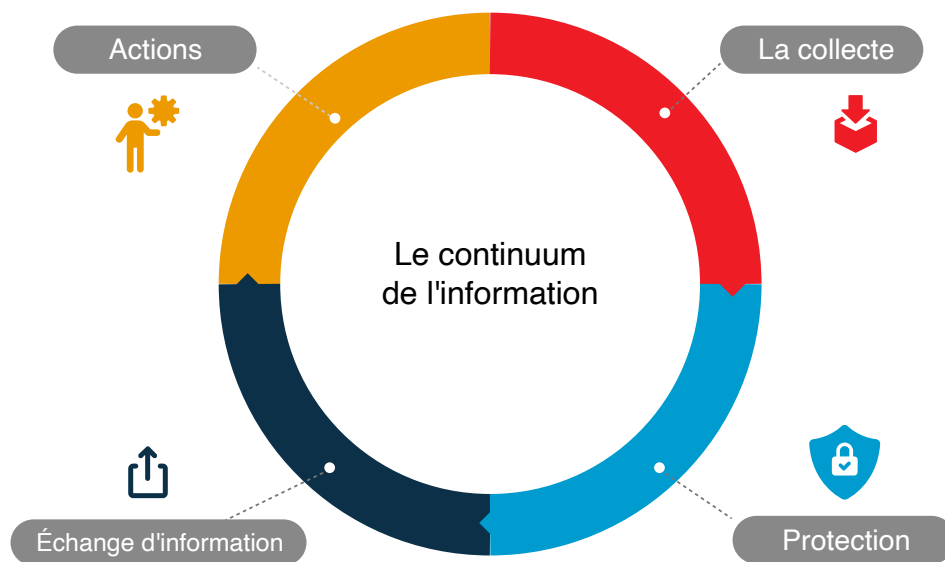
Section I

— Le continuum de l'information

02

Cette partie décrit le cadre adopté par l'OSSNR pour discuter des constatations et des tendances en cours d'examen et fournit une analyse détaillée en fonction des quatre catégories de ce cadre. Cette partie ne traite pas en détail de la méthodologie d'examen et de l'établissement des priorités. En bref, à mesure que nous aurons une meilleure connaissance des activités liées à la sécurité nationale et au renseignement dans tout le gouvernement du Canada, l'OSSNR entend entreprendre des examens de plus en plus complexes au cours des trois prochaines années.

- 27.** Les membres de l'OSSNR prévoient caviarder et publier de façon proactive les examens complets, ainsi que les résumés non classifiés, au fur et à mesure qu'ils sont approuvés et traduits, plutôt que d'avoir à attendre le rapport annuel pour présenter les examens réalisés par l'organisation. Grâce à cette nouvelle pratique, le rapport annuel peut traiter des leçons apprises tout au long de l'année et les analyser de façons novatrices et intéressantes. Plutôt que de discuter des constatations et des recommandations de chaque examen individuellement (ou verticalement), comme cela a été fait dans les rapports annuels du Comité de surveillance des activités de renseignement de sécurité (CSARS) et du Bureau du commissaire du Centre de la sécurité des télécommunications (BCSEC), l'OSSNR se concentrera sur l'ensemble du travail horizontalement et déterminera quelles leçons, quelles tendances ou quels thèmes généraux en ressortent. L'OSSNR croit que cela permettra une analyse plus complète des constatations et aidera à procéder à une planification plus complète et interconnectée des examens.
- 28.** La discussion qui suit est organisée selon ce que l'OSSNR appelle le « continuum de l'information ». Ce continuum vise à refléter le cycle de vie de l'information, de la façon dont elle est recueillie et protégée, à la façon dont elle est utilisée pour éclairer les mesures concrètes prises à des fins de sécurité nationale ou de renseignement, en passant par la façon dont elle est partagée.



- 29.** L'OSSNR reconnaît que le continuum de l'information diffère du cycle d'information de la sécurité nationale et du renseignement. Par exemple, le continuum n'est pas un processus unidirectionnel, et tous les concepts qui y sont mentionnés sont interreliés. Toutefois, nous souhaitons que la présentation de nos constatations dans ce cadre aide les lecteurs à comprendre les principaux thèmes et priorités dans le contexte de la sécurité nationale et du renseignement. Une structure différente pourrait être adoptée pour les futurs rapports annuels en fonction des recommandations que l'OSSNR reçoit et de l'information que nous souhaitons communiquer.

Section II

— Collecte

- 30.** La collecte constitue la première étape du cycle du continuum de l'information décrit dans le présent rapport. Par collecte, on entend toutes les formes de récupération d'information ayant trait à la sécurité nationale ou au renseignement par les ministères et organismes du gouvernement du Canada. Cela comprend toute l'information recueillie directement par ces ministères et organismes au Canada et à l'étranger, ainsi que celle reçue d'autres entités fédérales ou d'autres ordres de gouvernement (p. ex. services d'application de la loi provinciaux ou municipaux). La réception d'information de la part d'entités étrangères correspond aussi à une forme de collecte, mais, compte tenu des considérations particulières relatives aux droits de la personne qui régissent cette activité, le présent rapport traite de ce sujet dans la section sur l'échange d'information.
- 31.** Les ministères et organismes collectent de l'information au moyen de diverses techniques. Certains recrutent des sources humaines pour qu'elles recueillent de l'information pour eux, et d'autres interceptent des télécommunications par différents moyens techniques, comme l'écoute électronique. Les télécommunications, dans ce contexte, désignent à la fois la collecte du contenu de communications (p. ex. l'interception d'une conversation vocale ou d'un courriel) et celle de métadonnées (p. ex. données d'abonné à un moyen de télécommunication ou liées à des connexions Internet). Dans le cas présent, il importe de souligner que la collecte désigne l'information recueillie par les institutions du gouvernement du Canada secrètement ou ouvertement, ce qui comprend l'information accessible au public. La distinction entre l'information accessible au public et celle qui ne l'est pas fait l'objet d'une controverse. L'OSSNR se penchera sur la question ultérieurement. Souvent, l'information recueillie ne porte que sur une personne ou quelques personnes. D'autres fois, les ministères et organismes recueillent des données en masse.¹⁶
- 32.** De toute évidence, la collecte de certaines informations par les ministères et organismes peut constituer une intrusion dans les affaires privées de Canadiens. En effet, des nombreuses activités liées à la sécurité nationale et au renseignement que l'OSSNR a le mandat d'examiner, la collecte est celle qui est la plus susceptible d'empiéter sur le droit à la vie privée des Canadiens. Néanmoins, les Canadiens s'attendent à ce que leur vie privée, leurs communications et leurs activités en ligne ne soient pas surveillées par l'État, à moins que l'intrusion soit conforme à la loi (et, au besoin, qu'elle soit préautorisée par un officier de justice indépendant), et que la collecte soit raisonnable et n'excède pas la limite nécessaire pour atteindre un objectif légitime, comme une enquête sur une infraction criminelle ou sur une menace pour la sécurité du Canada. Pour ces raisons, l'OSSNR fait de la collecte d'information par le gouvernement un de ses points permanents d'examen.

Cadres juridiques

- 33.** Les cadres juridiques qui régissent la collecte d'information par les ministères et organismes sont complexes et diffèrent d'un ministère et d'un organisme à l'autre. Il y a toutefois quelques principes généraux. En termes simples, tous les ministères et organismes sont assujettis à la *Charte canadienne des droits et libertés* (la Charte) et doivent s'assurer que leur collecte d'information est « raisonnable », conformément à l'article 8 de la Charte, qui indique que « chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives » à l'endroit de leur personne, de leur propriété ou de leur information. Cette disposition signifie que lorsque les actes de l'État s'immiscent dans la vie privée qu'une personne s'attend raisonnablement à avoir, la fouille doit généralement être préautorisée par un officier de justice indépendant (habituellement un juge qui accorde un mandat). Toutefois, dans de rares circonstances, il est permis de recueillir de l'information sans mandat sur une personne ayant une attente raisonnable en matière de respect de la vie privée, pour autant que la collecte soit autorisée par une loi considérée comme raisonnable dans l'établissement d'un juste équilibre entre le droit à la vie privée et l'intérêt de l'État, et que la fouille soit effectuée de manière raisonnable.
- 34.** Au Canada, les policiers et autres agents de la paix doivent demander différentes autorisations pour procéder à des fouilles, des perquisitions ou des saisies intrusives qui impliquent l'attente raisonnable d'une personne en matière de respect de la vie privée. Ces autorisations d'« accès légal » comprennent les mandats de perquisition, les ordonnances de communication pour obtenir des documents ou des dossiers, et les mandats autorisant l'interception de communications privées. Le Service canadien du renseignement de sécurité (SCRS)¹⁷ peut obtenir des mandats de la Cour fédérale l'autorisant à intercepter toute communication ou à obtenir toute information, tout dossier, tout document ou tout objet.¹⁸ Les démarches à suivre pour obtenir ces autorisations varient selon la loi qui régit l'organisme qui fait la demande et selon le caractère intrusif de la fouille ou perquisition. Le Centre de la sécurité des télécommunications (CST),¹⁹ pour sa part, recueille de l'information à l'extérieur du Canada conformément à ses divers mandats liés au renseignement étranger et à la cybersécurité. Lorsqu'il est possible que ces activités de collecte contreviennent à une loi du Parlement ou compromettent l'attente raisonnable en matière de respect de la vie privée d'un Canadien ou d'une personne se trouvant au Canada, le CST doit obtenir des autorisations du ministre de la Défense nationale.²⁰ Avant d'entrer en vigueur, les autorisations du ministre obtenues par le CST dans le cadre de son mandat relatif au renseignement étranger et de son mandat relatif à la cybersécurité et à l'assurance de l'information doivent être approuvées par le commissaire au renseignement, qui est un juge à la retraite.²¹
- 35.** Peu importe la nature délicate de l'information recueillie, les ministères et organismes doivent avoir l'autorisation légale de recueillir cette information. Ils se voient conférer cette autorisation légale par leur loi habilitante (p. ex. la Loi sur le SCRS pour le SCRS; la Loi sur le CST pour le CST), et par les pouvoirs de la common law, surtout dans le cas de la GRC.

36. Ces lois établissent également des limites importantes, souvent en énonçant l'information que les ministères ont le droit de recueillir, le moment où ils peuvent le faire et dans quelle mesure. Par exemple, le CST n'a pas le droit de viser des Canadiens ou des personnes se trouvant au Canada lors de sa collecte d'information, mais il n'est pas toujours possible de savoir à l'avance quelles informations sont liées à des Canadiens et lesquelles ne le sont pas. Par conséquent, il peut arriver que le CST recueille accidentellement (c'est-à-dire en ne cherchant pas expressément à collecter) de l'information liée à des Canadiens ou à des personnes se trouvant au Canada. Le CST doit traiter cette information conformément à la Loi sur le CST et aux autorisations qu'il a reçues du ministre de la Défense nationale.²²

Instructions ministérielles et politiques

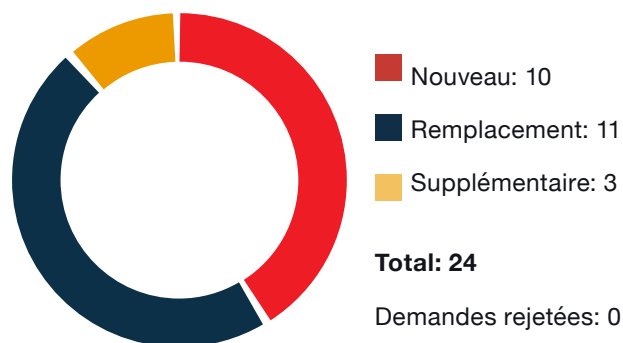
37. La collecte d'information par le gouvernement du Canada est orientée non seulement par les lois, mais aussi par diverses instructions ministérielles et politiques internes. Les instructions ministérielles sont un guide officiel envoyé par un ministre à un ministère ou à un organisme ²³. Ces instructions ne constituent pas un texte réglementaire, mais elles ont un plus grand statut juridique que de simples politiques ministérielles internes et servent souvent à énoncer les attentes d'un ministre quant au fonctionnement d'un ministère et à la façon dont ses pouvoirs juridiques devraient être interprétés. Ces instructions sont utilisées, par exemple, pour mettre en œuvre les priorités du gouvernement du Canada en matière de renseignement, qui sont approuvées périodiquement par le Cabinet. Les priorités en matière de renseignement établissent les secteurs d'activité sur lesquels le gouvernement du Canada a déterminé qu'il avait le plus besoin d'information. Les ministres demandent alors aux ministères d'affecter des ressources à la collecte d'information en conséquence, mais celles-ci doivent toujours respecter les limites de leurs mandats légaux de collecte. Lorsque l'OSSNR réalise un examen sur une activité de collecte liée à la sécurité nationale ou au renseignement, nous n'examinons pas seulement la conformité aux lois, mais aussi le respect des instructions ministérielles et des politiques internes.

La collecte de 2019 en chiffres

Mandats de collecte du SCRC

1 avril 2018 - 31 décembre 2018

1 janvier 2019 - 31 décembre 2019



Cibles du SCRS

1 avril 2018 - 31 décembre 2018: 430

1 janvier 2019 - 31 décembre 2019: 467

Ensembles de données du SCRS en 2019

Nombre d'ensembles de données canadiens conservés par le SCRS après une autorisation de la Cour:	0
Nombre de demande d'autorisation par le SCRS à la Cour pour la rétention d'un ensemble de données canadien:	0
Nombre d'ensembles de données étrangers conservés par le SCRS après une autorisation du ministre et du commissaire au renseignement:	0
Nombre de demande d'autorisation par le SCRS au commissaire au renseignement pour la rétention d'un ensemble de données étranger:	0

Autorisations ministérielles du CST en 2019

Autorisation ministérielles octroyées en vertu des articles suivant de la Loi sur le CST:

paragraphe	26(1),	renseignement étranger:	x
paragraphe	27(1),	cybersécurité - fédérale:	x
paragraphe	27(2),	cybersécurité - non fédéral:	x
paragraphe	29(1),	cyberopérations défensives:	x
paragraphe	30(1),	cyberopérations actives:	x

Le CST a confirmé qu'en 2019, des autorisations ministérielles ont été signées sous chaque paragraphe répertoriée dans ce tableau. Cependant, le CST est d'avis que la publication de ces chiffres serait préjudiciable à la sécurité nationale. L'OSSNR est désaccord avec cette perspective. En date du 20 novembre 2020, ce problème n'a pas pu être résolu. L'OSSNR continuera à travailler avec le CST en vue de trouver un compromis.

Défis liés à la collecte

Technologie et protection des renseignements personnels

- 38.** Les criminels et les personnes qui représentent une menace envers la sécurité nationale cherchent constamment à adopter les plus récentes technologies pour protéger leurs activités de sorte qu'elles ne puissent pas être vues. Ces mesures font pression sur les organismes d'enquête, au Canada et à l'étranger, qui doivent maintenir leur capacité de recueillir de l'information utilisable. Par conséquent, les organismes de sécurité nationale et de renseignement du Canada doivent rapidement adopter les nouvelles technologies pour déjouer ou devancer les capacités de leurs sujets d'enquête.
- 39.** Malheureusement, bon nombre de nouvelles technologies peuvent être utilisées de façons qui minent la protection des renseignements personnels. L'essor d'Internet et des communications mobiles fait en sorte que les personnes génèrent maintenant une quantité beaucoup plus grande d'information et de métadonnées les concernant qu'auparavant. Parallèlement, ceux qui recueillent du renseignement perdent progressivement l'accès direct aux communications privées en raison de l'omniprésence des fonctions de cryptage avancées. Ceci explique en partie l'intérêt grandissant qui s'est fait sentir à l'échelle mondiale envers la collecte en masse d'information et de métadonnées au cours des dernières décennies. Ce contenu brut est ensuite trié et analysé afin de mieux le comprendre et d'en faire ressortir des tendances. Par exemple, l'utilisation de téléphones intelligents laisse des traces numériques qui, surtout lorsqu'elles sont réunies ou identifiées ultérieurement, peuvent révéler des contacts, des habitudes en matière de déplacements et d'autres détails personnels. L'une des principales différences entre la collecte en masse et les techniques plus classiques, comme l'écoute électronique, est que la majorité de l'information recueillie porte sur des citoyens ordinaires qui ne font pas l'objet de l'enquête. Ces techniques présentent un risque réel quant à la protection des renseignements personnels.²⁴
- 40.** Un défi de taille pour les ministères et organismes canadiens consiste à veiller à ce que leur utilisation des nouvelles technologies respecte les lois en matière de protection des renseignements personnels ainsi que les droits garantis par la Charte. De manière générale, pour ce faire, les ministères et organismes doivent obtenir des conseils auprès du ministère de la Justice concernant les paramètres légaux qui gouvernent l'utilisation de la technologie, puis doivent mettre en place un cadre stratégique solide et obtenir les autorisations requises avant de commencer à utiliser une nouvelle technologie. Souvent, les choses se déroulent exactement ainsi, mais l'OSSNR est également au courant de situations où la technologie a été utilisée d'une manière qui dépassait les autorisations légales. Ces situations sont décrites ci-dessous. Certains exemples sont tirés des examens de l'OSSNR réalisés jusqu'à présent, alors que d'autres sont tirés d'examens sur le SCRS réalisés par le CSARS.

41. À quelques reprises au cours des dernières années, le SCRS s'est servi de nouvelles techniques de collecte sans d'abord avoir entièrement compris et évalué leurs implications d'ordre juridique et stratégique. Dans ces cas, les travaux de nature juridique et stratégique n'ont pas été à la hauteur du besoin opérationnel de maintenir et d'améliorer les capacités en matière de collecte. Ces activités ont mis à risque – et même parfois compromis – le caractère licite de l'activité de collecte ainsi que la protection des renseignements personnels des Canadiens. Le premier exemple est tiré d'un examen de l'OSSNR :
- a. **Géolocalisation:** L'un des premiers examens de l'OSSNR portait sur l'utilisation par le SCRS de données de géolocalisation accessibles au public. L'examen a soulevé des questions pressantes à propos de l'utilisation de données accessibles au public, mais qui peuvent quand même porter atteinte à l'attente raisonnable d'une personne en matière de protection des renseignements personnels. L'OSSNR a conclu que l'utilisation par le SCRS de ces données sans mandat risquait de contrevenir à l'article 8 de la Charte, qui protège contre les fouilles, les perquisitions et les saisies abusives. L'examen de l'OSSNR portait sur le processus de décision ayant mené le SCRS à utiliser ces données sans mandat, et a permis de constater que le SCRS n'avait pas de politique ni de procédure en place pour veiller à ce que le SCRS demande un avis juridique avant d'utiliser les données afin d'éviter d'en faire une utilisation illicite. Le 16 mars 2020, nous avons présenté un rapport en vertu de l'article 35 de la Loi sur l'OSSNR ²⁵ au ministre de la Sécurité publique et de la Protection civile décrivant la possible activité illicite. Selon l'article 35, l'OSSNR doit présenter un rapport au ministre compétent sur toute activité liée à la sécurité nationale ou au renseignement qui, à son avis, pourrait ne pas être conforme à la loi. Le ministre doit ensuite remettre le rapport au procureur général du Canada.
42. D'autres exemples datent d'avant la création de l'OSSNR et ont fait l'objet d'examens par d'anciens organismes d'examen, soit le CSARS et le BCCST :
- a. **Utilisation de métadonnées par le SCRS:** Dans un examen du CSARS datant de 2014 ²⁶ on a évalué si la collecte, l'utilisation et la conservation par le SCRS de métadonnées visées par un mandat de la Cour fédérale ont été effectuées de façon licite et appropriée. À l'époque, toutes les communications et métadonnées recueillies accessoirement en vertu d'un mandat du SCRS (c.-à-d. qui n'étaient pas liées aux personnes visées par le mandat) devaient être détruites, sauf dans certains cas, par exemple s'il y avait des motifs raisonnables de croire que l'information « pourrait faire avancer » une enquête relative à une menace envers la sécurité du Canada. Le SCRS a conclu que les termes « pourrait faire avancer » établissaient un critère peu élevé, et a conservé et utilisé des métadonnées en conséquence, malgré le fait que les données avaient été recueillies accessoirement. Rien n'a indiqué au CSARS que le SCRS avait informé la Cour fédérale de la nature et de la portée de ses activités. Le CSARS a donc recommandé que le SCRS informe la Cour fédérale de l'étendue de la conservation et de l'utilisation des métadonnées recueillies en vertu d'un mandat. Alertée par la recommandation du CSARS, la Cour a conclu en octobre 2016 que le SCRS ne pouvait pas conserver l'information à moins qu'elle soit liée à une menace envers la sécurité du Canada, étant donné que

le mandat du SCRS énoncé à l'article 12 de sa loi habilitante précise que le SCRS peut recueillir de l'information et du renseignement seulement « dans la mesure strictement nécessaire ». La Cour a conclu que le pouvoir du SCRS de conserver de l'information était établi d'après cette limite. Par conséquent, la Cour a estimé que le SCRS avait outrepassé son pouvoir légal en conservant la plupart des métadonnées recueillies en vertu d'un mandat. La Cour a également conclu que le SCRS a failli à son obligation de franchise envers la Cour. Comme il est mentionné ci-dessous, la question de la conservation d'ensembles de données électroniques est davantage pleinement régie par la Loi sur le SCRS, depuis que des modifications y ont été apportées lors de l'entrée en vigueur de la *Loi de 2017 sur la sécurité nationale*.

- b. Utilisation de métadonnées par le CST :** Les avancées technologiques sont à l'origine de grandes quantités d'information dans le domaine numérique. Les organismes ont souvent recours à l'automatisation pour appliquer efficacement des mesures de protection des renseignements personnels à de grandes quantités d'information. En 2013, le CST a informé son ancien organisme d'examen, le BCCST, que certaines métadonnées contenant de l'information sur l'identité de Canadiens n'avaient pas été correctement supprimées par le logiciel²⁷. Cet échec du logiciel a fait en sorte que les alliés du Canada du Groupe des cinq ont reçu des données que, selon les lois canadiennes, le CST n'est pas autorisé à communiquer. Le CST a mis en suspens la communication de certains types de métadonnées le temps d'élaborer une solution à ce problème. Même s'il s'agit du seul incident où le BCCST a jugé que le CST n'a pas été conforme à la loi, des situations similaires se sont produites à l'occasion, notamment lorsque le CST a présenté un rapport incomplet au sujet de communications privées. Le BCCST a conclu que cet incident pouvait être attribuable à l'erreur humaine et à l'erreur système. Bon nombre des observations présentées par le BCCST portaient sur l'interaction entre des éléments humains et techniques participant à la collecte et aux activités subséquentes d'établissement de rapport.
- c. Ensembles de données:** En 2016, le CSARS a examiné l'utilisation d'ensembles de données par le SCRS²⁸. Ces ensembles de données n'ont pas été recueillis en vertu d'un mandat. L'examen visait à déterminer si la collecte de tels ensembles de données satisfaisait au critère prévu à l'article 12 de la Loi sur le SCRS, selon lequel le SCRS peut recueillir de l'information seulement « dans la mesure strictement nécessaire ». La plupart des ensembles de données n'étaient pas directement liés à des menaces envers la sécurité nationale. Le CSARS a conclu qu'il n'existait aucun cadre de gouvernance complet orientant les activités de collecte, de conservation et d'utilisation d'ensembles de données en masse. En outre, il n'existait aucune exigence d'évaluer les ensembles de données afin de s'assurer qu'ils satisfaisaient l'exigence de la collecte « dans la mesure strictement nécessaire » en vue de conseiller le gouvernement du Canada à l'égard de menaces présumées. Ces incidents ont poussé le SCRS à revoir les fondements juridiques de ses activités de collecte d'ensembles de données. Des modifications à la Loi sur le SCRS apportées par la *Loi de 2017 sur la sécurité nationale* ont depuis accordé au SCRS le pouvoir explicite de recueillir, de conserver et d'utiliser des ensembles de données contenant des renseignements personnels qui n'ont pas de lien direct et immédiat avec une menace envers la sécurité du Canada. Comme

indiqué dans le certificat remis par le CSARS, en attendant l'entrée en vigueur de la *Loi de 2017 sur la sécurité nationale*, le SCRS a poursuivi les activités de son programme d'ensembles de données malgré les risques juridiques cernés.

- 43.** Ces exemples démontrent en quoi le fait d'adopter de nouvelles technologies de collecte constitue également un défi pour les organismes d'examen, qui doivent posséder l'expertise technique nécessaire pour s'assurer de pleinement comprendre les implications liées aux technologies déployées. Cet aspect revêt une importance particulière étant donné que l'utilisation de nombreuses nouvelles technologies est un secret étroitement gardé, et donc protégé de l'examen du public. Par conséquent, il incombe en grande partie aux organismes d'examen et de surveillance d'examiner l'utilisation de ces technologies. La façon dont l'OSSNR prévoit aborder cette question est présentée à la section sur les priorités à venir.

Franchise

- 44.** Le SCRS a eu de la difficulté à éliminer une culture du secret institutionnelle ayant contribué à des omissions de communiquer entièrement certaines activités et informations à la Cour fédérale, au ministre de la Sécurité publique et de la Protection civile, ainsi qu'aux organismes d'examen. Un manque de franchise peut s'avérer particulièrement problématique quand il est associé à l'utilisation de nouvelles technologies. La différence entre une collecte légale et illégale repose souvent sur des détails très précis concernant l'information que la technologie permettra au SCRS de recueillir. L'un des principaux éléments dont il faut tenir compte est le fait de savoir si l'information révélera des détails personnels concernant le mode de vie et les choix particuliers d'une personne. L'étendue de l'information recueillie et d'autres détails concernant son utilisation peuvent également avoir une incidence sur le niveau d'intrusion d'une technologie. Il est donc essentiel que les organismes de surveillance et d'examen soient pleinement informés des activités ministérielles pour exécuter leur mandat. Plus l'examen de l'utilisation d'une nouvelle technologie est approfondi, plus une évaluation rigoureuse de ses implications est faite.
- 45.** Au cours des dernières années, la Cour fédérale a conclu à trois reprises ²⁹ au non-respect du SCRS de son obligation de franchise envers la Cour dans le cadre de demandes de mandat. Dans deux des trois cas, le SCRS a omis certaines informations concernant l'utilisation de la technologie pour recueillir de l'information. Les omissions ont compromis la capacité de la Cour d'exercer adéquatement sa fonction de contrôle judiciaire. En effet, il convient de noter que la Cour n'est pas tenue d'approuver les demandes de mandat du SCRS, même si le SCRC satisfait les exigences législatives de base. La Cour doit également être convaincue que les pouvoirs conférés par le mandat sont raisonnables en tenant compte de l'ensemble des circonstances, et doit donc recevoir toute l'information nécessaire pour effectuer cette évaluation clé. La Cour peut également imposer des conditions qu'elle croit être dans l'intérêt du public sur les mandats du SCRS; elle doit donc être en mesure de reconnaître les implications des nouvelles technologies en matière de protection des renseignements personnels.

46. Le ministre de la Sécurité publique et de la Protection civile joue également un rôle important dans la surveillance des activités du SCRS en raison de ses responsabilités prévues par la loi dans le cadre du processus relatif aux mandats du SCRS. Avant que le SCRS puisse présenter une demande de mandat à la Cour fédérale, il doit d'abord la faire approuver par le ministre. Il doit donc fournir toute l'information pertinente au ministre et aux fonctionnaires qui le conseillent. Il convient de noter que le ministre a ressenti le besoin de fournir des directives encore plus précises et détaillées au SCRS, indiquant que l'organisation doit tenir le ministre au courant de ses activités. L'exemple le plus récent concerne les instructions du ministre de 2019 à l'intention du SCRS concernant la reddition de comptes, selon lesquelles le SCRS doit informer le ministre des activités « qui font appel à une autorisation, à une technique ou à une technologie nouvelle. Cela comprend les nouvelles utilisations des autorités, des techniques ou des technologies existantes³⁰. »

Activités faisant appel à des sources humaines

47. Récemment, le SCRS a manqué à son obligation de franchise envers la Cour en ce qui a trait à ses activités faisant appel à des sources humaines³¹. Parfois, le SCRS paie des sources humaines pour recueillir du renseignement. Souvent, l'accès qu'ont ces sources humaines à de l'information utile est directement lié à leur participation personnelle à des activités terroristes ou d'autres activités de menace. Lorsque le SCRS offre une rémunération à ces personnes pour obtenir leurs informations, il prend le risque d'enfreindre les lois qui interdisent de verser de l'argent ou de fournir toute autre ressource à l'appui d'activités terroristes ou d'autres activités criminelles. Pendant des années, le SCRS s'est appuyé sur le principe de l'immunité de la Couronne comme justification juridique de ses actions et pour continuer d'agir dans les limites de la primauté du droit. Toutefois, les lois canadiennes ont évolué au cours des dernières décennies, rendant plus ténue la possibilité d'avoir recours à l'immunité de la Couronne comme justification.

48. En 2015 et en 2016, le CSARS a soulevé des questions concernant la légalité des activités du SCRS faisant appel à des sources humaines. Notamment, le CSARS a recommandé que le SCRS obtienne un avis juridique concernant la viabilité continue du fait qu'il se fie à l'immunité de la Couronne³². En réponse, le SCRS a obtenu un avis juridique au début de 2017, qui a permis de conclure que le SCRS ne pouvait plus se servir de l'immunité de la Couronne pour justifier des activités qui, en temps normal, seraient considérées comme étant illicites. Cette information a déclenché une chaîne d'événements au sein du gouvernement qui a mené à la création d'un nouveau régime législatif permettant au SCRS de prendre des mesures qui, en temps normal, seraient considérées comme étant illicites dans le cadre de ses activités faisant appel à des sources humaines. Le nouveau régime a été introduit dans le cadre du projet de loi C-59, *Loi de 2017 sur la sécurité nationale*, qui est entré en vigueur au milieu de 2019. Toutefois, pendant que le projet de loi C-59 était à l'étude au parlement, le SCRS a décidé de poursuivre plusieurs activités

faisant appel à des sources humaines en raison de leur valeur du point de vue du renseignement, même si ces activités semblaient enfreindre la loi. Le SCRS a décidé de suspendre ces activités seulement en janvier 2019.

- 49.** En mars 2019, le CSARS a achevé sa certification du rapport annuel de 2017-2018 présenté par le directeur du SCRS au ministre de la Sécurité publique et de la Protection civile. Avant l'entrée en vigueur de la *Loi de 2017 sur la sécurité nationale*, le CSARS devait certifier la légalité des activités décrites dans chacun des rapports du SCRS à l'intention du ministre. Le rapport de 2017-2018 portait sur le recours constant du SCRS à l'immunité de la Couronne dans le contexte de ses activités faisant appel à des sources humaines. Le CSARS a examiné la situation et a conclu que le SCRS avait en fait été informé qu'il ne pouvait plus se servir de l'immunité de la Couronne à titre de défense juridique. Par conséquent, dans son certificat, le CSARS a conclu que le SCRS avait enfreint la loi en toute connaissance de cause. Le CSARS a également précisé que même si les activités du SCRS étaient importantes du point de vue de la sécurité nationale, cela ne le dispensait en aucun cas de respecter la primauté du droit ³³.
- 50.** Au début de 2018, la Cour fédérale a commencé à remettre en question le fondement juridique des activités du SCRS faisant appel à des sources humaines, indépendamment du CSARS. Ces questionnements ont entraîné une série de procédures qui ont abouti, comme mentionné, à la détermination du non-respect du SCRS à son obligation de franchise envers la Cour ³⁴. Plus précisément, le SCRS n'a pas informé la Cour que ses demandes de mandat étaient fondées sur du renseignement susceptible d'avoir été recueilli de manière illégale. La Cour a également constaté certaines omissions en ce qui a trait au rôle du ministère de la Justice Canada dans la situation. La Cour a recommandé la réalisation d'un examen indépendant plus approfondi des lacunes et défaillances systémiques, culturelles et relatives à la gouvernance démontrées par le SCRS et le ministère de la Justice, et ayant mené le SCRS à prendre des mesures illégales et à ne pas respecter son obligation de franchise envers la Cour.
- 51.** En réponse aux lacunes cernées, le gouvernement a soumis la question à l'OSSNR aux fins d'examen en vertu de l'alinéa 8(1)c) de la Loi sur l'OSSNR. L'examen est en cours ³⁵, à la demande du ministre et en vertu du pouvoir d'examen indépendant de l'OSSNR prévu à l'article 8 de sa loi habilitante. L'examen est dirigé conjointement par deux membres de l'OSSNR : l'honorable Marie Deschamps, C.C., ancienne juge de la Cour suprême du Canada; et le professeur Craig Forcese de la faculté de droit de l'Université d'Ottawa.
- 52.** Ces incidents sont préoccupants. Non seulement le SCRS a enfreint la loi, mais le SCRS et ses avocats ont également omis de divulguer des éléments importants à la Cour fédérale alors qu'ils étaient dans l'obligation de le faire. Le SCRS a également omis de fournir des avis juridiques clés au CSARS, ou il les a fournis plusieurs années en retard, même si le CSARS avait le droit, en vertu de la loi, d'obtenir cette information.

Priorités à venir

- 53.** Le mandat de surveillance de l'OSSNR comporte trois grands volets : l'examen du SCRS, l'examen du CST et l'examen des activités en matière de sécurité nationale ou de renseignement menées par toutes les autres entités fédérales. L'examen du SCRS et du CST demeure au cœur de la mission de l'OSSNR; par contre, au cours des prochaines années, l'OSSNR répertoriera et examinera de façon systématique les activités de collecte d'autres ministères. Ce faisant, l'OSSNR examinera en profondeur les activités de collecte pour s'assurer qu'elles sont légales, raisonnables et nécessaires. En d'autres mots, l'OSSNR vérifiera non seulement si un ministère peut recueillir de l'information, mais aussi s'il est raisonnable qu'il le fasse, compte tenu de son mandat et des conséquences sur la vie privée.
- 54.** Pendant nos examens, l'OSSNR examinera tout particulièrement l'utilisation des technologies d'un ministère ou d'un organisme, surtout les technologies nouvelles ou émergentes qui présentent les plus grands risques. Après ses examens, l'OSSNR formulera des recommandations dans l'optique d'améliorer les procédures ministérielles visant à gérer les risques juridiques et les risques relatifs à la vie privée que comporte l'utilisation des technologies. Le cas échéant, l'OSSNR examinera la franchise ministérielle auprès des ministres et des organes de surveillance, conformément au plus vaste système de reddition de compte en matière de sécurité nationale et de renseignement au Canada.
- 55.** Pour atteindre ces buts, l'OSSNR investira dans le développement d'une expertise technologique interne, par une combinaison d'embauche d'experts en technologies, de formation et de sollicitation de la communauté technologique élargie. De plus, l'OSSNR collaborera avec les organes redditionnels alliés par l'intermédiaire d'un forum appelé le Conseil de surveillance et d'examen du renseignement du Groupe des cinq (FIORC) ³⁶. L'OSSNR cherchera à se tenir à jour en ce qui concerne les technologies nouvelles et émergentes, comme l'intelligence artificielle, l'apprentissage machine et l'informatique quantique, de même que les inquiétudes qu'elles soulèvent, comme les « mégadonnées ». Notre objectif est de pouvoir revoir l'usage ministériel de ces technologies et leurs effets en temps opportun et de manière efficace.
- 56.** En outre, l'OSSNR travaille de concert, et continuera de le faire, avec le Commissariat à la protection de la vie privée du Canada (CPVP) et le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) sur des questions d'intérêt commun pour s'assurer de couvrir l'éventail le plus vaste possible des points de vue.

SCRS

- 57.** Au cours de la prochaine année, l'examen en profondeur du SCRS portera surtout sur l'examen qui découlera de la décision de la Cour fédérale mentionnée plus haut.

58. De plus, l'OSSNR répertoriera systématiquement l'utilisation des technologies par le SCRS et les pouvoirs conférés par mandat. Par la suite, l'OSSNR examinera les technologies et les pouvoirs qui présenteraient les plus grands risques. Ainsi, au fil du temps, l'OSSNR acquerra des connaissances sur les activités les plus intrusives du SCRS. L'OSSNR examinera également plus en profondeur le processus relatif aux mandats afin de surveiller la franchise du SCRS à l'égard de la Cour fédérale.
59. En outre, la *Loi de 2017 sur la sécurité nationale* a conféré au SCRS de nouveaux pouvoirs. L'OSSNR examinera l'utilisation de ces pouvoirs au cours des prochaines années pour aider le Parlement à réaliser l'examen législatif de la *Loi de 2017 sur la sécurité nationale*, qui commencera en 2022 ou en 2023. Plus précisément, l'OSSNR examinera l'usage que fait le SCRS des ensembles de données, y compris ceux qui sont accessibles au public, de même que le nouveau régime de justification des activités que mène le SCRS pour recueillir des données, lesquelles seraient autrement illicites. L'OSSNR est également tenu d'examiner chaque année au moins un aspect des activités du SCRS dans l'exercice de son mandat de réduction de la menace. Ce mandat autorise le SCRS à aller au-delà de la collecte d'information afin de prendre des mesures actives pour « réduire » les menaces à la sécurité du Canada. Au cours des prochaines années, l'OSSNR fera le point sur l'utilisation que fait le SCRS de ces pouvoirs qui lui ont été conférés depuis 2015.

CST

60. Dans l'exercice de ses fonctions, le CST fait quotidiennement appel à un éventail de pouvoirs et de technologies de collecte. Au fil du temps, l'OSSNR compte examiner en profondeur la gamme complète des techniques de collecte en place au CST. Dans un premier temps, l'OSSNR se penchera sur des techniques de collecte autorisées par le ministère et les comparera aux techniques autorisées par d'autres voies. En outre, l'OSSNR examinera de quelle manière le CST traite l'information interceptée accidentellement, surtout l'information qui touche des Canadiens ou des personnes au Canada, et la façon dont le CST décide de conserver ou non cette information.
61. L'évolution technologique rapide dans des domaines tels que l'informatique quantique, la 5G et l'intelligence artificielle affectera les travaux du CST, peut-être plus que toute autre entité fédérale. Ces technologies pourraient entraîner la collecte de nouvelles informations ou le développement de nouvelles techniques de collecte. Grâce à notre expertise technique en expansion dans ces domaines, l'OSSNR effectuera des examens généraux et ciblés de l'utilisation de ces technologies.
62. La *Loi de 2017 sur la sécurité nationale* a également conféré de nouveaux pouvoirs au CST, notamment la possibilité de mener des cyberopérations défensives et offensives. Le CST ne peut pas invoquer ces pouvoirs pour recueillir de l'information séparément des autorisations conférées par ses mandats relatifs au renseignement étranger et à la cybersécurité. Lorsque le CST entreprendra ces opérations, l'OSSNR les examinera pour s'assurer que le CST ne s'en sert pas pour recueillir de l'information ou que les opérations n'entraînent pas une telle collecte.

Autres ministères fédéraux

- 63.** Dans le cas des entités autres que le SCRS et le CST, les premiers examens de l'OSSNR serviront à constituer une connaissance de base des ministères ayant des programmes importants de collecte. Il est à noter que le CPSNR a déjà examiné les activités relatives à la sécurité et au renseignement de l'Agence des services frontaliers du Canada (ASFC), et celles du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC). Ces examens ont cerné certains secteurs de risque, y compris le recours à ce qu'on appelle le « ciblage fondé sur des scénarios », qui sert à contrôler les voyageurs qui entrent au pays, de même que le recours par l'ASFC à la surveillance secrète³⁷. L'OSSNR s'appuiera sur les travaux du CPSNR pour examiner en profondeur les activités de collecte de ces ministères et organismes.
- 64.** L'OSSNR a également l'intention de répertorier la collecte au sein du reste de l'appareil fédéral de la sécurité nationale et du renseignement. En particulier, l'OSSNR étudiera les programmes de collecte de la GRC en examinant en détail le programme des enquêtes criminelles relatives à la sécurité nationale de la GRC et la façon dont la GRC recueille du renseignement pour appuyer ces enquêtes. Tout au long de la surveillance, l'OSSNR gardera en tête les inquiétudes du public en ce qui a trait à l'application de la loi et portera attention aux activités de la GRC dans des secteurs délicats et à toute apparence de partialité.
- 65.** Au cours des trois prochaines années, l'OSSNR examinera les activités de collecte à Affaires mondiales Canada (AMC). L'OSSNR répertoria également la collecte et l'utilisation des données biométriques dans l'ensemble du gouvernement en ce qui a trait aux activités relatives à la sécurité et au renseignement. L'examen analysera la collecte et l'utilisation des données biographiques par Immigration, Réfugiés et Citoyenneté Canada, l'ASFC et Transports Canada en ce qui concerne leurs responsabilités en matière de sécurité nationale, et sondera l'utilisation des données biométriques par le SCRS et la GRC dans les enquêtes policières touchant le renseignement de sécurité et la sécurité nationale.
- 66.** Parmi les secteurs de collecte nouveaux et complexes que l'OSSNR examinera, est la collecte du renseignement financier. Le renseignement financier est une composante de base de la collecte d'information relative à la sécurité nationale, surtout en ce qui a trait au terrorisme. Il est également au cœur de vastes opérations de renseignement d'application de la loi, surtout celles qui concernent le blanchiment d'argent et le financement d'activités terroristes. Le centre d'expertise et de responsabilité du renseignement financier au Canada est le Centre d'analyse des opérations et des déclarations financières du Canada (CANAFE). L'OSSNR examinera les activités de CANAFE et sa relation avec les partenaires nationaux.
- 67.** Au cours de la prochaine année, l'OSSNR réalisera des examens ciblés du MDN et des FAC. L'OSSNR a déjà commencé à examiner l'Unité nationale de contre-ingérence des Forces canadiennes pour déterminer la façon dont cette unité mène ses activités de collecte relative à la contre-ingérence, en particulier la façon dont

les activités de l'unité s'inscrivent dans les cadres juridiques et de gouvernance en se concentrant sur les cas d'extrémisme de droite. L'OSSNR examinera aussi l'entreprise du renseignement de défense, afin d'en obtenir un aperçu général et de connaître son positionnement au sein des cadres de gouvernance et des autorités du MDN et des FAC. À la lumière de la récente couverture médiatique, l'examen portera sur le renseignement médical et de sources ouvertes.

Renseignement médical et renseignement de santé publique

68. Compte tenu de la pandémie de la COVID-19, l'OSSNR étudiera la façon dont le gouvernement du Canada recueille le renseignement sur des questions médicales ou sur la santé des Canadiens. C'est ce qu'on appelle le renseignement médical ou le renseignement de santé publique. À l'heure actuelle, l'OSSNR n'a pas une bonne compréhension de ce que le gouvernement considère comme étant du renseignement médical ou de la portée dans laquelle le renseignement médical est utilisé. Pour pallier ce manque, l'OSSNR examinera l'Agence de la santé publique du Canada, de même que le MDN et les FAC, dont les homologues américains exploitent le National Center for Medical Intelligence. Au Canada, les questions médicales ne font pas habituellement partie du discours public en ce qui concerne ce qui devrait ou ne devrait pas être des priorités du gouvernement en matière de renseignement. Le renseignement médical sera un domaine complètement nouveau pour l'OSSNR. L'OSSNR espère que l'examen entraînera une conversation utile à la lumière des événements en cours.

Section III

— Protection

69. La protection renvoie à la protection des personnes, de l'information et d'autres biens gouvernementaux au sein du portefeuille de la sécurité nationale et du renseignement. L'information recueillie, analysée et utilisée au sein de l'appareil est souvent de nature délicate, soit en raison des sources et des méthodes employées pour les obtenir, soit en raison des protections juridiques connexes ³⁸.

70. Les conséquences sont réelles lorsque les mesures de protection échouent. Si des acteurs hostiles, comme des terroristes ou des gouvernements étrangers, devaient accéder à de l'information sur des sources humaines, par exemple, des vies pourraient être en péril. De même, si des acteurs hostiles apprenaient des détails sur les méthodes électroniques de collecte, ils pourraient appliquer des contre-mesures, ce qui limiterait la connaissance du Canada sur des priorités clés de sécurité et de renseignement. Il y a également un risque d'atteinte à la réputation de l'appareil canadien de la sécurité et du renseignement si les alliés avaient l'impression que l'information de nature délicate qu'ils échangent avec le Canada, en toute confiance, n'était pas bien protégée. Il incombe donc au gouvernement de faire en sorte qu'une telle information soit à l'abri de l'exploitation, de la compromission ou d'une communication non autorisée.

71. Au cours des dernières années, plusieurs atteintes à la sécurité ont démontré que l'appareil de sécurité nationale canadien n'est pas immunisé contre les risques de « menaces internes »³⁹. Le premier rappel public contemporain de ce risque a été la poursuite en justice de Jeffrey Delisle. Il était enseigne canadien de vaisseau de 1re classe, et, en 2007, il a commencé à divulguer de l'information classifiée au gouvernement russe⁴⁰. Le 30 novembre 2013, Qing Quentin Huang a été arrêté et accusé de tentative de communication d'information protégée à l'ambassade de Chine à Ottawa. M. Huang était un employé d'un secteur fournissant des services spécialisés au gouvernement⁴¹. L'année dernière, la police a déposé des accusations contre Cameron Ortis, un cadre supérieur civil à la GRC, pour avoir communiqué de l'information classifiée à des entités étrangères⁴². Les affaires *Huang* et *Ortis* sont toujours devant les tribunaux.

Politique de protection et critères juridiques minimaux

72. Le mot « protection » n'est ni un terme technique juridique ni un terme défini avec précision dans les politiques. Il englobe plusieurs éléments distincts regroupés en raison de leur incidence sur la protection des personnes, de l'information et des biens. C'est pourquoi les règles de protection commencent par deux instruments de politique qui régissent la gestion de la sécurité au gouvernement du Canada: la Politique sur la sécurité du gouvernement et la Directive sur la gestion de la sécurité⁴³. Ces instruments de politique énoncent les diverses exigences auxquelles doivent se conformer les organisations et les employés pour assurer la sécurité en milieu de travail.

73. Le Secrétariat du Conseil du Trésor (SCT) est l'organisme gouvernemental responsable d'établir les normes minimales, ou les mesures de protection, suivies pour appuyer ces instruments de politique; elles couvrent les éléments suivants:

- l'assurance de l'information et de l'identité;
- les enquêtes de sécurité;
- la sécurité matérielle;
- la sécurité des technologies de l'information⁴⁴;
- la gestion des urgences et de la continuité des activités;
- les marchés publics⁴⁵.

74. Les politiques et les procédures propres aux ministères et organismes dans l'ensemble de l'appareil de la sécurité et du renseignement, qui découlent des normes du SCT, indiquent également d'autres exigences de sécurité⁴⁶. Bien qu'il soit important de définir ce que signifie la protection, il est tout aussi important de comprendre ce qu'elle n'est pas. Dans le présent contexte, la protection ne couvre pas les mesures visant les personnes qui n'ont pas accès à l'information ou aux biens de nature délicate du gouvernement⁴⁷.

75. Les employés de l'appareil de la sécurité et du renseignement peuvent également être tenus responsables d'atteintes aux dispositions de la Loi sur la protection de l'information (LPI)⁴⁸, qui présente les diverses infractions concernant la manipulation de documents classifiés. Par exemple, selon la LPI, des « renseignements opérationnels spéciaux » sont les renseignements à l'égard desquels le gouvernement fédéral prend des mesures de protection⁴⁹.
76. L'un des objectifs importants de la LPI est d'interdire la révélation illicite d'information de nature délicate. Cependant, un mécanisme autorise les situations dans lesquelles une personne croit que la révélation d'une telle information est d'intérêt public (c'est-à-dire une dénonciation), par exemple, pour empêcher des fonctionnaires de commettre un crime dans l'exercice de leurs fonctions. La protection des dénonciateurs permet de se prémunir contre les atteintes à la confiance du public qui effritent la confiance qu'a le public à l'égard des pratiques du gouvernement. La protection des dénonciateurs confère à une personne une légitime défense potentielle en cas de poursuites pour certaines infractions à la LPI⁵⁰.
77. Parce que les enjeux sont élevés lorsqu'une information protégée est révélée, la LPI prévoit des conditions préalables qui permettraient à une personne accusée de telles révélations d'éviter une responsabilité criminelle⁵¹. Si les conditions sont remplies, le tribunal se livrera à un exercice de prépondérance pour déterminer si la révélation était d'intérêt public. Parmi ces conditions préalables, mentionnons les facteurs de pondération, comme la gravité du risque de préjudice causé par la révélation et la gravité de l'infraction présumée. Cependant, si l'accusé allègue qu'une infraction a été commise (et sauf si la révélation de l'information est nécessaire pour éviter des blessures graves ou la mort), le juge peut décider que l'intérêt public l'emporte sur la révélation seulement si l'accusé a d'abord dénoncé l'acte répréhensible. L'OSSNR est la dernière étape dans la chaîne de dénonciation.

Thèmes relatifs à la protection

78. Le concept de protection a une incidence sur le travail de l'OSSNR, et ce, de trois façons majeures. D'abord, comme expliqué précédemment, l'Office a des procédures pour recueillir les témoignages des dénonciateurs qui souhaitent signaler des actes répréhensibles. Ensuite, l'Office doit s'assurer que nos membres, nos employés et nos systèmes veillent à ce que l'intégrité de l'information et des biens de nature délicate ainsi que des personnes ne soit pas compromise. Enfin, l'Office joue un rôle fondamental dans le cadre des activités d'examen et d'enquête sur les plaintes en déterminant si les systèmes de gouvernance utilisés pour décourager et détecter les actes répréhensibles ou pour atténuer les risques de tels actes sont conformes, raisonnables et nécessaires.
79. L'OSSNR a décidé de faire de la protection un thème prioritaire qui sera étudié chaque année. Ce faisant, nous contribuerons à déterminer dans quelle mesure l'appareil de la sécurité et du renseignement protège adéquatement ses employés,

ses informations et ses biens, et si de telles pratiques sont légitimes, raisonnables et nécessaires pour réduire les risques cernés. C'est pourquoi dans notre première année, l'OSSNR a complété un examen de la protection au sein du SCRS et en a débuté une autre au sein du MDN. L'examen visant le MDN était en cours au moment d'écrire ces lignes. En appréhendant globalement les résultats de ces deux examens parallèlement aux informations de source ouverte, il est possible de formuler des observations plus larges sur la protection.

- 80.** Une observation majeure est l'importance de rester vigilant au chapitre de la sécurité. Actuellement, le système de sécurité assure un examen attentif à intervalles prédéterminés – filtrage avant l'embauche, mises à jour quinquennales des cotes de sécurité, semaine de sensibilisation à la sécurité organisée chaque année au profit des employés, etc. – et comprend des périodes (entre ces intervalles) où la sécurité est moins saillante. De plus, si d'autres priorités prennent le dessus, le temps entre ces intervalles est susceptible d'augmenter. Dans le cas de M. Delisle, par exemple, sa cote de sécurité de niveau très secret était arrivée à échéance et n'avait pas été mise à jour comme elle aurait dû l'être avant son arrivée dans les installations gouvernementales où il a commis ses crimes. Or, si les normes en matière de cote de sécurité avaient été appliquées correctement, sa loyauté à l'égard du Canada aurait été évaluée et d'autres vulnérabilités auraient été scrutées⁵².
- 81.** Une autre observation majeure est le rôle fondamental joué par des politiques claires, concises et à jour pour établir des normes pour l'ensemble de l'appareil gouvernemental. Comme il a déjà été mentionné, le SCT établit des normes de sécurité minimales que les organismes et ministères fédéraux doivent suivre. Toute lacune à ce chapitre pourrait avoir un effet domino en incitant les organismes et ministères à élaborer leurs propres politiques et procédures. De telles lacunes pourraient non seulement se traduire par un manque d'uniformisation à l'échelle du gouvernement, mais aussi, dans certains cas, par une mise en application déraisonnable et superflue de pratiques en matière de sécurité.

Le polygraphe

- 82.** Une dernière observation porte sur l'utilisation par le gouvernement du polygraphe dans le cadre du filtrage des employés de la sécurité et du renseignement. Le polygraphe, communément appelé un détecteur de mensonges, est une technologie qui mesure plusieurs indicateurs physiologiques (pression sanguine, pouls, respiration, conductivité de la peau, etc.) lorsqu'une personne répond à des questions. Des réponses « trompeuse » produisent des indicateurs physiologiques qui pourraient être différenciés des indicateurs associés avec des réponses dites « non-trompeuse ».
- 83.** En vertu de la Norme sur le filtrage de sécurité du SCT, établie en 2014, le polygraphe est considéré un outil approprié pour évaluer les candidats qui doivent obtenir une cote de niveau très secret approfondie. Le SCRS utilise le polygraphe pour procéder à l'évaluation de sécurité de ses employés. Pour le SCRS, les résultats obtenus au

test constituent un élément déterminant pour l'octroi d'une cote de niveau très secret approfondie plutôt que d'être un élément éclairant pris en considération parmi un ensemble de facteurs pertinents⁵³. Pour passer un contrat avec le gouvernement du Canada, une personne, un employé ou un candidat externe doit avoir une cote de sécurité. En cas de refus ou d'annulation de cette cote de sécurité, il est impossible d'obtenir ou de conserver un emploi (ou un contrat) auprès du gouvernement fédéral. Les personnes qui se sentent lésées peuvent déposer une plainte en vertu de l'article 18 de la Loi sur l'OSSNR. Si la compétence de l'Office est établie, la plainte peut alors être enquêtée par un des membres de l'Office. Il pourrait s'agir, par exemple, d'un employé du SCRS qui perd son emploi uniquement parce qu'il s'est vu retirer sa cote par l'administrateur général sur la base de son échec au test du polygraphe. Or, vu la nature très invasive et fort controversée de cette technologie, l'Office avait décidé, dans le cadre de son dernier examen de la protection du SCRS, de se pencher sur la question du recours au polygraphe afin de déterminer si son utilisation était justifiée et dans quelle mesure il était raisonnable et nécessaire de prendre des décisions basées sur les résultats des tests.

- 84.** Cette réflexion sur l'utilisation du polygraphe a permis de formuler plusieurs observations importantes. Premièrement, le polygraphe peut avoir des répercussions délétères graves sur la santé mentale d'un employé s'il n'est pas utilisé correctement. Deuxièmement, le SCRS n'a pas été en mesure de justifier la compétence des examinateurs (qui ne sont pas des médecins) pour ce qui est de poser des questions d'ordre médical aux gens auxquels ils font passer un test. Troisièmement, les conséquences d'un échec à un test de polygraphe ne sont pas les mêmes pour les employés du SCRS et pour les candidats externes. [Texte supprimé – Au 20 novembre 2020, l'OSSNR et le SCRS ne pouvaient s'entendre sur la manière dont tous les faits de cet examen devraient être présentés dans un document public non classifié]. Fondamentalement, le résultat du test de polygraphe est un facteur déterminant pour l'octroi par le SCRS d'une cote de niveau très secret approfondie à un candidat externe. Quatrièmement, le SCRS manque de clarté de politique pour les cas où les employés échouent des tests de polygraphe. Finalement, le SCRS n'a pas réalisé une évaluation des facteurs relatifs à la vie privée en lien avec l'utilisation du polygraphe, et ce, en dépit du fait que le gouvernement exige qu'une telle évaluation soit réalisée par tout organisme ou ministère qui traite des « renseignements personnels »⁵⁴.
- 85.** Les points soulevés dans le contexte de l'examen de la protection du SCRS sont liés à une question beaucoup plus large. Notamment, dans quelle mesure le document de politique général du gouvernement, intitulé « Norme sur le filtrage de sécurité »⁵⁵, fournit aux organismes et ministères fédéraux des directives adéquates pour mettre en œuvre cette mesure de protection. Par exemple, le document précise que le polygraphe doit être utilisé avant l'octroi d'une cote de niveau très secret approfondie, mais ne donne aucune précision quant à la mise en application de cette exigence (y compris pour ce qui est des conditions relatives à l'usage raisonnable du polygraphe), laissant ainsi ces considérations clés à la discrétion de chacun des organismes et ministères.

- 86.** Le CPVP a également fait part au SCT de ses préoccupations quant à la façon dont les tests de polygraphe sont utilisés pour l'octroi d'une cote de sécurité approfondie en vertu de la Norme sur le filtrage de sécurité de 2014. Ainsi, dans une correspondance datant de juillet 2017, le CPVP a exprimé certaines préoccupations quant à l'efficacité, au degré de sensibilité du polygraphe et aux répercussions des tests sur la protection de la vie privée, ainsi qu'aux conséquences négatives qui pourraient en découler⁵⁶.
- 87.** Or, de telles observations ne sont pas nouvelles. En effet, dans sept rapports annuels successifs (de 1985-1986 à 1991-1992), le CSARS a demandé que le SCRS cesse d'utiliser le polygraphe. Une des principales raisons invoquées était les « graves doutes » du CSARS quant à l'utilisation de cette technologie puisque les résultats des tests peuvent être inexacts dans 10 % ou plus des cas⁵⁷. De plus, des tribunaux canadiens ont refusé d'admettre les résultats d'un test de polygraphe comme preuve dans le cadre de procès criminels. La Cour suprême du Canada a conclu que ces tests n'étaient pas fiables et qu'ils ne l'aideraient pas à juger de la culpabilité ou de l'innocence d'une personne⁵⁸.
- 88.** À la lumière de ce qui précède, l'OSSNR a envoyé une lettre au SCT le 12 décembre 2019 dans laquelle il sollicitait l'accès à l'avis juridique établi pour le Conseil du Trésor expliquant comment le polygraphe se conforme aux exigences juridiques canadiennes, un résumé des éléments de preuve utilisés pour établir la nécessité de recourir au polygraphe, ainsi que des évaluations démontrant comment l'utilisation du polygraphe permet d'atteindre les résultats escomptés. Or, la réponse du SCT n'a pas répondu aux questions de l'OSSNR. La lettre a toutefois précisé que des modifications étaient en train d'être apportées aux politiques sur la sécurité.
- 89.** En 1985, lorsque le CSARS avait recommandé que le SCRS cesse d'utiliser le polygraphe, cette recommandation visait à laisser au gouvernement le temps nécessaire pour tirer des conclusions définitives quant à l'opportunité pour les organismes canadiens d'utiliser cet outil et, dans l'éventualité où l'utilisation du polygraphe serait jugée opportune, pour déterminer dans quelles circonstances et en vertu de quelles règles elle l'est. Le CSARS rappelait qu'il fallait toujours, pour que les instruments de politique du gouvernement soient solides, s'assurer : i) que les approches sont uniformes à l'échelle de l'appareil gouvernemental; ii) que les risques sont bien gérés; iii) que les politiques reflètent les valeurs de la fonction publique comme la probité, la prudence, l'équité et la transparence. Or, l'OSSNR n'a obtenu aucune preuve lui permettant de croire que l'utilisation du polygraphe répond à toutes ces exigences. Dans le cadre de ses examens futurs, l'OSSNR s'attardera à l'utilisation du polygraphe ailleurs qu'au SCRS. Il pourra ainsi, à la lumière de l'information recueillie, prendre une décision définitive quant à l'utilité et la légalité du polygraphe.

Priorités relatives aux examens à venir

- 90.** L'OSSNR effectuera plusieurs examens visant les pratiques en matière de protection au cours des prochaines années afin de s'assurer que nous couvrons l'éventail le plus vaste possible d'acteurs de l'appareil de la sécurité et du renseignement. Les examens de la protection permettront à l'OSSNR de rester au fait des principales priorités du domaine, comme la légalité, la protection des renseignements personnels, les outils scientifiques et les pratiques exemplaires à l'échelle internationale.
- 91.** À titre d'organisme indépendant chargé d'évaluer le bien-fondé et la légalité, nous faisons notre propre évaluation du caractère licite des activités de l'appareil de la sécurité et du renseignement. Cette évaluation est à la base des constatations, des recommandations et des rapports de l'OSSNR. À cette fin, l'OSSNR prévoit porter une attention particulière à l'évaluation du processus visant à obtenir des conseils juridiques spécialisés. Dans le contexte de certains examens, l'OSSNR examinera le rôle du ministère de la Justice consistant à fournir une analyse juridique aux intervenants de l'appareil de la sécurité et du renseignement.
- 92.** Compte tenu de la primauté de la protection des renseignements personnels applicable à la majorité de l'information recueillie et utilisée par le gouvernement dans ce domaine, une autre priorité correspond au besoin d'évaluer le respect du gouvernement envers les droits de la protection des renseignements personnels, peu importe le bien-fondé des mesures de protection. Le CPVP, l'un des organismes de reddition de compte partenaire de l'OSSNR, contribue grandement à veiller à ce que le gouvernement respecte les lois canadiennes en matière de protection des renseignements personnels⁵⁹. L'OSSNR continuera de collaborer avec le CPVP dans le cadre de prochains examens de la protection.
- 93.** Conformément à son mandat d'évaluer le caractère raisonnable et la nécessité de l'exercice des pouvoirs d'un ministère, l'OSSNR ne compte pas se limiter à évaluer si les mesures de protection sont valides sur le plan juridique et qu'elles respectent les exigences en matière de protection des renseignements personnels. Dans le cadre de son mandat, l'OSSNR peut également évaluer la nécessité et le caractère raisonnable. Tout gouvernement qui désire continuer d'instaurer un système de sécurité adaptatif doit déterminer quels processus et outils de protection sont nécessaires en se fondant sur des preuves scientifiques et des analyses axées sur les données. Actuellement, l'OSSNR craint qu'il existe un manque d'information scientifique transparente et défendable qui soutiendrait la prise de décisions stratégiques qui visent à sélectionner des mesures de sécurité. Par conséquent, les prochains examens de l'OSSNR comprendront un examen des justifications scientifiques de mesures de protection précises.
- 94.** Enfin, l'OSSNR évaluera la possibilité que le gouvernement ait davantage recours à des pratiques de collaboration en menant des activités de sensibilisation supplémentaires auprès de partenaires étrangers de pays alliés. Même s'il est

connu que ce type d'échanges est courant au sein de certains secteurs de l'appareil de la sécurité et du renseignement, un autre aspect de ces échanges qui devrait faire l'objet d'un examen est la mesure dans laquelle les efforts de sensibilisation et de coordination sont liés aux mesures de protection, ainsi que la mesure dans laquelle ces efforts permettent de renforcer la posture de sécurité du gouvernement. Les examens de l'OSSNR donneront également un aperçu de cet aspect du point de vue des pratiques exemplaires à l'échelle internationale.

95. Cinq examens de la protection sont prévus au cours des prochaines années de manière à couvrir l'éventail le plus vaste possible d'acteurs de l'appareil de la sécurité et du renseignement. Le premier examen portera sur un aspect des enquêtes de sécurité au sein d'AMC. Le deuxième examen de la protection portera sur l'utilisation du polygraphe par le CST dans le cadre des enquêtes de sécurité des employés. Cet examen s'ajoutera aux examens annuels du CST qui abordent régulièrement diverses initiatives en matière de cybersécurité servant à protéger les systèmes du gouvernement contre l'exploitation. Le troisième examen visera l'utilisation de données biométriques dans l'ensemble du gouvernement du Canada. Les deux derniers examens évalueront certains aspects de la GRC (le premier portera sur la division consacrée à la recherche opérationnelle au sein du service de police; l'autre sur les répercussions en matière de sécurité et de protection de l'affaire Ortis, pour laquelle les examens internes de la GRC serviront de point de départ à notre analyse).
96. Cette série d'examens de la protection permettra de communiquer au Parlement et aux Canadiens des faits concernant la convenance des pratiques en matière de sécurité au sein de l'appareil de la sécurité et du renseignement, et, idéalement, contribuera à améliorer les mesures de protection. Surtout, le rôle de l'OSSNR est de s'assurer que toutes les normes de sécurité gouvernementale créées sont mises à l'essai au moyen d'examens réalisés par des experts, et que leur application fait l'objet de rapports en vue de favoriser un débat public soutenu.

Section IV

— Échange d'information

97. L'information que les ministères et organismes recueillent par leurs propres moyens est complétée à l'aide d'un processus d'échange d'information solide, tant à l'échelle nationale qu'internationale. La lutte contre le terrorisme, en particulier, nécessite une intervention intégrée impliquant plusieurs ministères et organismes, au Canada et à l'étranger. En effet, il s'agit de l'une des leçons qui ont été apprises après les attentats du 11 septembre 2001, mais elle comporte des risques et nécessite de faire preuve de prudence.
98. Toutefois, la question de l'échange d'information au sein de l'appareil de la sécurité et du renseignement ne se limite pas à l'échange d'information visant à prévenir les actes terroristes. Les ministères échangent de l'information non seulement pour prévenir des actes terroristes, mais également pour lutter contre l'espionnage, l'ingérence étrangère et la prolifération de technologies à diffusion restreinte. Ils

le font également pour faire progresser les priorités du Canada en matière de politique étrangère et de défense. De plus, les ministères échangent de l'information à grande échelle : au sein de l'appareil de la sécurité et du renseignement, mais également avec des organismes fédéraux, provinciaux et municipaux ne faisant

99. Il convient également de noter l'incidence de la technologie sur l'échange d'information. Les ministères sont non seulement en mesure de recueillir de grandes quantités d'information, mais également de communiquer cette information plus rapidement et facilement que jamais auparavant. En outre, le domaine en plein essor de l'analyse de données favorise l'échange d'information qui peut ensuite faire l'objet d'une analyse.
100. Dans ce contexte, l'échange d'information soulève des questions relativement à la protection des renseignements personnels ainsi qu'à des situations possibles de mauvais traitements à l'étranger, sans compter le besoin de protéger les sources et les méthodes sensibles lorsque de l'information est échangée. Ces questions sont importantes aux yeux des Canadiens et des responsables des politiques, alors elles le seront également aux yeux de l'OSSNR dans le cadre de nos travaux d'examen.

Cadre juridique pour l'échange d'information

101. Un cadre juridique complexe régit les activités d'échange d'information des ministères. La *Loi sur la protection des renseignements personnels* est un texte de loi général, qui ne se limite pas aux questions touchant la communication de renseignements personnels aux fins de la sécurité nationale. La Loi prévoit des règles précises concernant les cas où les organismes du gouvernement fédéral sont autorisés à communiquer des renseignements personnels et les raisons pour lesquelles ils sont autorisés à le faire. Plus récemment, le Parlement a adopté la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC)⁶⁰, qui sera abordée ci-dessous.
102. En outre, des organismes comme le CST, le SCRS et la GRC sont assujettis à des dispositions particulières de leurs lois habilitantes respectives en ce qui a trait à l'échange d'information. Les ministères peuvent aussi échanger de l'information à des fins précises en vertu de lois particulières. Par exemple, en vertu de la *Loi sur les douanes*, les fonctionnaires de l'ASFC peuvent partager des renseignements douaniers lorsque ces renseignements sont raisonnablement considérés par le fonctionnaire comme étant des renseignements qui se rapportent à la sécurité nationale ou à la défense du Canada. De même, dans certaines circonstances, CANAFE et des organismes chargés de l'application de la loi reçoivent et communiquent des renseignements financiers en vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*.
103. Les activités d'échange d'information des ministères peuvent également être façonnées par des résolutions et des ententes internationales, de même que par des directives de leurs ministres respectifs.

Défis liés à l'échange d'information

- 104.** Selon trois commissions d'enquête ayant eu lieu au cours des 15 dernières années⁶¹, ainsi que de nombreux examens effectués par les prédécesseurs de l'OSSNR, le BCCST et le CSARS⁶², nous pouvons affirmer que les principaux défis liés aux activités d'échange d'information aux fins de la sécurité nationale à l'échelle nationale et internationale sont bien documentés.
- 105.** Plusieurs questions ont été abordées dans le cadre de la Commission d'enquête du juge Major relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India⁶³, notamment la question consistant à savoir si une coopération et un échange d'information efficaces avaient eu lieu entre le SCRS et la GRC. Essentiellement, l'enquête a permis de conclure que l'incapacité d'organismes nationaux à échanger efficacement de l'information avait grandement contribué à l'écrasement tragique du vol d'Air India.
- 106.** Depuis, le SCRS et la GRC ont pris des mesures visant à renforcer leurs activités d'échange d'information et leur coopération. L'objectif d'une enquête du SCRS sur la sécurité nationale est de fournir du renseignement de sécurité au gouvernement. De son côté, la GRC recueille des éléments de preuve qui seront utilisés dans le cadre d'un processus judiciaire. Même s'ils font la collecte à des fins différentes, les deux organismes ont un intérêt commun à protéger leurs techniques d'enquête et leurs sources respectives.
- 107.** Dans le cadre d'enquêtes sur la sécurité nationale, les organismes du renseignement, surtout le SCRS, peuvent se montrer réticents à communiquer de l'information aux policiers. Les policiers, quant à eux, peuvent vouloir se tenir loin du renseignement, car il peut ultimement faire l'objet d'une divulgation; et les litiges en matière de divulgation peuvent retarder ou perturber les poursuites criminelles. Du point de vue de la sécurité du public, l'échange limité entre les organismes du renseignement et les services de police peut s'avérer dommageable. Il s'agit de la principale conclusion du juge Major. L'échange limité peut compliquer la coordination, et entraver et retarder la portée des mesures en matière de sécurité publique que peut prendre le gouvernement. Ce concept est ce qu'on appelle le dilemme du « renseignement à la preuve ».
- 108.** Pour régler cette question, le SCRS et la GRC ont élaboré le cadre de travail intitulé Une vision, qui vise à améliorer la coopération et à simplifier le processus d'échange d'information.
- 109.** La question entourant le dilemme du renseignement à la preuve faisait partie intégrante de la consultation sur la sécurité nationale à l'échelle du pays menée par le gouvernement du Canada en 2016⁶⁴. En définitive, le gouvernement n'a pas proposé de modifications législatives visant à régler cette question précisément. Toutefois, au cours de notre première année de service, l'OSSNR a entendu de la part d'un expert externe que le SCRS et la GRC étaient toujours aux prises avec ce défi. Les deux organisations sont en train de réaliser un examen approfondi afin

de trouver des moyens d'éliminer les obstacles inutiles aux activités d'échange d'information et de faciliter la prise de mesures d'application de la loi efficaces. Vu l'importance de la relation entre le SCRS et la GRC, l'OSSNR a lancé une étude de cas approfondie sur leur relation. L'étude de cas sera achevée plus tard en 2020.

Pouvoirs clairement établis pour l'échange d'information

110. Auparavant, les ministères qui voulaient échanger de l'information relative à la sécurité nationale concernant des menaces envers les intérêts et les citoyens du Canada étaient préoccupés par l'absence d'un pouvoir indépendant pour le faire. La disposition sur les « usages compatibles » de la *Loi sur la protection des renseignements personnels* peut servir dans le contexte de la sécurité nationale lorsqu'il existe un lien direct et raisonnable avec la raison pour laquelle l'information a été obtenue initialement. Toutefois, cette loi ne s'applique pas spécifiquement au contexte de la sécurité nationale⁶⁵. De manière générale, on croyait que la complexité du contexte juridique nuisait aux activités d'échange d'information avec les organismes de la sécurité nationale et du renseignement.
111. En réponse, le gouvernement a adopté la LCISC en 2015, qui établit une autorité législative unique permettant aux institutions fédérales de communiquer de l'information concernant une activité « portant atteinte à la sécurité du Canada ». L'objectif était d'améliorer l'efficacité et la rapidité des activités d'échange d'information concernant des menaces, même pour les ministères et les organismes qui ne font pas partie de l'appareil de la sécurité et du renseignement. Cependant, dans le cadre d'examens distincts au sujet des communications faites en vertu de la LCISC, le CSARS⁶⁶ et le CPVP⁶⁷ ont tous deux critiqué les contrôles internes et la tenue des dossiers des ministères.
112. La loi a été modifiée et renommée (en anglais) lors de l'adoption de la *Loi de 2017 sur la sécurité nationale*. En outre, l'OSSNR est maintenant tenu en vertu du paragraphe 39(1) de la Loi sur l'OSSNR de réaliser un examen des communications faites en vertu de la LCISC. Pour s'assurer de réaliser un examen rigoureux de ces communications, et conformément à l'autorisation légale de coordination en vue d'éviter un dédoublement inutile du travail, l'OSSNR et le CPVP ont convenu de collaborer dans le cadre de ces examens.

- 113.** L'OSSNR ne se limite pas à la LCISC et se concentre sur d'autres aspects du défi consistant à avoir des pouvoirs clairement établis relativement à l'échange d'information aux fins de la sécurité nationale. Au cours de notre première année d'existence, l'OSSNR a choisi de réaliser trois examens portant notamment sur la collecte d'information incidemment et son utilisation par le CST concernant l'identité de Canadiens, notamment la communication de cette information à des ministères. De manière générale, lorsque le CST communique à des ministères et organismes des rapports en matière de renseignement, il supprime l'information relative à l'identité de Canadiens, qui est recueillie incidemment dans le cadre de ses activités liées au renseignement étranger ainsi que de ses activités liées à la cybersécurité et à l'assurance de l'information. Toutefois, les ministères et organismes qui peuvent démontrer avoir une autorisation légale et une justification opérationnelle pour recevoir de l'information sur l'identité de Canadiens peuvent présenter une demande de communication de l'information au CST. L'OSSNR prévoit achever un examen plus tard en 2020 axé sur le caractère licite et approprié des communications d'information sur l'identité de Canadiens, ainsi qu'un examen axé sur les arrêtés ministériels et les autorisations ministérielles du CST.

MODÈLE DE COMMUNICATION D'INFORMATION DE LA LCISC

AVANT LA COMMUNICATION

Une institution fédérale demande de l'information auprès d'une autre institution fédérale. L'institution destinataire doit figurer à l'annexe 3 de la Loi.

Une institution fédérale, de sa propre initiative, décide de communiquer de l'information à une institution fédérale qui figure à l'annexe 3 de la Loi.

L'information que l'institution fédérale envisage de communiquer concerne des activités qui portent atteinte à la sécurité du Canada telles qu'elles sont définies à l'article 2 de la Loi.

TEST DE COMMUNICATION

L'institution qui communique l'information est convaincue :

- a) que la communication aidera à l'exercice de la compétence ou des attributions de l'institution fédérale destinataire prévues par une loi fédérale ou une autre autorité légitime; et
- b) que l'incidence de la communication sur le droit à la vie privée d'une personne sera limitée à ce qui est raisonnablement nécessaire dans les circonstances. (Alinéas 5(1)(a) et 5(1)(b)).

AUTRES EXIGENCES

Copie à l'OSSNR

En ce qui a trait à l'exigence de conservation de documents, une copie de chaque dossier de communication envoyée ou reçue doit être remise annuellement à l'OSSNR. (Paragraphe 9[3])

Destruction ou remise

L'institution destinataire détruit ou remet à l'expéditeur, dès que possible après leur réception, les renseignements personnels qui lui sont communiqués et qui ne sont pas nécessaires à l'exercice de sa compétence ou de ses attributions prévues par une loi fédérale ou une autre autorité légitime à l'égard d'activités portant atteinte à la sécurité du Canada. (Paragraphe 5.1 [1])

(suite)

Exactitude et fiabilité

L'institution fédérale qui communique de l'information en vertu du paragraphe (1) doit également fournir, au moment de la communication, des renseignements sur l'exactitude de l'information et la fiabilité quant à la façon dont celle-ci a été obtenue. (Paragraphe 5[2])

Conservation de documents

L'institution fédérale détruit ou remet à l'expéditeur, dès que possible après leur réception, les renseignements personnels, au sens de l'article 3 de la Loi sur la protection des renseignements personnels, qui lui sont communiqués au titre de l'article 5 et qui ne sont pas nécessaires à l'exercice de sa compétence ou de ses attributions prévues par une loi fédérale ou une autre autorité légitime à l'égard d'activités portant atteinte à la sécurité du Canada (paragraphe 5.1[1]) à moins que la conservation ne soit légalement exigée. (Paragraphe 5.1[2]).

SCRS - Exception

Les exigences de conservation de documents ne s'appliquent pas au Service canadien du renseignement de sécurité à l'égard des renseignements qui se rapportent à l'exercice de ses fonctions aux termes de l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité*. (Paragraphe 5.1[3]).

Examen du dossier des incidents liés à la protection des renseignements personnels du CST

- 114.** Le premier examen de l'OSSNR sur le CST abordait la question de l'information sur l'identité de Canadiens. L'examen portait sur le dossier des incidents liés à la protection des renseignements personnels du CST, qui contient des incidents liés à la protection des renseignements personnels découverts par le CST. Un incident lié à la protection des renseignements personnels a lieu lorsque les renseignements personnels d'un Canadien, d'une Canadienne ou d'une personne au Canada peuvent être compromis d'une façon contraire aux politiques du CST ou d'une façon non établie dans ces dernières. L'examen du dossier des incidents liés à la protection des renseignements personnels consistait en un examen annuel réalisé par le BCCST, l'ancien organisme d'examen indépendant du CST. Dans le cadre de cet examen, selon une analyse d'un échantillon d'incidents signalés dans le dossier des incidents liés à la protection des renseignements personnels pour la période allant du 1er juillet 2018 au 31 juillet 2019, l'OSSNR a félicité le CST pour sa réaction rapide pour ce qui est de signaler les incidents liés à la protection des renseignements personnels et d'atténuer les risques connexes. Toutefois, l'OSSNR a présenté cinq autres conclusions et recommandations correspondantes à l'intention du CST pour qu'il améliore sa documentation ainsi que ses pratiques en matière de protection des renseignements personnels et d'atténuation des risques.

Échange d'information avec les partenaires internationaux et risque de mauvais traitements

- 115.** L'enquête du juge O'Connor sur les actions des responsables canadiens relativement à Maher Arar a fait la lumière sur les circonstances dans lesquelles un citoyen canadien, Maher Arar, a été livré à la Syrie et torturé. L'enquête a notamment abouti à la conclusion que l'échange d'information inexacte ou non assortie d'une mise en garde⁶⁸ avec des partenaires étrangers peut mettre des individus à risque de mauvais traitements et de torture, comme dans le cas de M. Arar.
- 116.** Le gouvernement a réagi en publiant une série d'instructions ministérielles sur l'échange d'information avec des partenaires étrangers, ce qui a mené à la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, qui a pris effet en 2019 et qui requerrait la transmission d'instructions écrites par la gouverneure en conseil aux administrateurs généraux de plusieurs ministères et organismes. Les instructions de la gouverneure en conseil ont codifié les attentes à l'égard de ces organisations. En particulier, il est maintenant expressément interdit de communiquer de l'information qui entraînerait un risque sérieux que de mauvais traitements soient infligés à un individu. De plus, ces instructions restreignent l'utilisation de toute information vraisemblablement obtenue par suite de mauvais traitements infligés à un individu.

117. Tout au long de son existence, le CSARS a accordé une attention particulière à la façon dont le SCRS échangeait de l'information avec des partenaires étrangers. Il s'est aussi expressément penché sur la mise en application des instructions ministérielles pertinentes. Il a continué de surveiller ces enjeux à l'exercice 2018–2019, dans le cadre de deux examens distincts de postes à l'étranger du SCRS. Le premier a porté sur la nécessité que le SCRS instaure et suive un processus décisionnel rigoureux relativement à l'échange d'information avec des partenaires étrangers, et que ce processus s'appuie sur des ententes conclues avec eux qui seraient fondées sur des évaluations exhaustives de leur bilan au chapitre des droits de la personne.
118. Le second examen de poste à l'étranger visait aussi la relation du SCRS avec ses partenaires étrangers dans la région géographique couverte par le poste. Dans ce cas-ci, tous les partenaires étrangers étaient associés à un risque élevé sur le plan des droits de la personne, ce pour quoi des restrictions ont été imposées à l'égard de toute entente conclue avec eux dans le secteur de responsabilité du poste.
119. Un des premiers examens de l'OSSNR a porté sur les modifications aux procédures et politiques du SCRS en matière d'échange d'information. Dans le cadre de cet examen, l'OSSNR a analysé en détail trois cas associés à un risque élevé qui avaient été étudiés par le Comité d'évaluation des échanges d'information du SCRS ⁶⁹. L'examen a débouché sur deux recommandations visant à s'assurer que les décisions sont prises à un niveau conséquent avec l'évaluation du risque et que, au besoin, des avis juridiques sont sollicités avant d'échanger de l'information avec une entité étrangère afin de veiller à ce que les échanges soient conformes à la loi et aux instructions ministérielles.
120. En vertu de sa loi habilitante, l'OSSNR est maintenant tenu d'examiner dans quelle mesure les ministères ont mis en œuvre les instructions de la gouverneure en conseil relativement à l'échange d'information avec des partenaires étrangers sous le régime de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*. À ce jour, la gouverneure en conseil a émis ces instructions à 12 ministères, dont plusieurs n'avaient jamais reçu auparavant de directives formelles à ce sujet⁷⁰.
121. En vue d'assumer cette nouvelle responsabilité, nous avons lancé notre premier examen interorganisationnel, qui visait à évaluer comment six organismes et ministères — l'ASFC, le CST, le SCRS, le MDN, AMC et la GRC — mettaient en œuvre la directive ministérielle sur l'échange d'information avec des entités étrangères de 2017, laquelle a servi de base pour l'élaboration des instructions données en application de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*. Cet examen visait aussi à fournir une feuille de route aux ministères qui, conformément à cette loi, ont reçu de telles instructions pour la première fois en 2019.

- 122.** L'OSSNR a constaté d'importants écarts entre les six ministères et organismes pour ce qui est de la mesure dans laquelle ils ont réussi à mettre en œuvre la directive ministérielle de 2017. Certains, comme le CST, ont élaboré et diffusé des ensembles complets de politiques pour encadrer leurs activités d'échange d'information avec des partenaires étrangers, alors que d'autres peinent à mettre la directive en application. De plus, certains ont de la difficulté à mettre en place des mécanismes décisionnels indépendants des services opérationnels de première ligne lorsqu'il existe un risque de mauvais traitements. Un des principaux éléments mis en lumière par l'examen de l'OSSNR était l'application irrégulière du critère relatif au « risque sérieux » par l'ensemble des ministères et organismes. Cet aspect sera examiné dans l'avenir.

Priorités futures

- 123.** L'OSSNR a l'obligation légale expresse d'examiner la mise en œuvre des instructions de la gouverneure en conseil découlant de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* et d'examiner les échanges d'information effectués en vertu de la LCISC. Ces examens annuels visent à mettre en relief les risques potentiels occasionnés aux Canadiens lorsque des ministères et organismes communiquent des renseignements en vertu des mandats qui leur sont conférés par ces lois. L'OSSNR sera attentif à ces risques, y compris les risques potentiels de non-respect de la vie privée que posent les échanges d'information. Cela dit, l'OSSNR a aussi l'intention, parallèlement à cela, de schématiser et d'examiner l'ensemble des activités d'échange d'information des ministères, c'est-à-dire aussi celles qui sont réalisées en vertu d'autres lois et instruments juridiques, de même qu'à l'international et entre eux, avec des organismes provinciaux et territoriaux et avec le secteur privé.
- 124.** Au cours de nos trois premières années d'existence, l'OSSNR commencera à examiner les échanges d'information au sein de l'appareil de la sécurité et du renseignement. Nous focaliserons notre attention sur les principaux partenariats, de même que sur la façon dont les ministères et organismes collaborent pour assurer la sécurité des Canadiens et réaliser les objectifs du Canada en matière de défense et de politique étrangère. La portée des échanges d'information est vaste, et l'OSSNR espère parfaire notre compréhension de cet enjeu au fil du temps.
- 125.** L'OSSNR a entrepris un examen fondamental de la collaboration et des échanges d'information entre le SCRS et la GRC relativement à une enquête en particulier. L'un des objectifs de cet examen est de consigner les difficultés auxquelles ces deux organisations sont confrontées en ce qui a trait au dilemme des « renseignements mis en preuve ».

- 126.** L'OSSNR examinera d'autres partenariats cruciaux au sein de l'appareil de la sécurité et du renseignement, y compris les échanges d'information entre le SCRS et l'ASFC en vue d'empêcher des personnes ou des marchandises qui représentent une menace pour la sécurité nationale de traverser la frontière. Nous examinerons aussi de quelle façon le CST et le SCRS collaborent à la collecte du renseignement étranger utile pour les décideurs canadiens.
- 127.** De plus, l'OSSNR se penchera sur les arrangements horizontaux et sur les échanges d'information entre différents ordres de gouvernement. Par exemple, nous évaluerons les mesures instituées pour favoriser les échanges et la coopération, notamment dans le cadre des enquêtes des Équipes intégrées de la sécurité nationale. Ces équipes sont dirigées par la GRC et comptent des représentants d'autres organismes fédéraux, ainsi que de services de police municipaux et de la police provinciale dans le cas de l'Ontario et du Québec. L'OSSNR se penchera aussi sur les échanges d'information à l'extérieur du contexte antiterroriste, notamment sur la façon dont les ministères et organismes protègent la sécurité économique du Canada, en s'intéressant d'abord aux mesures prises sous le régime de la Loi sur Investissement Canada et en étendant ensuite son examen à toute la gamme d'outils dont dispose le gouvernement.
- 128.** L'OSSNR examinera les échanges d'information avec des organisations du secteur privé, par exemple les renseignements que le Centre canadien pour la cybersécurité recueille auprès d'organisations afin de prévenir ou d'atténuer les cyberattaques perpétrées par des acteurs étatiques hostiles ⁷¹, ou les renseignements que les banques à charte déclarent au CANAFE aux fins de la tenue d'enquêtes sur les opérations financières suspectes.
- 129.** Enfin, l'OSSNR reconnaît que nos examens des échanges d'information avec des partenaires étrangers nous permettent seulement de voir et de comprendre les actions du Canada. C'est pourquoi l'Office participe à des forums internationaux comme le FIORC, qui rassemble les organismes d'examen du Canada, de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis et qui vise à faire le point sur les tendances (non classifiées) à l'échelle internationale et à diffuser des pratiques exemplaires. Compte tenu des liens étroits qu'entretiennent les organismes de renseignement du Groupe des cinq, l'échange d'information fait l'objet de discussions au FIORC. Ces dernières constituent l'un des moyens dont dispose l'OSSNR pour remédier au manque potentiel de responsabilisation sur le plan de la coopération internationale.
- 130.** En somme, la coopération et l'échange d'information entre les membres de l'appareil de la sécurité et du renseignement du Canada ont toujours été des volets essentiels des efforts déployés par le Canada pour assurer la sécurité nationale. Concrètement, cela signifie que très peu d'examens de l'OSSNR n'aborderont pas la question de l'échange d'information de quelque manière. L'OSSNR sera attentif aux risques occasionnés par de tels échanges ainsi qu'à la nécessité de communiquer l'information efficacement et rapidement.

Section V

— Actions

- 131.** Le terme « action » renvoie à toute activité entreprise par un ministère ou un organisme fédéral pour influencer sur un résultat en matière de sécurité nationale ou de renseignement. Les actions peuvent aussi être le résultat d'une collecte ou d'un échange de renseignement. Le renseignement est un aspect de l'information et de l'analyse qui définit comment les actions sont interprétées et mises en œuvre. L'action elle-même, tout comme l'influence du renseignement, peut être réalisée au su (de façon manifeste) ou à l'insu (de façon secrète) des Canadiens. Une action manifeste finira par être portée à la connaissance de la personne visée, tandis qu'une action secrète ne sera peut-être jamais dévoilée.
- 132.** Les anciens organismes de surveillance, le CSARS et le BCCST, pouvaient seulement examiner les activités des principaux organismes de collecte d'information, soit le SCRS et le CST. Leurs examens des activités en matière de sécurité nationale étaient surtout axés sur la collecte, la protection et l'échange d'information. Cette portée a brièvement changé quand le Parlement a adopté la *Loi antiterroriste de 2015* et que le CSARS a commencé à mener des examens du nouveau mandat conféré au SCRS pour réduire les menaces à la sécurité du Canada. Le CSARS a effectué le seul examen postérieur de ces nouveaux pouvoirs extraordinaires. Cependant, les examens du CSARS sont demeurés circonscrits aux actions du SCRS — un sous-ensemble restreint du vaste éventail d'actions en matière de sécurité nationale entreprises chaque jour dans l'appareil de la sécurité et du renseignement du Canada.
- 133.** Le mandat de l'OSSNR n'englobe pas seulement le renseignement et les entités qui en font la collecte : il s'étend à toute activité en matière de sécurité nationale menée par tout ministère ou tout organisme. Les autorisations législatives qui nous sont conférées nous permettent de surveiller l'ensemble des activités qui correspondent à des actions. Ces activités ont rarement fait l'objet d'une surveillance indépendante, et l'OSSNR est en mesure de voir à ce que ce soit maintenant le cas.
- 134.** La *Loi de 2017 sur la sécurité nationale* a établi des mandats clairs pour les principales entités de collecte de renseignement faisant l'objet d'une surveillance, à savoir le SCRS et le CST qui les autorisent à agir dans certaines circonstances en cas de menace apparente à la sécurité nationale. En ce qui concerne le SCRS, cette nouvelle loi a mis à jour son mandat au chapitre de la réduction des menaces. Pour ce qui est du CST, elle a défini les cyberopérations actives (CA) et les cyberopérations défensives (CD) comme des aspects de son mandat. Ces nouveaux pouvoirs ne font que s'ajouter aux nombreux pouvoirs existants qui permettent à plus d'une douzaine d'autres ministères et organismes de la sécurité et du renseignement fédéraux de prendre des mesures pour assurer la sécurité nationale, ce qui fait que le groupe d'activités correspondant à des « actions » est vaste. Par exemple, les actions au sein de l'appareil de la sécurité et du renseignement comprennent l'interception de personnes et de marchandises à la frontière par l'ASFC ainsi que les arrestations pour infraction criminelle (y compris, possiblement, la détention préventive) effectuées par la GRC.

- 135.** La gamme d'actions visées par le mandat de l'OSSNR d'examiner « l'exercice par les ministères de leurs activités liées à la sécurité nationale ou au renseignement » est vaste et comprend des actions comme le fait de refuser l'entrée d'une personne au Canada, de révoquer un passeport canadien, d'inscrire une personne sur la liste établie en vertu de la *Loi sur la sûreté des déplacements aériens* (la « liste des personnes interdites de vol » du Canada), de perturber les affaires d'une personne en prenant une mesure de réduction de la menace, de détenir un terroriste présumé ou d'entreprendre des actions militaires dans le cadre d'un conflit armé. Parfois, une décision stratégique de haut niveau peut aussi constituer une activité correspondant à une action, comme l'adoption d'une politique relativement à une priorité nationale telle la sécurisation de l'Arctique.
- 136.** Les examens de l'OSSNR dans ce domaine abordent aussi d'autres domaines d'attention prioritaires. Nous pouvons examiner les actions en matière de sécurité nationale qui découlent d'une collecte de renseignement, les actions en matière de sécurité nationale qui ne sont pas liées à une collecte de renseignement, et les actions en matière de sécurité nationale qui mènent à une collecte de renseignement. Comme exemple pour illustrer cette dernière catégorie d'actions, un raid tactique réalisé par les FAC lors d'une mission outremer pourrait déboucher sur l'obtention de nouvelles sources de renseignement qui pourraient ensuite faire l'objet d'un examen du l'OSSNR dans ce domaine.
- 137.** Compte tenu de la nature principalement secrète des actions en matière de sécurité nationale et de renseignement, les effets et les incidences de ces actions sont souvent inconnus de la population. L'OSSNR est fort conscient des inquiétudes soulevées lors de nos consultations auprès de la société civile en ce qui concerne les répercussions que les actions des organismes de sécurité et de renseignement pourraient avoir sur la vie des Canadiens. Ces inquiétudes s'ajoutent aux préoccupations exprimées précédemment, qui portaient surtout sur les enjeux relatifs au respect de la vie privée soulevés par la collecte et l'échange d'information. C'est pourquoi l'un des principes fondamentaux de l'OSSNR est, dans la mesure du possible, d'assurer la transparence et la responsabilisation par nos examens des actions de l'appareil de la sécurité et du renseignement.

Observations relatives aux examens antérieurs

- 138.** Comme il a été mentionné, avant l'adoption de la *Loi de 2017 sur la sécurité nationale*, les examens ne s'étendaient pas d'ordinaire aux activités correspondant à des actions. Pour cette raison, l'OSSNR dispose seulement d'une modeste archive de documents d'examen antérieurs d'où il pourrait extraire des thèmes d'examen des actions. L'OSSNR s'emploie actuellement à établir des thèmes clés à aborder à partir des examens fondamentaux. La prochaine section du présent rapport explique l'approche qu'adoptera l'OSSNR pour ses examens futurs. Quoi qu'il en soit, certains thèmes ont ressorti des examens antérieurs des mesures de réduction des menaces (MRM) du SCRS — à savoir les seules activités correspondant à des actions qui ont fait l'objet d'examens dans le passé⁷².

- 139.** À compter de l'entrée en vigueur de son mandat concernant les MRM en 2015 jusqu'en août 2020, le SCRS n'a pas demandé de mandat à la Cour fédérale pour ce type d'activités. Au moment de leur introduction, les pouvoirs en matière de MRM ont soulevé des questions juridiques et d'éventuels préoccupations liés à la Charte. La *Loi de 2017 sur la sécurité nationale* a réglé bon nombre de ces ambiguïtés et contenait de nouvelles dispositions qui ont renforcé les protections prévues dans la Charte. L'OSSNR surveillera de près le recours aux MRM par le SCRS et examinera ses évaluations des circonstances dans lesquelles le SCRS doit obtenir un mandat pour prendre de telles mesures. L'OSSNR sera aussi attentif à la façon dont le SCRS exécute ses MRM autorisées par mandat — et il cherchera tout particulièrement à vérifier dans quelle mesure le SCRS se conforme à toutes les directives et à toutes les conditions établies par la Cour.

Activités correspondant à une action en chiffre

Mandats de MRM du SCRS présenté en vertu des articles 12.1/21.1 de la Loi sur le SCRS en 2018 et 2019

Demandes de mandats de MRM approuvées:	0
Demandes de mandats de MRM rejetées:	0

Autorisations ministérielles de CA/CD au CST en vertu des paragraphes ci-bas de la Loi sur le CST en 2019

paragraphe 29(1), cyberopérations défensives:	x
paragraphe 30(1), cyberopérations actives:	x

Le CST a confirmé qu'en 2019, des autorisations ministérielles ont été signées sous chaque paragraphe répertorié dans ce tableau. Cependant, le CST est d'avis que la publication de ces chiffres serait préjudiciable à la sécurité nationale. L'OSSNR est désaccord avec cette perspective. En date du 20 novembre 2020, ce problème n'a pas pu être résolu. L'OSSNR continuera à travailler avec le CST en vue de trouver un compromis.

CST

- 140.** D'autres thèmes ayant ressortis de notre examen des activités correspondant aux actions découlent du commentaire répandu au sein de la société civile ayant trait aux nouveaux pouvoirs du CST de réaliser des CA et des CD. Avant la promulgation de la *Loi de 2017 sur la sécurité nationale*, les mandats du CST se limitaient (principalement) à l'observation et à la collecte. Maintenant, dans le cadre de ses mandats liés aux CA et aux CD, le CST peut mener des actions par l'entremise de l'infrastructure mondiale de l'information qui ont trait aux activités de personnes ou d'entités étrangères à l'extérieur du Canada. Le CST peut mener des activités de CA dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin de réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités ou les activités d'entités dans la mesure où celles-ci se rapportent aux affaires internationales, à la défense ou à la sécurité. Le CST peut

mener des activités de CD dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci pour aider à protéger les renseignements électroniques et les infrastructures d'information des institutions fédérales ou de celles désignées comme étant importantes pour le gouvernement du Canada. Ces pouvoirs sont équivalents à ceux dont disposent les partenaires du Groupe des cinq. Ces pouvoirs habilite aussi le CST à jouer un rôle important, mais sans précédent, dans les activités qui correspondent aux actions de sécurité nationale.

141. Les groupes de défense des libertés civiles ont indiqué que les activités de CA ou de CD étaient une préoccupation principale en ce qui a trait à la *Loi de 2017 sur la sécurité nationale*, et ils soulignent précisément l'absence d'une surveillance indépendante (c'est-à-dire, une préautorisation) de ces activités. Dans le cadre du régime législatif actuel, pour que le CST puisse mener légalement une CA ou une CD, le ministre de la Défense nationale doit autoriser de telles activités. Pour que le ministre puisse accorder cette autorisation, il doit conclure qu'il y a des motifs raisonnables de croire que l'activité est raisonnable et proportionnelle, compte tenu de la nature de l'objectif à atteindre et de la nature des activités. De plus, le ministre des Affaires étrangères doit approuver les activités de CA et doit être consulté relativement aux activités de CD⁷³.
142. Les autorisations ministérielles pour les activités de CA ou le CD ne doivent pas être approuvées par le commissaire au renseignement, contrairement aux activités liées au renseignement étranger et à la cybersécurité⁷⁴. Par conséquent, aucun examen des autorisations en matière de CA ou de CD n'est réalisé par un organisme indépendant lié avant que celles-ci soient approuvées. Voilà pourquoi l'OSSNR considère comme très importants nos examens des activités de CA ou de CD. Contrairement aux MRM du SCRS, le CST n'a aucune obligation prévue par la loi d'aviser l'OSSNR qu'il réalise des activités de CA ou de CD. Or, l'OSSNR a l'intention de se concentrer de façon proactive sur ces activités.
143. Bien que la loi encadre les pouvoirs tels que les MRM et les CA ou les CD, ces activités se déroulent en secret, contrairement à d'autres types d'actions de sécurité nationale, comme les arrestations faites par la police, qui sont ouvertes et peuvent être contestées devant les tribunaux. L'OSSNR juge que l'opacité de certains types d'actions justifie des examens futurs. Plus l'action de sécurité nationale est secrète, plus il est essentiel que l'OSSNR en fasse un examen rigoureux.

Application de la loi

144. Avant la promulgation de la *Loi de 2017 sur la sécurité nationale*, c'est la Commission civile d'examen et de traitement des plaintes relatives à la GRC qui examinait les activités de la GRC ayant trait à la sécurité nationale⁷⁵. Ces activités sont maintenant examinées par l'OSSNR. La création de nouvelles infractions, particulièrement des infractions de terrorisme, et de l'accent mis sur le terrorisme, on fait en sorte que la police joue maintenant un plus grand rôle dans la sécurité nationale. La police enquête sur les crimes et joue un rôle dans la prévention de

ceux-ci. Ainsi, la police pourrait enquêter sur des infractions de terrorisme, entre autres, et, en même temps, participer à des programmes communautaires visant à lutter contre la radicalisation menant à la violence. Elle peut aussi participer à des activités de prévention du crime ou d'atténuation du risque qui ne mènent pas à des poursuites en bonne et due forme. Le système de justice pénale est l'outil traditionnellement utilisé pour tenir la police responsable. Par exemple, la conduite des policiers sera examinée soigneusement pendant un procès criminel. Toutefois, les mécanismes de responsabilité sont moins robustes lorsque la police adopte des stratégies de perturbation de menaces à la sécurité nationale qui ne sont pas contestées devant les tribunaux. Par conséquent, nous sommes d'avis que les fonctions d'examen de l'OSSNR deviendront particulièrement importantes dans ces circonstances⁷⁶.

- 145.** L'examen rigoureux des personnes et des marchandises qui traversent la frontière qu'effectue l'ASFC peut être déclenché par un renseignement provenant de partenaires nationaux ou étrangers ou de ses propres efforts de collecte d'information ou d'évaluation. Les activités de l'ASFC comprennent des fouilles à la frontière et la saisie ou l'interdiction de marchandises, de monnaie ou de personnes. Ces fouilles et la détermination par l'ASFC qu'un non-Canadien pourrait être interdit de territoire peuvent avoir des répercussions sur la liberté, la protection de la vie privée, la liberté de mouvement et les intérêts commerciaux d'une personne. La tâche de l'OSSNR consiste à examiner les activités de l'ASFC liées à la sécurité nationale et au renseignement dans le but, entre autres, de veiller à ce que l'Agence respecte rigoureusement ses obligations prévues par la loi. Cela est d'autant plus vrai à l'heure actuelle, car aucun organisme indépendant ne peut instruire les plaintes du public contre l'ASFC.

Priorités futures

- 146.** Dans le cadre de nos examens des activités correspondant aux actions, l'OSSNR formule des constatations et des recommandations sur la conformité d'une organisation à la loi et à toute instruction ministérielle applicable ainsi que sur le caractère raisonnable et la nécessité de l'exercice de ses pouvoirs. L'OSSNR est dans une position unique pour évaluer les actions visibles ou invisibles du gouvernement du Canada et pour donner aux Canadiens l'assurance que leurs organismes chargés du renseignement et de la sécurité nationale sont tenus responsables afin de protéger les intérêts du Canada en matière de sécurité nationale et de défendre les droits et libertés des Canadiens et des résidents du Canada.

- 147.** Le plan stratégique de l'OSSNR porte principalement sur l'examen de trois types d'activités correspondant aux actions : les actions opérationnelles, les actions d'application de la loi et les actions administratives (ces termes sont définis plus bas) ⁷⁷. Dans chacune des catégories suivantes, l'OSSNR a établi certaines activités d'intérêt sur lesquelles nous nous pencherons dans des examens futurs. Les éléments énumérés ne font pas nécessairement partie du plan d'examen de l'OSSNR; ils servent plutôt à souligner l'ampleur des situations qui font l'objet des examens des activités correspondant aux « actions » réalisées par l'appareil de la sécurité et du renseignement.
- *Opérationnelle* : activités correspondant à une action secrète appuyant directement un objectif de sécurité nationale. Les actions opérationnelles présentant un intérêt pour l'OSSNR comprennent les suivantes : le recours par le CST aux CA ou aux CD (examen annuel requis), les MRM du SCRS (examen annuel requis) et les opérations des FAC menées dans un théâtre et sur le champ de bataille.
 - *Application de la loi* : activités correspondant à une action secrète ou manifeste dans le but d'appliquer les lois, d'enquêter sur des crimes et de procéder à des arrestations. Les activités liées aux actions d'application de la loi sur lesquelles l'OSSNR pourrait se pencher, tout en tenant compte de l'administration de la justice et du concept de l'indépendance de la police dans les décisions faisant suite à des enquêtes, comprennent : le ciblage effectué par l'ASFC menant à la détection ou à l'interception de personnes, de marchandises et de moyens de transport à risque élevé qui constituent une menace pour la sécurité des Canadiens et les enquêtes de la GRC qui pourraient mener à une détention, à une arrestation ou à une poursuite.
 - *Administrative* : activités correspondant à une action visible réalisées lors de l'administration d'un pouvoir législatif conféré au gouvernement fédéral par le législateur. Les activités correspondant à une action administrative sur lesquelles l'OSSNR pourrait se pencher comprennent : la mise en œuvre par AMC de la politique étrangère et des sanctions commerciales, les examens des investissements qui pourraient porter atteinte à la sécurité nationale réalisés conformément à la Loi sur Investissement Canada, la décision d'ajouter une personne à la liste de la Loi sur la sûreté des déplacements aériens dans le cadre du Programme de protection des passagers et les problèmes d'admissibilité pour des raisons de sécurité nationale.
- 148.** À mesure que la capacité de l'OSSNR de mener des examens s'élargit, nous brosserons un portrait complet des actions que prennent les organismes chargés de la sécurité nationale et du renseignement pour remplir leurs mandats et évaluerons ces actions pour déterminer leur conformité aux lois, leur caractère raisonnable et leur nécessité.

Plaintes

Section I

— Mandat de l'OSSNR en matière d'enquête sur les plaintes

03



En vertu de la Loi sur l'OSSNR, l'une de ses fonctions principales est d'enquêter sur les plaintes dans les cas suivants :

- les plaintes relatives à une activité menée par le Service canadien du renseignement de sécurité (SCRS) ou le Centre de la sécurité des télécommunications (CST);
- les plaintes portées à son attention par la Commission civile d'examen et de traitement des plaintes relatives à la GRC (CCETP) concernant une activité de la Gendarmerie royale du Canada (GRC) étroitement liée à la sécurité nationale;
- les plaintes concernant le refus ou la révocation d'habilitations de sécurité aux employés et aux entrepreneurs du gouvernement fédéral⁷⁸.



- 150.** En vertu de la *Loi de 2017 sur la sécurité nationale*, l'OSSNR a hérité des fonctions de traitement des plaintes du Comité de surveillance des activités de renseignement de sécurité (CSARS) et du Bureau du commissaire du Centre de la sécurité des télécommunications, qui enquêtaient respectivement sur les plaintes liées au SCRS et au CST. De plus, l'OSSNR assume la responsabilité d'enquêter sur les plaintes relatives à la sécurité nationale qui concernent la GRC. L'OSSNR a également hérité de l'infrastructure d'enquête sur les plaintes du CSARS, mais nous avons constaté dès le début de notre mandat que le modèle du CSARS devait être amélioré pour assurer des enquêtes plus rapides et plus efficaces. L'OSSNR a donc commencé à revoir les règles de procédure en vue d'améliorer le processus global. L'OSSNR a également collaboré avec la GRC et la CCETP pour gérer efficacement les plaintes liées à la sécurité nationale dont la GRC fait l'objet⁷⁹.

Section II

— Synopsis des tendances et des principaux thèmes

151. L'OSSNR a connu une augmentation du nombre de plaintes reçues, plus précisément des plaintes contre le SCRS, ainsi que des plaintes relatives aux habilitations de sécurité. Comparativement aux statistiques sur les plaintes présentées dans le rapport annuel du CSARS de 2017-2018 et aux statistiques de 2018-2019, l'OSSNR a enregistré une augmentation de 40 % pour les dossiers de plaintes nouvellement ouverts. En particulier, le nombre de plaintes contre le SCRS a doublé, et le nombre de plaintes relatives aux habilitations de sécurité a augmenté de 30 %⁸⁰. L'OSSNR n'a pas enquêté sur la plupart des plaintes récentes contre le SCRS parce que nous avons conclu qu'elles ne relevaient pas de la compétence de l'OSSNR. Elles ne concernaient pas une activité menée par le SCRS, ou l'OSSNR était convaincu que les plaintes étaient frivoles, sans objet ou entachées de mauvaise foi⁸¹.
152. La majorité des plaintes reçues concernant le refus présumé ou la révocation d'une habilitation de sécurité ne relevaient pas du mandat de l'OSSNR, il s'est plutôt avéré qu'elles étaient liées à la cote de fiabilité ou à la cote de fiabilité approfondie du plaignant. L'OSSNR ne peut enquêter que sur les plaintes relatives aux habilitations de sécurité, et non sur les questions de cote de fiabilité. Les plaintes relatives à la cote de fiabilité doivent généralement être traitées dans le cadre d'un contrôle judiciaire devant la Cour fédérale. Par conséquent, l'OSSNR a enquêté sur très peu de plaintes relatives aux habilitations de sécurité. Une leçon tirée de la dernière année est que les ministères et les organismes devraient s'assurer de fournir des renseignements clairs et exacts sur les droits d'une personne concernant la révision et les recours, et indiquer correctement la nature du statut de sécurité en cause et l'organisme auquel la personne peut se plaindre parce qu'on lui a refusé ce statut. Dans le même ordre d'idées, l'OSSNR prend des mesures pour sensibiliser davantage le public à notre mandat, tout en veillant à ce que les plaignants soient informés de leurs mécanismes de recours le plus tôt possible afin que leur droit de demander réparation soit préservé.
153. En ce qui concerne les plaintes relatives aux habilitations de sécurité qui ont fait l'objet d'une enquête de l'OSSNR et du CSARS, certaines des questions clés portaient sur la vérification des antécédents à l'étranger et les cas où les renseignements étaient insuffisants pour accorder une habilitation de sécurité à une personne. L'une des leçons tirées de ces types de plaintes est que les ministères doivent s'assurer que les personnes reçoivent un avis écrit les informant des motifs de la décision, si cela est possible dans les circonstances (c.-à-d. que cette divulgation n'est pas interdite en vertu d'une loi fédérale). À l'avenir, l'OSSNR continuera d'encourager les parties à faire des efforts pour régler les plaintes de façon informelle le plus tôt possible.

Section III

— Protection des dénonciateurs

- 154.** La Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles (LPFDAR) est une loi sur la dénonciation qui offre aux employés du secteur public fédéral un mécanisme externe pour signaler les manquements à l'éthique et pour se plaindre des représailles dont ils croient avoir été victimes⁸². Toutefois, la LPFDAR exclut expressément les membres du SCRS, du CST et des Forces armées canadiennes (FAC), ainsi que toutes les personnes qui souhaitent divulguer des renseignements opérationnels spéciaux⁸³. Le SCRS, le CST et les FAC ont mis en place des mécanismes internes de divulgation d'actes répréhensibles, conformément aux exigences de la LPFDAR. Toutefois, la structure actuelle n'offre aucun mécanisme de rapport externe pour les divulgations de renseignements opérationnels spéciaux ou pour les employés du SCRS, du CST ou des FAC.
- 155.** Comme il a été mentionné précédemment, une «défense d'intérêt public» est disponible, dans certaines circonstances, pour les dénonciateurs canadiens qui sont astreints au secret à perpétuité et qui ont été accusés de certaines infractions en vertu de la Loi sur la protection de l'information (LPI)⁸⁴. Cette défense ne peut être invoquée que si l'accusé a suivi les étapes décrites dans la LPI avant de divulguer l'information au public⁸⁵. La LPI définit l'OSSNR comme une tribune où, dans certaines conditions, ce genre de divulgation d'actes répréhensibles peut être faite⁸⁶. Toutefois, la LPI ne décrit pas comment ce processus est censé fonctionner sur le plan de la procédure ni ne précise le rôle, le cas échéant, que l'OSSNR devrait jouer dans l'acceptation des divulgations d'actes répréhensibles d'employés du SCRS, du CST ou des FAC.
- 156.** Dans une correspondance antérieure adressée au procureur général⁸⁷, l'OSSNR a cerné ces lacunes législatives et les répercussions négatives sur la sécurité nationale qui peuvent survenir quand les pays démocratiques ont des protocoles déficients pour la dénonciation au sein de leurs appareils de la sécurité nationale et du renseignement. Entre-temps, l'OSSNR mettra en œuvre des procédures internes pour répondre aux préoccupations soulevées par les membres de l'appareil de la sécurité et du renseignement. Si la préoccupation portée à l'attention de l'OSSNR n'entre pas dans la portée de la défense d'intérêt public visé par l'article 15 de la LPI, l'OSSNR peut examiner la question si elle se rapporte au mandat d'examen de l'OSSNR, conformément au paragraphe 8(1) de la Loi sur l'OSSNR.

- 157.** En raison du contexte de menace et de sécurité nationale du Canada, il est essentiel que les secrets nationaux du Canada et les fonctionnaires qui les gardent soient adéquatement et efficacement protégés. Les modifications législatives possibles pour améliorer les protections actuelles des membres de l'appareil de la sécurité et du renseignement pourraient comprendre des modifications de la LPI, de la LPFDAR ou de la Loi sur l'OSSNR. Toute modification législative devrait comporter l'élément essentiel qu'est la responsabilisation externe, ainsi que des protections semblables à celles dont jouit le Commissariat à l'intégrité en vertu de la LPFDAR.

Section IV

— Priorités pour l'année à venir

- 158.** En 2020, l'OSSNR modernise le processus de traitement des plaintes. L'objectif de l'OSSNR demeure la tenue d'enquêtes justes et efficaces et le règlement des plaintes. L'évolution du contexte entourant les plaintes rend cette modernisation nécessaire. Deux priorités guideront la modernisation, soit l'accès à la justice pour les plaignants non représentés et un plus large éventail d'outils pour simplifier le règlement des plaintes.
- 159.** À cette fin, l'OSSNR met à jour notre site Web et révisé nos formulaires afin de fournir des directives plus claires aux plaignants éventuels. Nous avons l'intention de mettre davantage l'accent sur l'explication de la compétence de l'OSSNR et sur la façon de déposer une plainte; de ce fait, les plaintes devraient être examinées plus rapidement et être traitées dans la tribune appropriée. De plus, un guide à l'intention des plaignants non représentés se trouvera sur le site Web, afin que ces derniers puissent mieux s'y retrouver à chaque étape du processus et régler leur plainte de façon appropriée.
- 160.** Il n'y a pas de solution universelle. Chaque plainte que l'OSSNR reçoit exige une approche unique. Comme il a été mentionné, nous sommes en train de mettre à jour nos règles de procédure. Les nouvelles règles permettront d'accroître la souplesse, l'efficacité et la transparence. Voici quelques-uns des changements à l'étude : une discussion sur les attentes avec le plaignant dès le départ; un nouveau processus qui permet de déterminer rapidement la compétence; une entrevue avec le plaignant; plus d'options de règlement informel; la divulgation rapide et uniformisée de l'information entre les parties; et une exigence relative aux sommaires et aux chronologies des dossiers non classifiés. L'OSSNR croit que ces changements permettront d'enquêter sur les plaintes plus rapidement et plus efficacement.

Engagement et transparence

04



Comme l'indique le préambule de la *Loi de 2017 sur la sécurité nationale*, « la confiance de la population envers les institutions fédérales chargées d'exercer des activités liées à la sécurité nationale ou au renseignement est tributaire du renforcement de la responsabilité et de la transparence dont doivent faire preuve ces institutions »⁸⁸. Ce sont là, en plus de la participation du public, des valeurs fondamentales de l'OSSNR, toutes considérées comme essentielles pour la réalisation de notre mandat. Les avantages de la participation du public ont été soulignés au cours des dernières années, notamment dans le cadre des consultations sur la sécurité nationale menées par le gouvernement en 2016. La mobilisation des intervenants au cours de notre première année d'activité a aidé à établir des liens et des relations sur lesquels nous nous appuierons au cours des années à venir. Comme il est indiqué dans la présente section, l'OSSNR a pris des mesures énergiques au cours de notre première année d'activité afin de promouvoir une plus grande transparence des activités liées à la sécurité nationale et au renseignement. En plus de nos propres initiatives, l'OSSNR continuera d'encourager les ministères et les organismes à promouvoir la transparence de leurs activités, y compris dans le respect de l'Engagement de transparence en matière de sécurité nationale⁸⁹.



Section I

— Engagement

- 162.** En 2019, l'OSSNR a lancé une série de consultations publiques afin de mieux faire connaître l'organisation, d'élargir notre réseau et d'approfondir notre compréhension des préoccupations des Canadiens concernant les activités de sécurité nationale et de renseignement. En 2019 et en 2020, nous avons entrepris des séances de mobilisation partout au pays avec divers intervenants, y compris des universitaires, des représentants de la société civile, des organismes d'application de la loi et des organismes gouvernementaux.
- 163.** Ces séances ont été une occasion précieuse pour l'OSSNR d'entendre les intervenants parler des programmes et des enjeux qu'ils ont recommandés à l'OSSNR pour examen, ainsi que des risques liés à la protection de la vie privée et aux libertés civiles que, selon eux, ces programmes présentaient. Les commentaires uniformément positifs que l'OSSNR a reçus des intervenants ont démontré la valeur de ces engagements.
- 164.** À l'échelle internationale, l'OSSNR continue de participer activement aux activités du Conseil de surveillance et d'examen du renseignement du Groupe des cinq, ce qui nous permet : de mieux connaître les thèmes internationaux transversaux dans le domaine de la responsabilisation liée à la sécurité nationale et au renseignement; d'échanger des priorités et de comparer des pratiques exemplaires; de collaborer sur des questions clés d'intérêt mutuel; et de promouvoir un examen coordonné des questions d'importance internationale.
- 165.** Au cours de la prochaine année, l'OSSNR a l'intention de poursuivre notre programme de sensibilisation et d'engagement. Nous profiterons des occasions de communiquer par vidéoconférence avec les intervenants à l'échelle nationale et internationale et, dans la mesure du possible, en personne. Au cours de la prochaine année, l'engagement portera principalement sur les quatre domaines importants suivants :
- développer notre réseau en ce qui concerne les questions liées aux technologies nouvelles et émergentes (y compris l'intelligence artificielle), afin de mieux comprendre leur utilisation ainsi que les risques et les possibilités qu'elles présentent du point de vue de la responsabilisation en matière de sécurité nationale;
 - élargir notre dialogue avec les intervenants afin d'éclairer les priorités des examens futurs;
 - établir de nouvelles relations avec les groupes communautaires afin de démystifier le processus d'enquête sur les plaintes;
 - accroître les efforts de recrutement pour s'assurer que nous continuons à bâtir un effectif d'élite aux compétences et aux expériences diversifiées.

Section II

— Transparence

- 166.** L'OSSNR a pris un certain nombre de mesures pour accroître l'ouverture et la transparence de notre travail et du travail de l'appareil de la sécurité nationale et du renseignement. Nous avons créé un compte Twitter⁹⁰ au début de notre mandat, que nous utilisons pour partager du contenu, fournir des mises à jour sur notre travail et fournir une plateforme de dialogue sur les questions de sécurité.

Caviardage et rédaction pour diffusion

- 167.** Au cours des derniers mois, l'OSSNR a commencé à publier des rapports de notre organisme prédécesseur, le Comité de surveillance des activités de renseignement de sécurité (CSARS), qui avaient été caviardés pour communication aux personnes qui avaient demandé à voir les rapports en vertu de la *Loi sur l'accès à l'information*. En vertu de la *Loi sur l'accès à l'information*, les rapports devaient seulement être remis au demandeur. Pour favoriser la transparence, l'OSSNR prévoit publier graduellement en ligne des versions caviardées de tous les examens du CSARS, de 1985 à 2019, ce qui représente plus de 270 rapports⁹¹.
- 168.** Pour compléter cette initiative, l'OSSNR souhaite également caviarder et publier de façon proactive nos futurs rapports à mesure qu'ils sont approuvés et traduits tout au long de l'année, plutôt que d'attendre la publication de notre rapport annuel pour divulguer nos constatations et nos recommandations. Cela vise à améliorer le caractère opportun et la pertinence du travail de l'OSSNR dans le discours public sur les questions de sécurité nationale et de renseignement. Cela signifie également que l'organisation pourra consacrer plus de temps et d'espace dans nos futurs rapports annuels à la présentation et à l'analyse des tendances horizontales ou thématiques, plutôt que des examens ou des questions individuels (ou verticaux).
- 169.** L'OSSNR travaille avec les ministères et organismes pour veiller à ce que cette nouvelle approche soit mise en œuvre afin que les renseignements essentiels en matière de sécurité nationale et de renseignement soient protégés, et que le public obtienne le plus de renseignements possible sur les résultats de nos examens. Les ministres concernés auront l'occasion, au cas par cas, de soulever des préoccupations au sujet de la publication de rapports précis.
- 170.** Pour rendre plus efficaces les efforts de caviardage et diffuser les rapports en temps opportun, l'OSSNR a accepté d'adopter le principe de «rédaction pour diffusion». Cette méthode comprend la rédaction, dans la mesure du possible, à un niveau non classifié, y compris des sommaires non classifiés; l'identification claire dans un rapport des parties qui contiennent des renseignements classifiés; et l'exclusion, dans la mesure du possible, des renseignements classifiés du corps du rapport, pour les inclure plutôt dans des notes en bas de page ou des annexes.

Conclusion

- 171.** Nous sommes très fiers des réalisations de l'OSSNR au cours de nos cinq premiers mois d'activité. Notre programme est ambitieux pour l'année à venir, malgré les contraintes imposées par la pandémie. Nous avons mis en place un plan d'examen qui couvre plusieurs questions au cours de la prochaine année et qui fera intervenir de nombreux ministères et organismes. Nous révisons actuellement en profondeur notre processus d'enquête sur les plaintes, dans le but de le rendre plus accessible à tous. Nous développerons également notre infrastructure organisationnelle pour faciliter notre croissance au cours des années à venir, notamment grâce à l'acquisition de locaux à bureaux supplémentaires et à l'embauche de nouveaux employés talentueux.
- 172.** Nous nous réjouissons à l'idée d'approfondir nos relations avec d'autres organismes d'examen et de surveillance au Canada et à l'étranger, ainsi qu'avec divers groupes d'intervenants, afin de s'assurer que notre travail est aussi efficace et significatif que possible. À ce sujet, nous espérons que ce rapport sera utile. Tous les lecteurs sont invités à transmettre leurs réflexions sur le format, le contenu et tout aspect à améliorer dans la prochaine version⁹².
- 173.** Nous sommes très reconnaissants envers notre personnel qui continue à obtenir de bons résultats malgré les défis que pose la pandémie. C'est avec enthousiasme que nous relèverons les nombreux défis et saisirons les nombreuses occasions qui nous attendent au cours de l'année à venir.

Annexe A:

Résumés des examens de l'OSSNR terminés pendant la période de rapport

EXAMEN DE L'UTILISATION PAR LE SCRS D'UNE TECHNOLOGIE DE GÉOLOCALISATION

1. Le présent examen a pour toile de fond de récentes décisions de la Cour fédérale – plus particulièrement la décision rendue en septembre 2017 sur l'identité internationale d'abonné mobile (IMSI) – qui ont une incidence sur la collecte, l'utilisation et la conservation de données par le Service canadien du renseignement de sécurité (SCRS), dont des données de géolocalisation. Dans sa décision, la Cour fédérale a conclu que, bien que le SCRS soit autorisé en vertu de l'article 12 à obtenir des renseignements de géolocalisation pour lesquels il existe une faible attente en matière de protection de la vie privée, toute activité qui dépasse ce cadre, telle que la géolocalisation d'une personne, nécessite un mandat.
2. Les activités de collecte et d'exploitation de données du SCRS revêtent un intérêt constant pour l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). Il s'agit de la première fois où l'OSSNR a expressément examiné la collecte par le SCRS de données de géolocalisation, un type particulier de renseignements numériques pouvant servir à géolocaliser une personne.
3. L'objectif principal du présent examen consistait à évaluer si la collecte de renseignements de géolocalisation par le SCRS était conforme à la *Charte canadienne des droits et libertés* (la Charte) et à la Loi sur le SCRS, ainsi qu'aux instructions du ministre et à la politique opérationnelle. Il s'agissait en l'occurrence d'établir si l'utilisation des données pour recueillir des renseignements sur l'emplacement d'une personne constituait une perquisition au sens de l'article 8 de la Charte, de sorte qu'un mandat soit requis. Aux fins de cette évaluation, une étude de cas approfondie portant sur une forme particulière de renseignements de géolocalisation a été réalisée.
4. Par ailleurs, l'examen a été l'occasion de souligner de façon plus générale que, dans ce contexte, un soutien juridique continu aux activités d'exploitation de données du SCRS est essentiel pour que l'organisme puisse fonctionner à un niveau de risque acceptable, et qu'on s'attend à ce que le SCRS et le ministère de la Justice fassent preuve de leadership institutionnel à cet égard.

Constatations et recommandations

Le SCRS était susceptible d'avoir contrevenu à l'article 8 de la Charte

5. L'examen a révélé que le SCRS était susceptible d'avoir contrevenu à l'article 8 de la Charte pendant la période d'essai au cours de laquelle il a utilisé les données sans mandat. L'OSSNR a conclu que, dans la plupart des cas, le SCRS aura besoin d'un mandat pour recueillir les renseignements sur la localisation d'une personne; sinon, il y aura un risque de violer l'article 8 de la Charte, qui protège contre les fouilles, les perquisitions ou les saisies abusives.

Recommandation : Que le SCRS passe en revue son utilisation des données de géolocalisation qu'il a recueillies et qu'il établisse lesquels des rapports opérationnels issus de l'utilisation de ces données contreviennent à l'article 8 de la Charte. Ces rapports opérationnels et/ou tout document lié à ces résultats devraient être purgés de ses systèmes.

Le SCRS a fait fi de plusieurs indicateurs selon lesquels l'utilisation de ces données pourrait soulever des questions d'ordre juridique.

6. L'examen a révélé que le SCRS a fait fi de plusieurs indicateurs selon lesquels l'utilisation de ces données pourrait soulever des questions d'ordre juridique. Il y a notamment eu dès le départ des discussions internes au cours desquelles des préoccupations liées aux risques juridiques ont été soulevées. De plus, avant même que l'essai ne débute, il y avait en l'occurrence des indications quant à la nécessité de faire preuve de prudence à l'égard des données, dont la décision de la Cour fédérale sur l'IMSI, selon laquelle la géolocalisation d'une personne nécessite un mandat.
7. Il a été avancé qu'il n'aurait pas été possible de procéder à une évaluation approfondie des données avant la période d'essai, au motif qu'une évaluation des risques n'est pas possible à moins d'une pleine utilisation des données. L'OSSNR accepte en principe qu'il existe des situations où il serait difficile d'apprécier la nature des risques juridiques avant que les données ne soient accessibles au SCRS et pleinement évaluées. Malgré les difficultés, il incombe au SCRS d'atténuer tous les risques, y compris les risques juridiques, dans toute la mesure du possible.

Recommandation : Que soit élaborée une politique ou que soient modifiées les politiques en vigueur, selon le cas, afin qu'une évaluation documentée des risques, y compris des risques juridiques, soit exigée dans des situations comme celle-ci où des informations recueillies au moyen de technologies nouvelles et émergentes peuvent contenir des renseignements pour lesquels il peut exister une attente raisonnable en matière de protection de la vie privée. Un centre de décision à l'égard de ce type de collecte devrait être clairement établi.

Il n'existait aucun centre de décision clairement responsable de l'utilisation des données

8. Dans le cadre de l'examen, il s'agissait notamment d'établir si le SCRS disposait de mesures de protection suffisantes sous forme de procédures et de politiques

officielles permettant de veiller à ce que l'organisme puisse respecter ses obligations juridiques dans un contexte caractérisé par l'évolution rapide de la technologie et la fluidité correspondante de l'environnement juridique.

9. L'examen a révélé qu'il n'existait aucun centre de décision clairement responsable de l'utilisation des données. C'est ce qu'a permis de corroborer une analyse des politiques et des procédures du SCRS alors en vigueur qui ont guidé la décision d'autoriser l'utilisation initiale des données pour une période d'essai. L'examen a fait ressortir trois unités distinctes qui ont participé à l'acquisition, à l'évaluation et à l'approbation des données pour la période d'essai. En fin de compte, l'examen n'a toutefois pas permis de déterminer laquelle des trois unités aurait dû être responsable de l'évaluation de ce type de données.

Il n'y avait aucune politique ni procédure entourant l'évaluation et le traitement des technologies de collecte nouvelles et émergentes

10. Dans le cadre de l'examen, il s'agissait aussi d'établir s'il existait des politiques ou des procédures relatives à ce type de collecte au SCRS. L'examen a révélé qu'il n'y avait aucune politique ni procédure entourant l'évaluation et le traitement des technologies de collecte nouvelles et émergentes et exigeant une évaluation officielle des risques juridiques. L'OSSNR a également été informé qu'il n'y avait pas de processus officiel d'évaluation des risques, y compris des risques juridiques, dans des cas comme celui-ci, étant donné que les données étaient considérées comme des données de « sources ouvertes ». Il s'agit d'une possible lacune du processus du SCRS puisque les instructions du ministre exigent que les risques posés par les activités opérationnelles soient évalués en fonction de quatre piliers (risques opérationnels, risques politiques, risques liés à la politique étrangère et risques juridiques).

Le document d'approbation n'a pas été conservé comme il se doit

11. Enfin, l'examen a permis de constater que le document d'approbation concernant l'essai pilote des données consistait en un courriel et que ce courriel ne faisait pas partie du dossier officiel, comme cela aurait dû être le cas.

EXAMEN DU DOSSIER DES INCIDENTS LIÉS À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DU CST

1. L'OSSNR a réalisé son tout premier examen du CST depuis l'entrée en vigueur de la Loi sur l'OSSNR.
2. L'examen de l'OSSNR a porté sur le Dossier des incidents liés à la protection des renseignements personnels du CST, qui rassemble les incidents de ce type découverts par le CST. 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.

3. Les objectifs de l'examen étaient d'examiner et d'évaluer les politiques et les pratiques du CST en réponse aux incidents liés à la protection des renseignements personnels. Les chercheurs de l'OSSNR ont examiné un échantillon de 72 incidents sur un total de 123 incidents signalés dans le Dossier des incidents liés à la protection des renseignements personnels pour la période du 1^{er} juillet 2018 au 31 juillet 2019.

Constatations et recommandations

4. En ce qui concerne les incidents liés à la protection des renseignements personnels examinés, l'OSSNR estime que le CST a pris des mesures de conformité en temps utile et conformément à sa politique. Toutefois, l'OSSNR a formulé cinq constatations supplémentaires et les recommandations correspondantes afin d'améliorer la documentation, l'évaluation et l'atténuation des incidents liés à la protection des renseignements personnels au sein du CST.

Le Dossier des incidents liés à la protection des renseignements personnels en tant qu'outil pour prévenir les incidents systémiques et déterminer les points faibles

5. Bien que le CST ait adopté une approche par étapes pour renforcer les mesures de protection des renseignements personnels, le CST n'utilise pas le Dossier des incidents liés à la protection des renseignements personnels, ou tout autre registre similaire d'incidents liés à la protection des renseignements personnels, pour empêcher que des incidents systémiques ne se reproduisent, ou pour cerner toute lacune dans les politiques ou les pratiques existantes qui pourrait réduire la fréquence des incidents liés à la protection des renseignements personnels.

Recommandation : Le CST devrait examiner la totalité des incidents liés à la protection des renseignements personnels en vue de déterminer les tendances systémiques ou les lacunes des politiques ou des pratiques existantes susceptibles de réduire les incidents liés à la protection des renseignements personnels.

Incohérence dans l'atténuation, le signalement et la documentation des incidents liés à la protection des renseignements personnels

6. Après examen du Dossier des incidents liés à la protection des renseignements personnels et de toutes les pièces justificatives, l'OSSNR a constaté que l'atténuation, la documentation et le signalement des incidents liés à la protection des renseignements personnels étaient incohérents et ne répondaient pas toujours aux objectifs fixés dans la politique interne du CST.

Recommandation : Le CST devrait adopter une approche cohérente pour évaluer et documenter tous les incidents liés à la protection des renseignements personnels.

Capacité à atténuer davantage les préjudices potentiels qu'entraînent les incidents liés à la protection des renseignements personnels

7. Les mesures d'atténuation de nombreux incidents liés à la protection des renseignements personnels visent à mettre un terme à la persistance des préjudices potentiels après la découverte d'un incident. Toutefois, pour certains types d'incidents, l'OSSNR estime que le CST est en mesure de faire davantage pour atténuer les préjudices potentiels découlant des incidents.

Recommandation : Le CST devrait examiner davantage les préjudices potentiels résultant d'incidents liés à la protection des renseignements personnels afin de déterminer si des mesures d'atténuation supplémentaires sont justifiées.

Évaluation limitée des incidents pour déterminer s'ils constituent une atteinte substantielle à la vie privée

8. Conformément à la directive du Secrétariat du Conseil du Trésor du Canada sur les pratiques en matière de protection de la vie privée, le CST doit signaler les cas d'atteintes substantielles à la vie privée. Toutefois, l'évaluation des incidents par le CST pour déterminer s'ils constituent une atteinte substantielle à la vie privée est limitée.

Recommandation : Le CST devrait normaliser sa politique pour déterminer si les incidents constituent une atteinte substantielle à la vie privée.

Une méthode d'atténuation inappropriée

9. L'OSSNR a constaté qu'une politique du CST en réponse à certains incidents est une méthode d'atténuation inappropriée. Cette méthode ne semblait pas répondre aux critères juridiques et d'autorisation ministérielle et pourrait porter atteinte à l'article 8 de la Charte.
10. Le CST a réexaminé l'utilisation de la méthode d'atténuation en question à la suite des préoccupations exprimées par l'OSSNR au cours de l'examen, ce qui a conduit le CST à résilier cette pratique en novembre 2019.

Recommandation : Le CST devrait abolir cette politique ou obtenir un avis juridique sur la légalité de cette pratique.

EXAMEN DU PARTAGE D'INFORMATION PAR LE SCRS

1. Dans le but de répondre aux exigences du mandat d'enquête des menaces à la sécurité nationale du Canada, le SCRS se doit d'échanger des informations avec des organismes étrangers. Toutefois, il existe des risques associés à l'échange d'informations avec ces organismes, ce qui signifie que le SCRS a dû développer diverses mesures afin d'atténuer les risques. Par exemple, l'échange d'informations est assujéti à des mises en garde ainsi qu'à des

demandes de garantie, par écrit ou de vive voix, qui ont pour effet de placer des restrictions sur la façon dont l'information du SCRS peut être utilisée ou partagée.

2. Le but de l'examen de l'OSSNR consistait à déterminer si, dans les trois cas à l'étude, le SCRS avait mis des garanties suffisantes dans le but de s'assurer que, lors de l'échange d'informations, il est apte à se conformer à ses obligations légales et aux instructions ministérielles; et, dans la mesure du possible, il est apte à atténuer les risques de l'échange d'informations avec des organismes étrangers.
3. Trois études de cas ont été examinées en se basant sur les décisions prises par le Comité d'évaluation des échanges d'informations (CEEI ou Comité) en 2018-2019. Dans les trois cas, l'examen a scruté le cycle de l'échange d'informations, c'est-à-dire de la création du protocole d'entente jusqu'au risque potentiel d'échanges d'informations avec un partenaire étranger.

Constatations et recommandations

Implication du Directeur dans la prise de décision

4. Lors de la prise de décision au sein du CEEI, le SCRS n'était pas dans l'obligation de se fier uniquement à l'avis du Service juridique dans son processus de décision. Une décision était adoptée si elle recueillait la majorité des voix, peu importe l'avis du Service juridique.
5. L'évaluation des mesures atténuantes et leur impact n'est pas seulement une question de droit, elle est aussi soumise aux faits présentés. Le SCRS demeure responsable des décisions prises au sein du CEEI. Néanmoins, le Service juridique possède une perspective unique en ce qui a trait d'informer le CEEI des principes, seuils et standards juridiques et d'exprimer des avis sur la question de savoir si le SCRS a agit à l'intérieur des règles et instruments légaux permis.
6. L'OSSNR est d'avis que le directeur du SCRS doit être avisé lorsque le représentant du Service juridique ne croit pas que l'action envisagée est permise par la loi. L'examen a constaté que quelques cas considérés par le CEEI auraient dû être transférés au directeur afin que ce dernier, et non le Comité, soit responsable de la décision finale en conformité avec l'IM : Éviter la complicité dans les cas de mauvais traitements par des entités étrangères.

Recommandation: Lorsque le Service juridique considère que le risque sérieux de mauvais traitements ne peut pas être atténué, le cas soit automatiquement transféré au directeur du SCRS pour la prise de décision.

Obtention d'un avis juridique écrit pour l'usage de nouvelles mesures

7. Lors de l'examen, le SCRS étudiait des nouvelles mesures pour atténuer le risque dans le but de permettre l'échange d'information lorsqu'il existe des préoccupations en matière de droits de la personne au sein de l'organisme étranger. Dans quelque cas à l'étude, ces mesures ont été proposées afin

d'atténuer le risque sérieux de mauvais traitements. Dans ces cas, le CEEI n'a obtenu qu'un avis juridique de vive voix.

8. L'OSSNR reconnaît que le temps alloué pour préparer un avis juridique avant une réunion ne permettait pas toujours d'obtenir un avis formel écrit. Néanmoins, le fonctionnement des mesures innovatrices devrait être compris par les membres du Comité avant que ceux-ci soient satisfaits que les mesures choisies constituent une mesure atténuante suffisante. Un avis formel permettrait au SCRS de déterminer la possible validité de ces nouvelles mesures comme mesures atténuantes.

Recommandation: Le SCRS devrait demander un avis juridique formel afin de déterminer si ces nouvelles mesures pourraient être considérées comme des mesures atténuantes à l'avenir lors de l'échange d'informations avec un organisme étranger.

EXAMEN DES CADRES MINISTÉRIELS POUR ÉVITER LA COMPLICITÉ DE MAUVAIS TRAITEMENTS PAR DES ENTITÉS ÉTRANGÈRES

1. En vertu de sa loi habilitante, l'OSSNR est maintenant tenu d'examiner dans quelle mesure les ministères ont mis en œuvre les instructions de la gouverneure en conseil relativement à l'échange d'information avec des partenaires étrangers sous le régime de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*. À ce jour, la gouverneure en conseil a émis ces instructions à 12 ministères, dont plusieurs n'avaient jamais reçu auparavant de directives formelles à ce sujet.
2. En vue d'assumer cette nouvelle responsabilité, nous avons lancé notre premier examen interorganisationnel, qui visait à évaluer comment six organismes et ministères — l'ASFC, le CST, le SCRS, le MDN, AMC et la GRC — mettaient en œuvre l'instruction du ministre de 2017 intitulée *Éviter la complicité dans les cas de mauvais traitements par des entités étrangères*, laquelle a servi de base pour l'élaboration des instructions données en application de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*. Cet examen visait aussi à fournir une feuille de route aux ministères qui, conformément à cette loi, ont reçu de telles instructions pour la première fois en 2019.
3. L'OSSNR a constaté d'importants écarts entre les six ministères et organismes pour ce qui est de la mesure dans laquelle ils ont réussi à mettre en œuvre la directive ministérielle de 2017. Certains, comme le CST, ont élaboré et diffusé des ensembles complets de politiques pour encadrer leurs activités d'échange d'information avec des partenaires étrangers, alors que d'autres peinent à mettre la directive en application. De plus, certains ont de la difficulté à mettre en place des mécanismes décisionnels indépendants des services opérationnels de première ligne lorsqu'il existe un risque de mauvais traitements. Un des principaux éléments mis en lumière par l'examen de l'OSSNR était l'application irrégulière du critère relatif au « risque sérieux » par l'ensemble des ministères et organismes. Cet aspect sera examiné dans l'avenir.

Examen relatif à la Direction de la sécurité interne du SCRS

1. La Direction de la sécurité interne du SCRS est chargée d'assurer la protection des personnes, des informations et d'autres biens en réalisant des enquêtes de sécurité sur le personnel, et en menant des enquêtes sur des employés ou des incidents de sécurité. L'examen de l'OSSNR donne suite à un examen du CSARS réalisé en 2013 au sujet de la Direction de la sécurité interne du SCRS, qui a permis de relever de graves lacunes quant à la manipulation de dossiers sensibles et de listes d'accès, ainsi qu'aux pratiques en matière d'enquêtes internes et à la gestion de ces dernières par le SCRS.
2. Les objectifs de l'examen de l'OSSNR visaient à évaluer les progrès réalisés par le SCRS en ce qui a trait à la mise en œuvre des recommandations de 2013, ainsi qu'évaluer la pertinence, la conformité et l'efficacité des processus en matière de sécurité interne servant à examiner les incidents, les infractions et les manquements, réels ou potentiels, relatifs à la sécurité.
3. L'OSSNR a conclu que, même si des améliorations importantes ont été apportées relativement à la sécurité interne au SCRS depuis l'examen de 2013, d'autres améliorations aux politiques en matière de sécurité interne pourraient renforcer l'uniformité dans la prise de décisions concernant les dossiers de sécurité du personnel et les enquêtes de sécurité sur le personnel, et pourraient accroître l'équité procédurale de ces processus en général.

Conclusions et recommandations

Les enquêtes internes du SCRS sont gérées de façon professionnelle et de manière à réduire au minimum les biais et la subjectivité, dans la mesure du possible.

4. L'examen réalisé par le CSARS en 2013 sur la Direction de la sécurité interne du SCRS a suscité des controverses, non pas en raison de sa nature, mais plutôt en raison de l'ensemble des répercussions découlant des conclusions : c'est-à-dire que les activités liées à la sécurité interne au sein du SCRS comportaient un certain nombre de graves lacunes. Les éléments probants évalués dans le cadre du présent examen ont permis à l'OSSNR d'aboutir à une nouvelle conclusion. Plus précisément, le SCRS a ajouté des activités à ses programmes de mentorat et de formation; de manière générale, les politiques ont été améliorées; la prise de décisions relative aux enquêtes a été documentée dans les dossiers appropriés; et le SCRS a pris des mesures constructives en vue de réduire les biais et la subjectivité en créant des outils novateurs et en consultant des intervenants pertinents à l'extérieur de la Direction de la sécurité interne pour contribuer à l'élaboration de stratégies pratiques d'atténuation des risques.

Le SCRS a mené les activités examinées conformément à ses obligations juridiques énoncées dans la Loi sur le SCRS. Toutefois, le SCRS n'a pas établi une gouvernance suffisamment détaillée quant au moment et à la façon de signaler une activité criminelle soupçonnée, découverte dans le cadre d'une enquête interne ou d'une vérification de sécurité.

5. Lorsque la Direction de la sécurité interne découvre une activité criminelle soupçonnée, elle doit souvent en informer les forces de l'ordre rapidement. Toutefois, ce faire peut également présenter un risque. Plusieurs questions importantes doivent être prises en compte au moment de déterminer si (et comment) on communique de l'information à la police. Une fois les forces de l'ordre impliquées, la relation entre l'employé et le SCRS est touchée de manière irrévocable. En outre, les questions peuvent couvrir : la protection des renseignements personnels, des obligations à l'égard des relations de travail, l'autorité sous laquelle la communication a lieu, la méthode de communication, l'autorité compétente pour recevoir l'information, si la personne doit être informée de la communication ou non, ainsi que tout préjudice possible à l'employé, au SCRS, à d'autres employés, au gouvernement et à l'intérêt public.

Recommandation : Que le SCRS élabore une politique interne, en collaboration avec le Secrétariat du Conseil du Trésor (SCT), présentant des paramètres relatifs à la communication en temps opportun aux forces de l'ordre d'information obtenue dans le cadre d'une vérification, d'une demande de renseignements ou d'une enquête de sécurité réalisée par la Direction de la sécurité interne.

L'Unité chargée de la méthode et de l'utilisation du polygraphe fait face à un certain nombre de problèmes interdépendants liés à la gouvernance, notamment:

- *des politiques et procédures informelles;*
 - *une absence de limites claires entre le polygraphe et l'analyse médicale;*
 - *une surveillance limitée du programme du polygraphe;*
 - *aucune évaluation des facteurs relatifs à la vie privée) au sujet du processus relatif au polygraphe;*
 - *aucun mécanisme de rétroaction des employés propre au polygraphe.*
6. L'examen a permis de constater que l'ensemble de politiques de la Direction de la sécurité interne n'est pas suffisamment détaillé pour répondre aux questions concernant la normalisation des tests polygraphiques, la formation des examinateurs, les mesures de contrôle de la qualité et les seuils de définition. Le SCRS n'était pas en mesure de justifier les mérites des examinateurs, qui ne sont pas des médecins, de poser des questions de nature médicale aux personnes qu'ils examinaient. En outre, les mesures de surveillance du programme du polygraphe sont limitées.
 7. Étant donné que le polygraphe est un outil invasif, les employés doivent consentir à passer le test polygraphique s'ils désirent obtenir ou renouveler leur cote de sécurité approfondie de niveau Très secret. L'OSSNR s'est donc informé au sujet des évaluations des facteurs relatifs à la vie privée (EFVP) réalisées pour le programme du polygraphe du SCRS. Selon le SCT, une EFVP doit être effectuée pour un programme ou une activité lorsque l'on utilise, ou que l'on prévoit utiliser, des renseignements personnels dans le cadre d'un processus décisionnel qui touche directement une personne. En dépit de cette exigence énoncée dans les politiques, aucune EFVP n'a été réalisée pour le processus du polygraphe du SCRS. À la suite de l'examen, le SCRS a signalé son intention d'effectuer une EFVP pour le programme.

8. En l'absence d'une EFVP, l'OSSNR s'est informé au sujet d'autres mécanismes ou processus permettant d'évaluer les expériences des employés avec le polygraphe. Les employés du SCRS comprennent la nécessité de subir un test polygraphique et s'attendent à ce que l'examen se déroule de manière professionnelle. Malgré cette attente raisonnable, aucun sondage auprès des employés ne comporte de question sur les activités liées au polygraphe. Par contre, les personnes qui subissent un test polygraphique peuvent soulever des questions auprès des gestionnaires responsables du polygraphe. Le directeur du SCRS a reconnu publiquement que le harcèlement, l'intimidation et les représailles sont des questions qui doivent être abordées dans l'ensemble du SCRS. L'OSSNR n'a observé aucun signe de questions systématiques semblables liées à l'administration du polygraphe.

Recommandation : Que le SCRS renforce la gouvernance interne des activités liées au polygraphe, notamment en modifiant la méthode utilisée pour réaliser des tests polygraphiques, au besoin.

Selon l'information examinée et les entrevues réalisées au sujet de l'utilisation du polygraphe par le SCRS, l'OSSNR a constaté que :

- *le polygraphe est un élément essentiel des processus d'enquête et de renouvellement aux cinq ans du SCRS;*
 - *les résultats ou les conséquences des tests polygraphiques subis par des candidats externes diffèrent de ceux subis par des employés du SCRS;*
 - *le SCRS manque de clarté de politique pour les cas où les employés échouent des tests de polygraphe*
-
9. Par le passé, le SCRS a souligné ne pas refuser des cotes de sécurité ou des emplois en se fondant seulement sur un test polygraphique; des preuves provenant de d'autres sources à l'appui ont toujours été requises. Le CSARS critiquait l'utilisation que faisait le SCRS du polygraphe, et a mis en doute l'exactitude du test polygraphique et la mesure dans laquelle les personnes le passaient sur une base volontaire. Dans le cadre du présent examen, on a soulevé des différences entre les conséquences découlant des tests polygraphiques entre les candidats externes et les employés du SCRS, malgré l'obtention de résultats semblables au test.
 10. Essentiellement, la réussite du test polygraphique est un facteur déterminant pour l'octroi par le SCRS d'une cote de sécurité approfondie de niveau Très secret aux candidats externes. La même norme ne s'appliquait pas aux employés. [Texte supprimé – Au 20 novembre 2020, l'OSSNR et le SCRS ne pouvaient s'entendre sur la manière dont tous les faits de cet examen devraient être présentés dans un document public non classifié]. Les politiques du SCRS ne comportent aucune directive claire à savoir comment ce problème doit être réglé.
 11. En plus des défis susmentionnés, l'examen a permis de constater qu'un test polygraphique peut avoir des répercussions négatives marquées sur la santé mentale d'un employé si on ne lui fait pas passer de manière appropriée. Les employés qui ont parlé à l'OSSNR sous le couvert de l'anonymat ont décrit les répercussions négatives qu'ont eues leurs résultats

défavorables au test polygraphique sur leurs vies. Ces répercussions étaient particulièrement évidentes lors de l'examen des documents, notamment de la correspondance après un examen entre les employés et l'unité chargée de faire passer les tests polygraphique.

Recommandation : Que le SCRS mette à jour les politiques et les procédures applicables sur l'utilisation du polygraphe pour tenir compte des implications relatives à l'équité procédurale et à la sécurité découlant d'un échec au test polygraphique.

L'information examinée et les entrevues réalisées ont permis à l'OSSNR de constater que la Direction de la sécurité interne respecte la Norme sur le filtrage de sécurité ainsi que ses propres politiques dans le cadre de la gestion de cas complexes découlant du processus d'évaluation de sécurité. Par contre, l'OSSNR estime que le processus de prise de décisions connexe pourrait être renforcé par l'amélioration de la gouvernance et par des politiques plus claires.

12. L'OSSNR estime que des normes équitables et uniformes pour l'interprétation d'activités criminelles, y compris les aveux d'activités criminelles mineures, permettraient de veiller à ce que le SCRS rende des jugements équitables compte tenu de la primauté de son rôle relativement aux évaluations de la sécurité pour le gouvernement du Canada. L'OSSNR souligne que la Direction de la sécurité interne assure un suivi de niveau global des décisions rendues et de leur justification, ce qui permettra d'améliorer la capacité des intervieweurs de la Direction de la sécurité interne de trouver des décisions antérieures pertinentes, de même que des considérations et des circonstances connexes. L'OSSNR appuie la décision de la Direction de la sécurité interne de renforcer cette responsabilité en créant un nouveau poste, et croit qu'il s'agit d'une étape importante pour améliorer la documentation et la définition des seuils pratiques.

Recommandation : Que la Direction de la sécurité interne harmonise davantage son ensemble de politiques générales aux critères d'évaluation relatifs aux renseignements défavorables énoncés dans la Norme sur le filtrage de sécurité, et qu'elle mette à jour son guide sur les questionnaires pour y intégrer des définitions claires et des indicateurs de risque.

Plusieurs documents et avis juridiques pertinents ont été reçus seulement après que l'examen ait été en grande partie rédigé et achevé, alors ils n'ont pas pu être intégrés et pris en compte en temps opportun dans le rapport final.

Puisqu'ils ont été fournis en retard, cinq avis juridiques pertinents en plus de deux autres documents juridiques pertinents ont été reçus après que l'ébauche du rapport ait été rédigée et distribuée pour examen interne. L'OSSNR a été en mesure d'apporter certaines modifications à l'ébauche concernant des questions précises afin de représenter adéquatement l'information récemment obtenue. Toutefois, ces avis juridiques étaient pertinents pour les questions abordées dans le rapport et il aurait été utile qu'ils soient entièrement pris en considération dans le cadre de l'examen. Toutefois, l'OSSNR souligne que l'accès à toutes les autres informations touchant l'examen a été fourni de manière efficace et efficiente, par voie électronique et sur papier.

Annexe B:

Résumés des examens non publiés du CSARS et du BCSEC jusqu'en juillet 2019

Examens du CSARS, avril 2018 à juillet 2019

Certificat 2018-07 remis par le CSARS

En mars 2019, le CSARS a terminé la certification du rapport annuel du directeur du SCRS au ministre de la Sécurité publique et de la Protection civile de 2017-2018.

Dans le processus de certification, le CSARS a examiné un certain nombre de sujets abordés dans le rapport, notamment les cibles du SCRS de moins de 18 ans; les cas d'échange d'information comprenant un risque considérable de mauvais traitement; un examen de la communication interne en matière de conformité du SCRS; et un aspect des activités du SCRS concernant des « institutions fondamentales canadiennes », ou IFC. Le SCRS définit les IFC comme étant les institutions politiques, gouvernementales, religieuses, les établissements postsecondaires et les organes médiatiques. Dans l'ensemble, le CSARS a constaté que ces activités respectaient la Loi sur le SCRS, les instructions du ministre et les politiques et procédures internes.

Il y avait toutefois eu une exception importante. Jusqu'en janvier 2019, le directeur du SCRS a approuvé certaines activités de sources humaines malgré le fait qu'on avait informé le SCRS qu'elles comportaient un « risque juridique élevé », c'est-à-dire qu'elles étaient fort probablement illicites. Par conséquent, le CSARS a conclu que « le SCRS a[vait] sciemment mené des activités de sources humaines sachant qu'elles contrevenaient à la Loi sur le SCRS et aux instructions du ministre, stipulant que la primauté du droit est respectée ». Par ailleurs, le CSARS a ajouté que l'importance ou l'aspect bénéfique des activités n'en atténuaient pas l'illicéité.

Depuis, l'OSSNR a publié une version caviardée du certificat, qui est accessible ici.
<https://nsira-ossnr.ca/wp-content/uploads/2020/09/2018-07-fra.pdf>

Examen des mesures de réduction de la menace du SCRS

Cet examen a été mené conformément à la Loi sur le SCRS, qui énonce que le CSARS doit examiner à chaque exercice « au moins un aspect de la prise, par le Service, de mesures pour réduire les menaces envers la sécurité du Canada ». Le CSARS a conclu que toutes les mesures de réduction de la menace examinées étaient conformes à

la Loi sur le SCRS, aux directives ministérielles ainsi qu'aux politiques et procédures applicables. Le CSARS a aussi examiné l'évaluation des activités de réduction de la menace – c'est-à-dire, la mesure du rendement. La mesure du rendement représente un défi pour tous les partenaires du Groupe des cinq dans le cadre des activités visant à perturber une menace. Le CSARS a conclu que le SCRS fait des efforts pour améliorer la mesure du rendement, mais il reste toutefois du travail à faire. Une attention particulière devra être portée à l'évaluation des résultats intermédiaires et stratégiques, pour éviter autant que possible toute subjectivité.

Examen de l'exécution de la collecte technique avec mandat du SCRS

Cet examen de base se penchait sur les pratiques du SCRS pour l'obtention de renseignements de tierces parties en soutien à sa collecte technique. Le CSARS a conclu que les modifications apportées au système de gouvernance de la conformité du SCRS ont amélioré en grande partie la gestion des risques de conformité dans le contexte d'opérations avec mandat. Le CSARS est satisfait des mesures prises par le SCRS dans les cas examinés pour gérer les risques identifiés par le procédé. Le CSARS estime aussi que le SCRS a pris des mesures pour gérer les risques et qu'il a signalé les incidents de non-conformité qui impliquaient des pouvoirs exécutés sous l'autorité d'un mandat, à la Cour fédérale, et dans certains cas, au ministre de la Sécurité publique et au CSARS.

Examen des activités du SCRS concernant les renseignements de base sur l'identité

Le SCRS définit les renseignements de base sur l'identité (RBI) comme étant les noms et les adresses – et, à l'occasion, d'autres identificateurs électroniques – qui se trouvent dans les dossiers des clients associés à des comptes de téléphone ou à d'autres comptes vendus par des fournisseurs de services de communication. L'accès aux RBI permet au SCRS d'identifier des personnes d'intérêt qui seraient autrement inconnues. Par exemple, le SCRS peut avoir en sa possession un numéro de téléphone associé à des activités susceptibles de constituer une menace. Il peut alors demander un mandat autorisant la collecte du nom et de l'adresse associés au compte auquel correspond le numéro de téléphone.

Les changements récents apportés au processus de collecte des RBI à la suite de décisions de la Cour fédérale ont rendu plus difficile la réalisation en temps voulu de ce processus pour le SCRS. Le CSARS a recommandé que, si des difficultés importantes persistent, le SCRS et ses partenaires chercheront des solutions pour résoudre ces défis. Les solutions doivent tenir compte des aspects relatifs à la protection de la vie privée et à la Charte des droits des RBI.

En temps normal, le SCRS ne connaît pas l'identité de la personne pour laquelle il demande des RBI. Il est donc inévitable que certaines des personnes dont l'identité est ainsi dévoilée se révèlent finalement n'être aucunement impliquées dans des activités représentant une menace. Malgré cela, le SCRS conserve les renseignements presque indéfiniment. Pourtant, la Loi sur le SCRS oblige le SCRS à recueillir et à conserver les renseignements uniquement dans la mesure où ils sont « strictement nécessaires ». Les RBI peuvent révéler des détails sur les activités d'une personne pour lesquels celle-ci s'attend raisonnablement à la confidentialité et que le SCRS n'aurait peut-être pas été autorisé à recueillir si l'identité de la personne avait été connue à l'avance. Le SCRS devrait alors être particulièrement prudent pour ce qui est de la conservation de ces renseignements.

Le SCRS n'a actuellement aucune politique écrite complète sur la collecte, le traitement, la conservation et l'élimination des RBI ni sur la gestion des risques inhérents au respect des mandats propres à ces renseignements. Cela augmente le risque que le personnel du SCRS enfreigne par inadvertance les politiques du SCRS ou même les conditions des mandats relatifs aux RBI. Le CSARS a recommandé que le SCRS procède en priorité à la rédaction d'un document complet sur les politiques et les procédures relatives à la collecte, au traitement, à la conservation et à l'élimination des RBI. Ce document devrait comprendre des procédures relatives à l'évaluation des RBI recueillis, à leur destruction, à leur classement ou à tout autre traitement spécial lorsqu'il s'avère peu probable qu'ils représentent une valeur ou une pertinence appréciables.

Examen de l'enquête du SCRS sur les activités influencées par l'étranger

Cet examen est une analyse de l'enquête sur les activités influencées par l'étranger d'un État étranger. Le CSARS a constaté que le SCRS était conscient des sensibilités politiques associées à certaines sources dans le cadre de cette enquête et a constaté que le SCRS respectait ses politiques internes. Le CSARS a recommandé que le SCRS consulte Sécurité publique Canada afin de clarifier les attentes quant au fait d'être mis au courant de certaines de ces sources. Le CSARS a également constaté que les conseils du SCRS sur les menaces que cet État étranger fait peser sur la sécurité du Canada étaient suffisants. Cependant, le CSARS a également recommandé que les conseils du SCRS sur les enquêtes de contre-espionnage soient suffisamment détaillés pour que le gouvernement soit pleinement conscient des défis opérationnels entourant l'enquête et de son incidence sur les conseils formulés.

Examen de l'engagement du SCRS auprès des services de renseignement étrangers présents au Canada

Cet examen a porté sur les relations du SCRS avec les services de renseignement étrangers et la façon dont le SCRS gère stratégiquement les activités des organismes étrangers au Canada ou avec les Canadiens, ainsi que les lois et les directives ministérielles connexes.

Le CSARS a constaté que les changements apportés graduellement aux instructions du ministre et aux politiques du SCRS ont, ensemble, réduit l'obligation d'informer le ministre des activités d'États étrangers au Canada. Le CSARS a constaté que l'ensemble de politiques utilisé pour guider les interactions du SCRS avec les organismes étrangers opérant au Canada ou avec des Canadiens à l'étranger n'avait pas été appliqué de manière uniforme et était parfois contradictoire. De plus, le CSARS a constaté qu'il n'y a pas de vérification systématique de cet ensemble de politiques pour s'assurer que les conditions sont respectées. Le CSARS a recommandé que le SCRS crée un processus systématique de vérification pour aider à gérer ce processus. Le CSARS a également constaté que le SCRS ne satisfaisait pas aux exigences du paragraphe 7(1) de la Loi sur le SCRS. Le CSARS a recommandé que le SCRS consulte le ministère de la Justice Canada au sujet de l'interprétation du paragraphe 7(1) de la Loi sur le SCRS et, sur cette base, qu'il reprenne les consultations avec Sécurité publique Canada exigées par la loi.

Examen d'un poste à l'étranger (1)

Le CSARS a procédé à l'examen d'un poste à l'étranger du SCRS. Le CSARS a constaté que la collecte de renseignement au poste était conforme aux directives ministérielles et que la présence du SCRS a amélioré la compréhension du Canada à l'égard des menaces à la sécurité nationale dans la région. Deux lacunes de procédure ont été relevées et considérées comme préoccupantes par le CSARS. La première concerne des ententes du SCRS avec des services étrangers pour lesquelles le poste n'avait pas demandé de garanties nouvelles ou renouvelées aux entités étrangères depuis 2010. Le CSARS s'attend à ce que le SCRS place en priorité la demande de garanties et le renouvellement des garanties antérieures en ce qui a trait au respect des droits de la personne lors de l'échange de renseignements. La seconde lacune est un processus incohérent d'évaluation des risques qui a eu pour conséquence que les décideurs n'ont pas pris conscience de toute l'ampleur des risques d'une certaine opération. Selon le CSARS, un point d'approbation unique pour les opérations permettra de consigner plus clairement l'évaluation complète des risques.

Examen d'un poste à l'étranger (2)

Le CSARS a examiné les activités d'un poste du SCRS à l'étranger. Il n'a relevé aucun problème quant à la nature et à l'étendue des renseignements communiqués à des organismes étrangers au cours de la période d'examen. Cependant, le CSARS recommande que le SCRS renforce les directives qu'il donne aux postes étrangers à la suite d'événements susceptibles d'affecter les partenariats étrangers. De plus, le CSARS a constaté qu'il n'existe ni politique ni centre décisionnel décrivant en détail des lignes directrices adéquates pour un dispositif de protection assurant la sécurité des employés dans les zones dangereuses. Le CSARS recommande que le SCRS crée une politique ou un centre décisionnel sur la gouvernance de tels dispositifs de protection, qui pourrait être intégré dans un cadre plus vaste d'équipement de protection individuelle.

Examen du programme de collecte de renseignements sur les États étrangers en vertu de l'article 16

Cet examen a porté sur la façon dont le SCRS a géré la demande accrue pour un type particulier d'opération en vertu de l'article 16. Le CSARS a relevé de nombreux problèmes administratifs qui peuvent survenir au cours des enquêtes menées en vertu de l'article 16, comme des retards causés par des partenaires nationaux et un manque de ressources du SCRS. Malgré ces problèmes, le CSARS a constaté que ce type de collecte, lorsqu'il est exécuté efficacement, est un outil utile et important pour le ministre des Affaires étrangères et le gouvernement du Canada. Le CSARS a également constaté que le SCRS ne dispose pas d'un ensemble de politiques régissant le programme relatif à l'article 16 et qu'il s'appuie sur une directive de 2014 d'un directeur adjoint, Opérations. Le CSARS a recommandé que le SCRS adopte et publie un ensemble de politiques ayant pour objet précis de détailler les exigences et les attentes du programme relatif à l'article 16.

Examens du BCCST, mars à juillet 2019

Examen d'un programme de collecte de renseignements électromagnétiques étrangers réalisé par le CST en vertu d'une autorisation et d'une instruction ministérielles

Cet examen a porté sur les activités qu'a réalisées le CST dans le cadre d'un programme particulier de collecte de renseignements étrangers de 2008 à 2015. Pour diverses raisons, dont le fait que l'examen a porté sur une période de huit ans, le roulement du personnel et les priorités concurrentes du Bureau du commissaire du CST, cet examen n'a pu être achevé avant juillet 2019. Au total, six recommandations ont été formulées, mais trois de celles-ci ne s'appliquent plus depuis l'entrée en vigueur de la Loi sur le CST. Le BCCST a conclu que bien que le CST s'est conformé à la loi, il n'a pas respecté deux attentes d'une directive ministérielle concernant le programme de collecte. Toutefois, depuis l'entrée en vigueur de la Loi sur le CST, cette directive ministérielle ne s'applique plus.

Examen d'un incident relatif à la protection des renseignements personnels concernant une activité d'analyse de métadonnées réalisée par le CST

Cet examen a porté sur un incident particulier relatif à la protection des renseignements personnels concernant une activité d'analyse des métadonnées du dossier de

2016-2017 sur ces incidents. L'examen, qui a été achevé le 21 juin 2019, concluait que le CST s'était conformé à la loi. Le BCCST a recommandé que le CST veille à ce que les rapports d'incidents relatifs à la protection des renseignements personnels contiennent toute l'information pertinente connue afin que chaque incident soit décrit et documenté de manière exhaustive. Le reste du rapport sur les dossiers d'incidents relatifs à la protection des renseignements personnels de 2016-2017 a été inclus dans le rapport annuel du BCCST au ministre de 2017 2018.

Annex C:

Résumés des enquêtes sur les plaintes

ALLÉGATIONS CONCERNANT UNE ÉVALUATION DE SÉCURITÉ LIÉE À UNE DEMANDE DE RÉSIDENCE PERMANENTE : PLAINTÉ EN VERTU DE L'ARTICLE 41 DE LA LOI SUR LE SCRS

Le Comité de surveillance des activités de renseignement de sécurité (CSARS) a enquêté sur une plainte en vertu de l'article 41 de la Loi sur le SCRS dans laquelle le plaignant alléguait que le Service canadien du renseignement de sécurité (SCRS) avait présenté de fausses allégations à un ministère quant à l'évaluation de sécurité relative à une demande de résidence permanente. Le plaignant alléguait également qu'il y avait eu retard indu dans le traitement de la demande de résidence permanente. Dans le processus de filtrage de sécurité lié à une demande de résidence permanente, le SCRS peut mener une entrevue de filtrage de sécurité. La question du mandat du SCRS et du filtrage de sécurité en immigration s'est posée quant à la prestation de conseils au gouvernement fédéral sur les questions d'immigration, en particulier lorsque le SCRS conseille les ministères concernés, soit Citoyenneté et Immigration Canada (CIC) et l'Agence des services frontaliers du Canada (ASFC).

Conformément aux articles 14 et 15 de la Loi sur le SCRS, le SCRS effectue des filtrages de sécurité en matière d'immigration et de citoyenneté. Le SCRS effectue ensuite des vérifications de filtrage. S'il n'y a pas d'information défavorable, le SCRS fournit sa réponse au ministère qui a fait la demande. Si le processus de filtrage révèle que des renseignements défavorables soulèvent certaines préoccupations, le SCRS rédige une note qu'il envoie au ministère compétent. Le SCRS a pour rôle de fournir aux ministères concernés des conseils et des renseignements à sa disposition susceptibles de présenter un intérêt dans la détermination de l'admissibilité de la personne. Le CSARS a fait enquête et il a examiné les conseils fournis par le SCRS.

Conclusions du CSARS

Le CSARS a conclu que le SCRS n'avait pas fait de fausses allégations à l'ASFC ni à CIC dans les conseils fournis en lien avec la demande de résidence permanente. Les politiques et procédures internes applicables et les dispositions pertinentes de la Loi sur le SCRS ont été respectées.

Par ailleurs, le plaignant a allégué que le SCRS n'avait pas respecté ses obligations de divulgation envers le CSARS. Le CSARS a conclu que c'est à lui de commenter la pertinence de la divulgation faite par le SCRS de renseignements classifiés. Le CSARS a estimé que les éléments de preuve pertinents lui avaient été correctement présentés.

Quant aux observations du plaignant touchant l'allégation de retard indu, le CSARS a déterminé que l'enquête de sécurité avait été menée en temps opportun.

Pour ces motifs, la plainte a été rejetée.

REFUS D'UNE HABILITATION DE SÉCURITÉ : PLAINTÉ EN VERTU DE L'ARTICLE 42 DE LA LOI SUR LE SCRS

Le CSARS a enquêté sur une plainte en vertu de l'article 42 de la Loi sur le SCRS concernant le refus de toute habilitation de sécurité au plaignant par un ministère. Ce ministère a également révoqué la cote de fiabilité du plaignant. Le CSARS a conclu qu'il y avait des motifs raisonnables de refuser l'habilitation de sécurité du plaignant selon l'ensemble des renseignements et de la preuve résultant du processus de filtrage de sécurité.

À la lumière de la preuve qui lui a été présentée, le CSARS a fait enquête sur le processus de filtrage de sécurité mené par le SCRS et le ministère. Le CSARS a entendu des témoignages sur le processus d'enquête de sécurité, et sur les politiques et pouvoirs en place pour la prise de décisions touchant l'évaluation de l'autorisation de sécurité.

Dans son témoignage, le plaignant a allégué qu'il avait fait l'objet d'intimidation et de harcèlement dans son milieu de travail en raison des répercussions de l'enquête de sécurité et qu'il était surveillé par les services de sécurité et les services de police américains et canadiens. Le plaignant a nié les allégations résultant de l'évaluation de sécurité.

Le CSARS a été convaincu que le plaignant avait bénéficié de l'équité procédurale pendant l'enquête de filtrage du SCRS et le processus d'examen du filtrage de sécurité du ministère. Le CSARS a conclu que le plaignant avait été correctement informé des

considérations présentées et qu'il avait eu l'occasion d'y répondre.

Le CSARS a enquêté sur les conclusions de l'évaluation de sécurité faite par le SCRS. Il a été convaincu que les renseignements sur lesquels le SCRS s'est fondé étaient exacts, crédibles, représentés équitablement et mis dans le bon contexte.

Conclusions et recommandation du CSARS

Le CSARS a conclu qu'il y avait des motifs raisonnables, selon la Politique sur la sécurité du gouvernement et la Norme sur le filtrage de sécurité du personnel, pour que l'administrateur général du ministère refuse toute habilitation de sécurité au plaignant.

Le CSARS a été convaincu de l'exactitude des renseignements sur lesquels le ministère s'est fondé pour prendre la décision.

Pour ces motifs, le CSARS a recommandé que la décision de refuser l'habilitation de sécurité soit maintenue.

ALLÉGATIONS CONCERNANT DES ACTES DU SCRS AYANT MENÉ AU REFUS D'ACCÈS À UN SITE ET À LA RÉVOCATION D'UNE HABILITATION DE SÉCURITÉ AYANT ENTRAÎNÉ UNE PERTE D'EMPLOI : PLAINTÉ EN VERTU DE L'ARTICLE 41 DE LA LOI SUR LE SCRS

Le CSARS a enquêté sur une plainte en vertu de l'article 41 de la Loi sur le SCRS dans laquelle le plaignant alléguait que les actes du SCRS avaient mené à la révocation de son autorisation d'accès à un site, ce qui avait entraîné la perte de son emploi. Le plaignant a aussi allégué que ces actes constituaient de la discrimination et violaient ses droits constitutionnels, et que le SCRS avait fourni une évaluation de sécurité injuste et déraisonnable. Enfin, le plaignant a allégué que le SCRS lui avait refusé l'autorisation d'accès à un site par mesure de représailles contre lui.

Le plaignant a demandé trois recours au CSARS, soit :

- que le SCRS soit sanctionné de manière à ce que son inconduite ne se reproduise pas à l'avenir;
- que le ministre lui offre une réparation appropriée, y compris pour le tort causé par les actes du SCRS, ainsi qu'une réparation en vertu de l'article 24 de la *Charte canadienne des droits et libertés*;
- que le ministre le dégage de toute allégation concernant la sécurité du Canada.

Le CSARS a examiné la preuve du plaignant et celle du SCRS ainsi que d'autres documents pertinents auxquels il a eu accès en cours d'enquête.

Conclusions du CSARS

Le CSARS a conclu que le SCRS a agi en conformité avec la loi et de manière appropriée en refusant au plaignant une habilitation de sécurité, et n'a pas retenu l'allégation du plaignant concernant des représailles du SCRS à son endroit.

Le CSARS a conclu que l'allégation du plaignant selon laquelle le SCRS a agi de façon illicite et inappropriée en exigeant qu'il se livre à de l'espionnage en son nom n'était pas fondée.

Le CSARS a également conclu que le SCRS avait violé les droits constitutionnels du plaignant en vertu de l'article 8 de la Charte.

Le CSARS a également conclu que le SCRS n'avait pas accordé au plaignant le niveau d'équité procédurale qui lui était dû dans le cadre de certaines enquêtes.

Le CSARS a également conclu que l'évaluation de sécurité faite par le SCRS avait privé le plaignant de l'autorisation d'accès à un site, ce qui avait entraîné une perte d'emploi.

Quant à l'allégation du plaignant selon laquelle le Comité devrait renvoyer l'affaire à la Commission canadienne des droits de la personne, le CSARS a conclu que ce renvoi serait inapproprié puisqu'il dispose d'une preuve suffisante pour tirer des conclusions sur les allégations du plaignant.

Enfin, le CSARS a conclu qu'aucune preuve ne lui permettait de conclure que le SCRS a agi de mauvaise foi en entreposant du matériel non sollicité provenant d'une organisation.

Recommandation du CSARS

Le CSARS a recommandé que le SCRS demande un avis juridique afin de dûment prendre en compte et appliquer les autorisations juridiques appropriées dans les décisions qu'il rend sur les mesures à prendre.

Quant à la demande du plaignant concernant les recommandations énoncées plus haut, le CSARS a indiqué que son mandat est d'enquêter sur les actes ou les actes présumés du SCRS. Le CSARS a également indiqué qu'il outrepasserait son mandat en formulant des recommandations au ministre sur les mesures qu'il pourrait envisager. Étant donné que le rapport sera transmis au ministre, le CSARS est convaincu que celui-ci prendra toute mesure qu'il jugera appropriée dans les circonstances en vertu des pouvoirs qui lui sont conférés.

Conclusion

Le CSARS a conclu que rien dans la preuve ne permet de conclure que les actes du SCRS constituent de la discrimination, et qu'il ne serait pas approprié qu'il demande à la Commission canadienne des droits de la personne son opinion et ses commentaires sur cette plainte. Pour ces motifs, la plainte a été appuyée en partie.

ALLÉGATIONS DE LA DIVULGATION ET TRANSMISSION DE FAUSSES INFORMATIONS ET DES IDENTITÉS À UN PAYS TIERS : PLAINTÉ EN VERTU DE L'ARTICLE 41 DE LA LOI SUR LE SCRS

Le plaignant s'adresse au CSARS en lien avec un épisode dramatique vécu par lui et sa famille. Le fils du plaignant, mineur à l'époque, a eu des contacts via les médias sociaux avec un individu que le plaignant identifie comme un « cybercriminel ». Selon le plaignant, le cybercriminel a tenté de manipuler son fils et de le convaincre que vivre dans une communauté occidentale était un péché. Le plaignant a accepté de rencontrer deux agents du SCRS et les a ensuite accueillis chez lui pour discuter avec son fils des interactions entre celui-ci et l'individu. Au cours de cet entretien, le plaignant allègue que les agents du SCRS ont encouragé le plaignant et sa famille à dénoncer la situation par téléphone à la Gendarmerie Royale du Canada (GRC), ce qui a été fait par le plaignant le soir même. Le lendemain, son fils se fait arrêter chez lui par la GRC et ce devant un cirque médiatique rassemblé près du domicile du plaignant. Son fils a ultimement été relâché peu après et n'a pas fait l'objet de chef d'accusations. Cependant, le plaignant soutient que les conséquences de ces événements continuent d'affecter sa famille.

Le plaignant blâme en partie le SCRS et ses agents pour ce qui est arrivé à sa famille, ne serait-ce que par leur inertie et par leur partage d'information. Le plaignant s'oppose au traitement que lui et son fils ont reçu après avoir fait leur devoir de citoyen qui était de coopérer avec les autorités et dénoncer une menace. Il accuse le SCRS et la GRC d'avoir pris des mesures contre la victime, son fils, plutôt que contre le cybercriminel.

Le plaignant a résumé ses allégations contre le SCRS comme suit :

- le SCRS a transmis de fausses informations à l'équipe intégrée de la sécurité nationale de la GRC;
- le plaignant a fait face au silence de deux membres de la GRC quant à l'arbitraire des membres de la GRC;
- le SCRS a transmis l'identité du plaignant et celui de son fils à un tiers pays ;
- le SCRS n'a pas respecté les conclusions et les recommandations du rapport de la commission du juge O'Connor en matière de communication d'informations;
- le SCRS a atteint à leur vie privée, leur intégrité et leur sécurité.

Conclusions

Le CSARS conclut que toutes les allégations à la base de cette plainte devaient être rejetées car elles sont infirmées par la preuve déposée. L'enquête de cette plainte a exploré toutes les facettes pertinentes découlant des allégations.

Le CSARS conclut que le SCRS a agi en conformité avec son mandat et ses priorités. Aucune preuve n'a été présentée démontrant que le SCRS s'est écarté de la Loi sur le SCRS ou de ses politiques applicables en matière de ciblage. Le CSARS constate que les procédures rigoureuses traitant des enquêtes impliquant des mineurs ont été

suivies. Le CSARS conclut que le SCRS avait des motifs raisonnables de soupçonner que les activités en question constituaient une menace à la sécurité du Canada et donc de prendre les démarches d'enquête qu'il a pris selon l'article 12 de la Loi sur le SCRS. Le CSARS ne voit pas le besoin d'émettre quelque recommandation au SCRS.

Annexe D: Tableau statistique des plaintes

Du 1er avril 2018 au 31 mars 2019

Demandes de renseignements reçues	91
Nouveaux dossiers de plaintes reçus Réputés reçus conformément à la Règle 5	25 art. 41 (plaintes sur le SCRS) : 14 art. 42 (autorisations de sécurité) : 11 art. 45 (CCDP) : 0
Dossiers de plaintes retirés avant la détermination de la compétence	19 Compétence acceptée Compétence refusée art. 41 : 3 art. 41 : 7 art. 42 : 2 art. 42 : 7 art. 45 : 0 art. 45 : 0
Complaint files withdrawn prior to determination on jurisdiction	2
ENQUÊTES ACTIVES SUR UNE PLAINTÉ PENDANT CETTE PÉRIODE (une fois que la compétence a été acceptée)	14
Enquêtes sur une plainte amorcées lors du dernier exercice	9 s. 41: 7 s. 42: 2
Enquêtes sur une plainte pour lesquelles la compétence a été acceptée pendant cette période	5
NOMBRE TOTAL D'ENQUÊTES SUR UNE PLAINTÉ TERMINÉES Enquêtes sur une plainte terminées	2 0 Retirées 0 Résolues 2 Reportées art. 41 : 2 art. 42 : 0
Enquêtes sur une plainte qui se poursuivront pendant la prochaine année civile	12 art. 41 : 9 art. 42 : 3

Du 1er avril au 31 décembre 2019

Demandes de renseignements reçues	67
Nouveaux dossiers de plaintes reçus Réputés reçus conformément à la Règle 5	32 art. 16 (plaintes sur le SCRS) : 17 art. 17 (plaintes sur le CST) : 0 art. 18 (autorisations de sécurité) : 10 art. 19 (plaintes sur la GRC) : 5 art. 19 (Loi sur la citoyenneté) : 0 art. 45 (CCDP) : 0
Dossiers de plaintes au sujet desquels la compétence a été déterminée	18 Compétence acceptée Compétence refusée s. 16: 3 s. 16: 6 s. 18: 0 s. 18: 8 s. 19: 1 s. 19: 0
Dossiers de plaintes retirés avant la détermination de la compétence	3
ENQUÊTES ACTIVES SUR UNE PLAINTÉ PENDANT CETTE PÉRIODE (une fois que la compétence a été acceptée)	16
Enquêtes sur une plainte amorcées lors du dernier exercice	12 s. 16: 9 s. 18: 3
Enquêtes sur une plainte pour lesquelles la compétence a été acceptée pendant cette période	4
NOMBRE TOTAL D'ENQUÊTES SUR UNE PLAINTÉ TERMINÉES	4
Enquêtes sur une plainte terminées	1 Retirées 1 Résolues 2 Reportées art. 16 : 3 art. 18 : 1
Enquêtes sur une plainte qui se poursuivront	12 art. 16 : 9 art. 18 : 2 art. 19 : 1

Annexe: E

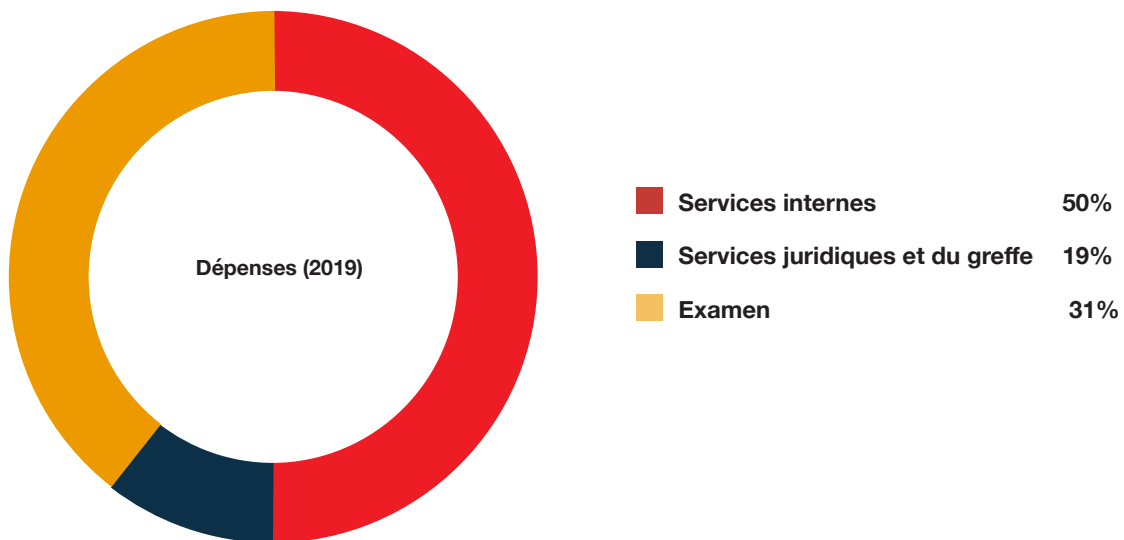
Organisation, réalisations et priorités de l'OSSNR

Le personnel du Secrétariat de l'OSSNR est organisé en fonction de trois principaux secteurs d'activité, soit l'examen, les enquêtes sur les plaintes et les services organisationnels. Afin de tenir compte du vaste mandat de l'OSSNR et d'appuyer l'examen d'un vaste éventail de nouvelles activités et organisations, le Secrétariat prendra de l'expansion au cours des prochaines années, et on prévoit un effectif final de 100 personnes.

Voici un aperçu budgétaire de l'organisation, suivi de renseignements détaillés sur la transition du Comité de surveillance des activités de renseignement de sécurité (CSARS) à l'OSSNR, sur nos principales réalisations et sur nos priorités pour l'année à venir.⁹³

Rapport sur les dépenses

	Dépenses du CSARS de janvier jusqu'à la fin de l'année fiscale	Dépenses du CSARS et de l'OSSNR d'avril à décembre	Dépenses (2019)
Services juridiques et du greffe	378 670	663 446	1 042 117
Examen	588 535	1 137 683	1 726 218
Services internes	1 278 813	1 541 302	2 820 115
Total	2 246 018 \$	3 342 431 \$	5 588 450 \$



Transition du CSARS à l'OSSNR

Tout au long de 2019, le Secrétariat de l'OSSNR s'est efforcé d'assurer une transition réussie et efficace vers une organisation beaucoup plus grande ayant un mandat beaucoup plus vaste. Dans le cadre de cette transition, l'accent a été mis sur les éléments suivants : l'obtention de nouveaux locaux; la dotation et la formation efficaces des employés; l'établissement de relations de travail solides avec les ministères et les organismes, ainsi qu'avec d'autres organismes d'examen canadiens; et le respect des exigences en matière de rapports obligatoires.

Les principaux défis du point de vue des services organisationnels tout au long de la période visée par le rapport et jusqu'en 2020 sont les suivants :

- embaucher et accueillir les personnes talentueuses nécessaires à la réalisation du mandat élargi de l'OSSNR — l'effectif devrait passer de 33 à 100 personnes;
- mettre à niveau les pratiques en matière de sécurité matérielle, de personnel et d'information;
- mettre en œuvre des politiques, des procédures et des systèmes pour guider la nouvelle organisation;
- apporter des améliorations à notre infrastructure technologique et de communication;
- gérer l'augmentation des autorisations de dépenses annuelles — de 5,3 M\$ à 24,1 M\$;
- accroître l'efficacité des politiques, des systèmes et des pratiques de gestion de l'information;
- mettre en place des pratiques efficaces de protection de la vie privée.

Ces défis ont été, depuis mars 2020, exacerbés par la pandémie qui se poursuit. Il a été particulièrement difficile de composer avec les répercussions de la COVID-19 notamment en ce qui a trait à l'accès aux renseignements classifiés, qui, bien sûr, ne peut se faire que dans un environnement sécurisé. Néanmoins, les réalisations du groupe des services organisationnels de l'OSSNR ont été nombreuses au cours de sa première année d'activité. Ces réalisations sont exposées en détail ci-dessous.

Ressources humaines

Réalisations de 2019

- Recrutement d'une équipe de ressources humaines spécialisée
- Achèvement et mise en œuvre des composantes de base d'une politique de gestion des ressources humaines et des Termes et conditions d'emploi
- Déploiement complet des systèmes de paye (PeopleSoft et Phénix) et résolution de la plupart des problèmes de paye de longue date du personnel
- Finalisation de la structure organisationnelle de l'OSSNR et achèvement de la majeure partie des classifications de poste
- Renforcement des pratiques de dotation et mise en œuvre d'un programme d'aide aux employés

- Conclusion d'ententes de prestation de services avec d'autres ministères pour appuyer les activités opérationnelles des ressources humaines comme le traitement des opérations de paye, la classification des postes et les activités de dotation

Sécurité et locaux

Réalisations de 2019

- Création d'une équipe spécialisée d'employés responsables des activités de sécurité et des locaux
- Élaboration d'un plan de sécurité à multiples facettes
- Achèvement de projets pour maximiser le nombre de bureaux à l'administration centrale de l'OSSNR et identification de solutions pour des locaux temporaires, permanents et satellites pour accueillir l'effectif croissant de l'OSSNR

Technologie de l'information et gestion de l'information

Réalisations de 2019

- Déploiement réussi du Réseau canadien très secret (RCTS) pour tous les employés qui doivent y avoir accès, ce qui permet l'échange électronique sécurisé de renseignements avec d'autres ministères et organismes
- Déploiement réussi de la fonctionnalité d'accès au réseau privé virtuel (RPV) et de chiffrement, permettant l'accès à l'information et l'échange d'information à partir des réseaux existants de l'OSSNR vers des ordinateurs de bureau/portables distants
- Numérisation de plusieurs versions papier d'examens et de plaintes

Finances, approvisionnement, planification, accès à l'information et protection des renseignements personnels

Réalisations de 2019

- Mise en œuvre des systèmes financiers et d'approvisionnement de l'OSSNR et de l'infrastructure de codage financier connexe
- Achèvement des activités de fin d'exercice pour le CSARS et des activités de fin d'exercice pour l'OSSNR
- Amélioration des rapports financiers pour mieux appuyer la prise de décisions par la haute direction
- Réalisation d'une évaluation des facteurs relatifs à la vie privée et amélioration du processus de caviardage et de diffusion de l'information

Annexe F:

Liste des abréviations

Abréviation	Nom complet
AMC	Affaires mondiales Canada
ASFC	Agence des services frontaliers du Canada
BCCST	Bureau du commissaire du Centre de la sécurité des télécommunications
BVG	Bureau du vérificateur général du Canada
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada
CCETP	Commission civile d'examen et de traitement des plaintes relatives à la GRC
COA	Cyberopérations actives
COD	Cyberopérations défensives
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement
CPVP	Commissariat à la protection de la vie privée
CSARS	Comité de surveillance des activités de renseignement de sécurité
CST	Centre de la sécurité des télécommunications
FAC	Forces armées canadiennes
FIORC	Conseil de surveillance et d'examen du renseignement du Groupe des cinq
GEC	Gouverneur en conseil
GRC	Gendarmerie royale du Canada
IRCC	Immigration, Réfugiés et Citoyenneté Canada
LCISC	Loi sur la communication d'information ayant trait à la sécurité du Canada
LDISC	Loi sur la divulgation d'information ayant trait à la sécurité du Canada
LPFDAR	Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles
LPI	Loi sur la protection de l'information
MDN	Ministère de la Défense nationale
MRM	Mesure de réduction de la menace
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement
SCRS	Service canadien du renseignement de sécurité
SCT	Secrétariat du Conseil du Trésor du Canada
TSA	Habilitation de sécurité de niveau Très secret approfondi

Notes de fin de document

- 1 Site Web du Bureau du vérificateur général du Canada (BVG), https://www.oag-bvg.gc.ca/internet/Francais/admin_f_41.html
- 2 Site Web de la Commission canadienne des droits de la personne, <https://www.chrc-ccdp.gc.ca/fra>
- 3 De plus amples renseignements sur ces éléments de l'organisation sont disponibles sur le site Web de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), <http://www.nsira-ossnr.gc.ca/index-fra.html>
- 4 Lettre de l'OSSNR au ministre de la Sécurité publique et de la Protection civile, le 16 mars 2020.
- 5 *Articles 12 et 21 de la Loi sur le service canadien du renseignement de sécurité, LRC 1985, ch. C-23 (Re)*, 2020 CF 616, lettre datée du 15 mai 2020. La décision est disponible à l'adresse : <https://decisions.fct-cf.gc.ca/fc-cf/decisions/fr/item/482466/index.do>
- 6 Lettre de l'OSSNR au procureur général du Canada, le 25 février 2020.
- 7 Site Web de l'OSSNR, <http://www.nsira-ossnr.gc.ca/>
- 8 Conformément aux dispositions transitoires 12(1) et 12(2) de la *Loi de 2017 sur la sécurité nationale*, ce rapport comprend également des résumés d'examens que nos prédécesseurs, le Comité de surveillance des activités de renseignement de sécurité (CSARS) et le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST), n'avaient pas encore rendus publics. Ces éléments se trouvent à l'annexe B.
- 9 Site Web du CSARS, <http://www.sirc-csars.gc.ca/index-fra.html>
10. Site Web du BCCST, <https://www.ocsec-bccst.gc.ca/fr>
11. Des renseignements supplémentaires sur les ressources et les résultats ministériels sont disponibles à l'adresse: <http://www.nsira-ossnr.gc.ca/pubpub/dppm/index-fra.html>
12. Site Web de la Gendarmerie royale du Canada (GRC), <https://www.rcmp-grc.gc.ca/fr>
13. Avant cette approche, la seule façon pour le public d'obtenir des copies des examens était de présenter des demandes en vertu de la *Loi sur l'accès à l'information*.
14. Site Web du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), <https://www.nsicop-cpsnr.ca/index-fr.html>
15. Site Web du Commissariat à la protection de la vie privée du Canada (CPVP), <https://www.priv.gc.ca/fr/>
16. Le CPSNR a présenté un aperçu des différentes catégories de collecte de renseignement au chapitre quatre de son rapport public annuel de 2018, disponible à l'adresse: <https://www.nsicop-cpsnr.ca/reports/rp-2019-04-09/intro-fr.html>.
17. Site Web du Service canadien du renseignement de sécurité (SCRS), <https://www.canada.ca/fr/service-renseignement-securite.html>.
18. Les mandats du SCRS pour la collecte d'information sont accordés conformément à l'article 21 de la Loi sur le SCRS. Ces mandats peuvent servir à appuyer les enquêtes du SCRS sur les menaces pour la sécurité du Canada en vertu de l'article 12 de la Loi ou à appuyer les enquêtes du SCRS sur le renseignement étranger en vertu de l'article 16 de la Loi. L'article 21 de la Loi sur le SCRS se trouve à l'adresse: <https://laws-lois.justice.gc.ca/eng/acts/c-46/page-41.html#h-118715>.
- 19 Site Web du Centre de la sécurité des télécommunications (CST), <https://www.cse-cst.gc.ca/en>.
20. Voir la partie sur les « Autorisations » de la Loi sur le CST à l'adresse: <https://laws-lois.justice.gc.ca/fra/lois/C-35.3/page-3.html#h-1170483>.

21. Voir la partie sur les « Attributions » du commissaire au renseignement dans la *Loi sur le commissaire au renseignement* à l'adresse: <https://laws-lois.justice.gc.ca/fra/lois/l-14.85/page-1.html#h-1170243>. D'autres renseignements sur le rôle du commissaire au renseignement sont fournis sur le site Web du Bureau du commissaire au renseignement à l'adresse: <https://www.canada.ca/fr/commissaire-renseignement.html>.
22. Un certain nombre de lois générales régissent la façon dont les ministères peuvent recueillir, conserver et communiquer des renseignements personnels. La plus importante d'entre elles est la *Loi sur la protection des renseignements personnels*.
23. Un exemple récent à cet effet sont les Instructions du ministre à l'intention du Service canadien du renseignement de sécurité : Reddition de comptes, publiées le 10 septembre 2019 et disponibles à l'adresse: <https://www.securitepublique.gc.ca/cnt/trnsprnc/ns-trnsprnc/mnstrl-drctn-csisacc-fr.aspx>
24. Pour en savoir plus, voir : CPVP (2014), « Métadonnées et vie privée – Un aperçu technique et juridique », https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/; ainsi que l'examen du CSARS sur l'utilisation des métadonnées au SCRS, <http://www.sirc.gc.ca/anrran/2014-2015/index-fra.html#sc2-7>.
25. *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (L.C. 2019, ch. 13, art. 2), <https://laws-lois.justice.gc.ca/fra/lois/N-16.62/page-1.html>
26. CSARS (2015), Vers de nouveaux horizons: préparer le terrain du changement dans la surveillance des activités de renseignement de sécurité— Rapport annuel 2014-2015, « Étude de base: L'utilisation des métadonnées au SCRS », <http://www.sirc.gc.ca/anrran/2014-2015/index-fra.html#sc2-7>
27. Discuté dans le rapport annuel de 2014-2015 du BCCST, http://www.sirc.gc.ca/anrran/2015-2016/index-fra.html#section_2_4.
28. CSARS (2016), Rapport annuel 2015-2016 — Sur notre lancée, « Un examen des activités de gestion et d'exploitation des données du SCRS », http://www.sirc.gc.ca/anrran/2015-2016/index-fra.html#section_2_4
29. X (Re), 2013 CF 1275, confirmé dans le cadre de l'appel 2014 CAF 249; 2016 CF 1105; et 2020 CF 616, daté du 15 mai 2020.
30. Ministre de la Sécurité publique et de la Protection civile (10 septembre 2019), Instructions du ministre à l'intention du Service canadien du renseignement de sécurité : Reddition de comptes. <https://www.securitepublique.gc.ca/cnt/trnsprnc/ns-trnsprnc/mnstrl-drctn-csisacc-fr.aspx>.
31. *Articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité* (L.R.C. (1985), ch. C-23), 2016 CF 1105 et 2020 CF 616, daté du 15 mai 2020. La décision est disponible à l'adresse: <https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/482466/index.do>.
32. Dans le cadre de l'examen daté du 12 mai 2015 au sujet de la relation et des échanges entre le SCRS et le ministère des Affaires étrangères, du Commerce et du Développement, le CSARS a attiré l'attention sur les contraintes juridiques auxquelles le SCRS a fait face en ce qui a trait à ses activités faisant appel à des sources humaines lorsqu'il a été mentionné que certaines des activités du SCRS à l'étranger pourraient avoir été réalisées en violation du Règlement d'application des résolutions des Nations Unies sur le Talibane, EIIL (Daech) et Al-Qaïda ainsi que d'autres lois similaires. Le CSARS a ensuite demandé au SCRS d'examiner en profondeur ses propres activités afin de s'assurer de leur conformité. Plus tard, dans le rapport d'examen daté du 27 mai 2016, traitant des combattants étrangers canadiens, le CSARS a souligné les risques juridiques liés à certaines activités du SCRS et a recommandé que « le SCRS demande des éclaircissements d'ordre juridique pour déterminer si ses employés et sources humaines sont protégés en vertu de la règle de common law de l'immunité de la Couronne en ce qui a trait aux infractions relatives au terrorisme du Code criminel du Canada ».
33. Une version caviardée du certificat est disponible à l'adresse: <http://www.nsira-ossnr.gc.ca/pubpub/cercer/2018-07-fra.html>.
34. X (Re), 2020 CF 616, daté du 15 mai 2020. <https://decisions.fct-cf.gc.ca/fc-cf/decisions/fr/item/482466/index.do>.
35. Voir le communiqué du 16 juillet 2020 de l'OSSNR, disponible à l'adresse: <http://www.nsira-ossnr.gc.ca/nwsspr/riscmq/20200716-fra.html>

36. États-Unis, National Counterintelligence and Security Center (s.d.), « Conseil de surveillance et d'examen du renseignement du Groupe des cinq (FIORC) ». (En anglais seulement)
<https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc>

37. Pour consulter l'examen de l'Agence des services frontaliers du Canada (ASFC) complété par le CPSNR, voir le chapitre 3 du rapport public annuel de 2019 du CPSNR, disponible à l'adresse:
<https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/intro-fr.html>.
Pour le ministère de la Défense nationale (MDN), consultez le chapitre 4 du rapport annuel de 2018 du CPSNR disponible à l'adresse:
<https://www.nsicop-cpsnr.ca/reports/rp-2019-04-09/intro-fr.html>,
de même que le rapport spécial disponible à l'adresse:
<https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-sr/intro-fr.html>.

38. Comme les connaissances de l'OSSNR sur les thèmes de protection s'approfondiront au cours des prochaines années, il est attendu que les examens dans ce domaine évoluent également pour inclure les liens pertinents entre le gouvernement et le secteur privé, y compris l'examen des activités du secteur privé sous réglementation fédérale qui ont des répercussions sur les personnes, l'information et d'autres biens du portefeuille de la sécurité nationale et du renseignement.

39. Une menace interne est une menace qui provient de personnes au sein d'une organisation (des employés ou des entrepreneurs) qui se servent de leur accès à de l'information, à des biens ou à des systèmes internes pour procéder à des communications non autorisées.

40. CBC News (8 mars 2019), « Convicted spy Jeffrey Delisle released on full parole », (en anglais seulement)
<https://www.cbc.ca/news/canada/nova-scotia/convicted-spy-russians-canadian-armed-forces-parole-1.5049166>.

41. CBC News (28 juin 2019), « Case of Hamilton man allegedly spying for China, tangled in secrecy », (en anglais seulement)
<https://www.cbc.ca/news/canada/hamilton/case-of-hamilton-man-allegedly-spying-for-china-tangled-in-secrecy-1.5193658>.

42. Globe and Mail (16 octobre 2019), « RCMP senior officers explored appointing Cameron Ortis as a police officer », (en anglais seulement)
<https://www.theglobeandmail.com/politics/article-rcmp-senior-officers-explored-appointing-cameron-ortis-as-a-police/>

43. La Politique sur la sécurité du gouvernement est entrée en vigueur le 1er juillet 2019. Elle remplace la Politique sur la sécurité du gouvernement qui était en vigueur du 1er juillet 2009 au 30 juin 2019. Disponible à l'adresse : <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578>. La Directive sur la gestion de la sécurité et ses procédures obligatoires sont entrées en vigueur le 1er juillet 2019 et ont remplacé diverses normes et directives de sécurité. Disponible à l'adresse:
<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611>

44. Cette norme de protection pourrait aussi concerner la cybersécurité, une question que l'OSSNR couvrira dans de nombreux examens du CST.

45. Les ministères et organismes gouvernementaux canadiens peuvent choisir parmi des marchés qui relèvent de leurs responsabilités de passation de marchés déléguées, et comportent un accès à de l'information et à des biens de nature délicate. Le ministère peut lui-même s'assurer que l'entrepreneur satisfait aux exigences de sécurité appropriées ou demander à Services publics et Approvisionnement Canada (SPAC) de s'en occuper à l'aide du Programme de la sécurité industrielle. Ce programme vise la protection de l'information et des biens protégés ou classifiés. Si un marché déborde les responsabilités de passation de marchés déléguées, SPAC est le responsable par défaut. <https://www.tpsgc-pwgsc.gc.ca/aiprp-atip/efvp-pia/prgsecind-indsecprg-fra.html>

46. Par exemple, les employés de l'appareil de la sécurité et du renseignement sont plus susceptibles de suivre une formation rigoureuse et d'obtenir des rappels de sécurité régulièrement, de plus leurs systèmes électroniques et matériels ainsi que leurs locaux font régulièrement l'objet de vérifications de sécurité.

47. Les concepts de filtrage de sécurité, comme le contrôle de sécurité des immigrants, les mesures de sécurité dans les aéroports et aux frontières ou encore les listes de surveillance des voyageurs, sont complètement distincts de la protection.

48. Voir en particulier l'article 8 de la *Loi sur la protection de l'information* (LPI) sur les renseignements opérationnels spéciaux. <https://laws-lois.justice.gc.ca/fra/lois/O-5/index.html>

49. L'article 4 de la LPI résume les infractions diverses.
<https://laws-lois.justice.gc.ca/fra/lois/o-5/page-2.html#h-384913>

50. Les paragraphes 154 à 157 du présent rapport abordent plus en détail la protection des dénonciateurs.

51. Sauf dans des situations d'urgence, l'accusé doit épuiser tous les recours internes avant de faire une divulgation. L'OSSNR a un rôle à jouer pour donner suite aux préoccupations concernant un acte répréhensible.

52. CBC News (29 novembre 2012), « Early clues to navy spy Delisle's guilt overlooked ». (En anglais seulement)
<https://www.cbc.ca/news/canada/early-clues-to-navy-spy-delisle-s-guilt-overlooked-1.1235506>

53. Secrétariat du Conseil du Trésor du Canada (20 octobre 2014), « Norme sur le filtrage de sécurité ». h27. <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115>

54. OSSNR (août 2019), Examen relatif à la Direction de la sécurité interne du SCRS.

55. Secrétariat du Conseil du Trésor du Canada (20 octobre 2014), « Norme sur le filtrage de sécurité ». <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115>

56. Lettre de l'OSSNR à l'intention du Secrétariat du Conseil du Trésor, 12 décembre 2019.

57. Voir les rapports annuels du CSARS de 1985 1986 à 1991 1992,
<http://www.sirc.gc.ca/anrran/index-fra.html>

58. *R. c. Béland* [1987] 2 RCS 398.

59. CPVP, « Pour les institutions fédérales ».
<https://www.priv.gc.ca/fr/pour-les-institutions-federales/>

60. *Loi sur la communication d'information ayant trait à la sécurité du Canada* (L.C. 2015, ch. 20, art. 2).
<https://laws-lois.justice.gc.ca/fra/lois/S-6.9/index.html>

61. Les trois commissions d'enquête sont les suivantes : Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar (<https://www.canada.ca/fr/conseil-privé/services/com-missions-enquete/arar.html>), Enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin (<https://www.securitepublique.gc.ca/cnt/cntrng-crm/plcng/cnmcs-plcng/rsrch-prtl/dtls-en.aspx?d=PS&i=73612571>), et Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India (<https://www.securitepublique.gc.ca/cnt/rsrscs/lbrr/ctlg/dtls-fr.aspx?d=PS&i=85557953>). Voir également les délibérations du Comité spécial sur la mission canadienne en Afghanistan <https://www.noscommunes.ca/Committees/fr/AFGH?parl=40&session=2>

62. Voir, par exemple : « Examen d'études de cas concernant le partage de l'information entre le SCRS et des entités étrangères » dans le rapport annuel 2017-2018 du CSARS : Bâtir pour demain : l'avenir de la reddition des comptes en matière de renseignement de sécurité au Canada (http://www.sirc-csars.gc.ca/anrran/2017-2018/index-fra.html#section_2_2); et « Examen annuel des divulgations d'information sur l'identité de Canadiens par le CST » dans le rapport annuel 2018-2019 du BCCST (<https://www.ocsec-bccst.gc.ca/s21/s85/d445/fra/points-saillants-rapports-presentes>).

63. Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India (16 juin 2010). https://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/fr/reports/finalreport/index.asp

64. Consultation sur la sécurité nationale, disponible à l'adresse suivante : <https://www.canada.ca/fr/services/defense/securitenationale/consultation-securite-nationale.html>; ainsi que son document de référence à l'appui : « Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016 », disponible à l'adresse : <https://www.securitepublique.gc.ca/cnt/rsracs/pblctns/ntnl-scrtn-grn-ppr-2016/index-fr.aspx>
65. La Loi sur la protection des renseignements personnels énonce une série de circonstances où des renseignements personnels recueillis par les ministères et organismes fédéraux peuvent être communiqués sans le consentement de la personne concernée. Plusieurs de ces circonstances se rapportent à des activités d'échange d'information dans le contexte de la sécurité nationale. La disposition sur les « usages compatibles » permet la divulgation des renseignements personnels « destinés à un usage, ou communiqués pour un usage, compatible avec les fins auxquelles les renseignements ont été recueillis ou préparés par l'institution ». Cette disposition offre une souplesse aux institutions fédérales pour réaliser leurs activités dans le cadre de leur mandat.
66. Comité de surveillance des activités de renseignement de sécurité (2017), CSARS Rapport annuel 2016-2017 : Accélérer la reddition de comptes. « Partie 2 : Études », *La Loi sur la communication d'information ayant trait à la sécurité du Canada*. http://www.sirc-csars.gc.ca/anrran/2016-2017/index-fra.html#section_2_8
67. CPVP (2017). Examen de la mise en œuvre et du mode d'application de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/verifications/ar-vr_scisa_2017/
68. Les mises en garde sont des restrictions d'utilisation qui accompagnent les produits de renseignement communiqués aux partenaires. Par exemple, une mise en garde particulière, la « règle des tiers », précise que l'information fournie est communiquée à des fins de renseignement seulement et qu'elle ne devrait pas être utilisée dans le cadre de poursuites ou communiquée à d'autres organismes sans avoir l'autorisation préalable de l'organisme d'origine. L'information non assortie d'une mise en garde ne fixe par conséquent aucune limite.
69. Voir le Rapport public annuel du SCRS 2018 pour obtenir plus d'information sur le Comité d'évaluation des échanges d'information, sous « Considérations relatives aux droits de la personne ». <https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/rapport-public-2018/la-confiance-des-canadiens.html>
70. Le 4 septembre 2019, la gouverneure en conseil, donnant suite à la recommandation du ministre des Finances, a publié par décret des Instructions visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères (les Instructions) à l'intention de 12 ministères et organismes. Le décret interdit toute communication de renseignements susceptible d'entraîner un risque sérieux que de mauvais traitements soient infligés à un individu, ainsi que certaines formes d'utilisation de renseignements vraisemblablement obtenus à la suite de mauvais traitements infligés à un individu.
71. Le 17 septembre 2020, le CPSNR a annoncé qu'il mènera un examen portant sur les activités de cyberdéfense du gouvernement. <https://www.nsicop-cpsnr.ca/press-releases/pr-cp-2020-09-17/pr-cp-2020-09-17-fr.html>
72. En juillet 2019, l'entrée en vigueur de la *Loi de 2017 sur la sécurité nationale* a modifié les pouvoirs du SCRS en lien aux mesures de réduction de la menace. Les changements apportés à cet égard ont ajouté des restrictions quant aux types de mesures de réduction de la menace (MRM) autorisées. Ils ont établi l'obligation de consulter d'autres ministères et organismes fédéraux relativement à leur capacité de réduire la menace, ont clarifié dans quelles circonstances il est nécessaire d'obtenir un mandat pour prendre une MRM proposée et, en application du critère de raisonnable et de proportionnalité, ont imposé au SCRS l'obligation de prendre en compte les effets prévisibles potentiels des MRM sur les droits de tiers. En outre, le SCRS doit maintenant informer l'OSSNR de l'ensemble des mesures de MRM qu'il prend.
73. La Loi sur le CST interdit au CST d'utiliser les cyberopérations actives (CA) ou les cyberopérations défensives (CD) dans le but de causer, intentionnellement ou par négligence criminelle, des lésions corporelles ou la mort, ou de tenter intentionnellement d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie. De plus, le CST ne peut pas utiliser les CA ou les CD dans le but de recueillir de l'information. Il semble probable, selon le cadre législatif qui régit le CST, que les activités de CA ou de CD entreprises par ce dernier doivent également être en accord avec le droit international concerné.

74. Des renseignements supplémentaires sur le rôle du commissaire au renseignement relativement aux autorisations ministérielles sont disponibles à l'adresse:

<https://www.canada.ca/fr/commissaire-renseignement.html>.

75. Site Web de la Commission civile d'examen et de traitement des plaintes relatives à la GRC,

<https://www.crc-cetp.gc.ca/fr>

76. L'article 18 de la Loi sur la GRC énonce les fonctions des membres de la GRC comme, notamment, assurer l'application des lois et l'exécution des mandats, « le maintien de la paix » et « la prévention du crime ».

77. Dans ce contexte, « les actions » n'incluent pas: les activités menées tout au long du processus de renseignement, les produits du renseignement comme les documents d'information, les rapports et les recommandations, et les activités de protection de l'information classifiée.

78. L'OSSNR a également l'obligation d'examiner les plaintes qui sont portées à son attention par la Commission canadienne des droits de la personne (CCDP), ainsi que celles découlant de rapports ministériels présentés en vertu de la *Loi sur la citoyenneté*. Ces cas sont toutefois très rares.

79. Pour de plus amples renseignements sur le processus d'enquête sur les plaintes de l'OSSNR, y compris la façon de déposer une plainte, veuillez consulter OSSNR (2020), « Plaintes ».

<http://www.nsira-ossnr.gc.ca/cmpplt/index-fra.html>

80. Pour une ventilation statistique, veuillez consulter l'annexe D.

81. Les enquêtes sur les plaintes contre le SCRS dont l'OSSNR a déterminé qu'elle avait compétence sont résumées dans l'annexe C.

82. *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles* (L.C. 2005, ch. 46).

<https://laws-lois.justice.gc.ca/fra/lois/P-31.9/>

83. *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles*, paragraphe 2(1).

84. Voir paragraphe 15(1) de la Loi sur la protection de l'information.

85. Voir paragraphe 15(1) de la Loi sur la protection de l'information.

86. Voir paragraphe 15(5) de la Loi sur la protection de l'information.

87. Lettre de l'OSSNR au procureur général du Canada, le 25 février 2020.

88. Parlement du Canada (2019), « Projet de loi C-59 ».

<https://www.parl.ca/DocumentViewer/fr/42-1/projet-loi/C-59/sanction-royal>

89. Canada (2020), « Engagement de transparence en matière de sécurité nationale ».

<https://www.canada.ca/fr/services/defense/securitenationale/engagement-transparence-securite-nationale.html>

90. OSSNR [@NSIRACanada] <https://twitter.com/nsiracanada?lang=en>

91. Ce processus est en cours et les rapports caviardés seront disponibles sur le site Web de l'OSSNR à l'adresse: <http://27.www.nsira-ossnr.gc.ca/index-fra.html>

92. Les commentaires peuvent être envoyés à la boîte de réception de l'OSSNR à l'adresse: OSSNR (2020) « Contactez-nous ». <http://www.nsira-ossnr.gc.ca/cttctz-fra.html>

93. Tous les rapports corporatifs de l'OSSNR sont disponibles à l'adresse suivante: OSSNR (2020), « Services ministériels ». <http://www.nsira-ossnr.gc.ca/abtprp/cormin-fra.html>