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

National Security and Intelligence Review Agency

Canada

OSSNR

2020 // Rapport Annuel

ISSN 2563-5778
No de catalogue : PS106-9E-PDF

Le 18 octobre 2021

Le très honorable Justin Trudeau, C.P., député
Premier ministre du Canada
Bureau du premier ministre et du Conseil privé
Ottawa (Ontario)
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 deuxième 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 2020, ainsi que nos constatations et nos recommandations.

Conformément à l'alinéa 52(1)b) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement,* notre rapport a été préparé après 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, 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,

L'honorable Marie Deschamps, C.C.

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

Table des matières

Message des membres

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a commencé à œuvrer en 2019 en tant que nouveau mécanisme de responsabilité indépendant au Canada. Notre vaste mandat d'examen et d'enquête porte sur les activités en matière de sécurité nationale et de renseignement des ministères et des organismes du gouvernement fédéral. Dans notre premier rapport annuel, publié en 2020, nous avons discuté de nos activités initiales, de la création de l'OSSNR en juillet 2019 jusqu'à décembre 2019.

Maintenant, nous sommes heureux de présenter notre deuxième rapport annuel, qui porte sur les activités de notre première année complète d'activité. En 2020, nous avons effectué de nombreux examens et enquêtes, consulté les intervenants de l'appareil de la sécurité nationale et du renseignement (y compris nos homologues internationaux), lancé un plan d'examen ambitieux pour les prochaines années, amorcé une réforme complète de notre processus d'enquête sur les plaintes, élaboré une approche uniforme de la vérification de l'information dans les examens (notre approche « faire confiance, mais vérifier »), commencé à normaliser nos processus d'examen et progressé dans l'officialisation des efforts visant à assurer une coordination et à collaborer avec diverses organisations partenaires. De plus, la taille, l'expertise et la capacité administrative, technique et fonctionnelle du Secrétariat de l'OSSNR ont continué d'augmenter à un rythme soutenu. Nous avons réalisé toutes ces activités malgré les contraintes considérables imposées par la pandémie de COVID-19.

Nous nous engageons à faire preuve de transparence, à mobiliser le public, à tenir la population canadienne au courant des activités en matière de sécurité nationale et de renseignement et à veiller à ce que nos plans reflètent les priorités de tous les Canadiens. Notre rapport annuel est un moyen parmi tant d'autres de respecter cet engagement. Nous entendons également atteindre ces buts en mobilisant régulièrement des intervenants, des membres de diverses communautés et des organismes d'examen parallèles à l'échelle internationale, y compris ceux qui font partie du Conseil de surveillance et d'examen du renseignement du Groupe des cinq. De même, nous nous engageons, et avons débuté, à publier des versions publiques de nos rapports dès leur achèvement (notre initiative de « rédaction pour diffusion ») et à fournir des mises à jour en temps opportun sur notre site Web et nos plateformes de médias sociaux.

Après la publication de notre premier rapport annuel, nous avons sollicité les commentaires des intervenants universitaires et de l'appareil. À la suite de ces consultations, nous avons réorganisé la présentation d'une partie du contenu dans notre rapport annuel 2020. Plus particulièrement, nous avons regroupé nos résumés d'examens, y compris les constatations et

les recommandations, selon les institutions auxquelles ils se rapportent. Nous discutons aussi des résultats et des thèmes des examens interorganismes. Par ailleurs, le présent rapport établit un cadre pour la production de rapports statistiques plus rigoureux sur certains aspects des activités du Service canadien du renseignement de sécurité et du Centre de la sécurité des télécommunications, afin de permettre une comparaison d'une année à l'autre.

La pandémie a différé nos plans et les progrès concernant les examens, les enquêtes et les initiatives ministérielles en 2020, comme ce fut le cas pour de nombreux secteurs et industries dans le monde entier. Au moment de la rédaction du présent rapport, notre personnel a commencé à avoir un accès plus régulier à nos bureaux et aux documents classifiés essentiels à notre travail. Un accès fréquent et soutenu nous aidera à effectuer notre travail plus rapidement et efficacement. Nous sommes impatients d'exécuter l'ambitieux programme qui nous attend dans l'année à venir.

Nous tenons à remercier sincèrement le personnel de l'OSSNR pour son dévouement et sa diligence au cours de cette dernière année difficile, ainsi que pour les efforts soutenus qu'il a déployés à bâtir une organisation solide.

Marie Deschamps
Craig Forcese
Ian Holloway
Faisal Mirza
Marie-Lucie Morin

Résumé

1. L'année 2020 a été la première année d'activité complète de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). En vertu de sa vaste compétence prévue par la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, l'OSSNR a mené des examens et des enquêtes sur des questions de sécurité nationale et de renseignement se rapportant non seulement au Service canadien du renseignement de sécurité (SCRS) et au Centre de la sécurité des télécommunications (CST), mais aussi à plusieurs ministères et organismes fédéraux, notamment :
    - le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC);
    - Affaires mondiales Canada (AMC);
    - la Gendarmerie royale du Canada (GRC);
    - Immigration, Réfugiés et Citoyenneté Canada (IRCC);
    - l'Agence des services frontaliers du Canada (ASFC);
    - Transports Canada;
    - l'Agence de la santé publique du Canada;
    - tous les ministères et organismes qui participent à des activités de sécurité nationale et de renseignement dans le cadre des examens annuels de l'OSSNR relatifs à la *Loi sur la communication d'information ayant trait à la sécurité du Canad*a et à la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*.
2. L'Office de surveillance a également axé ses efforts sur la normalisation et la modernisation des processus qui régissent les deux principales fonctions du mandat de l'OSSNR – les examens et les enquêtes – afin de veiller à ce que nos processus soient robustes, clairs et transparents.
3. En 2020, l'organisation a également vu sa taille et sa capacité augmenter, alors qu'elle poursuit ses efforts en vue d'améliorer son expertise technique et son savoir-faire spécialisé.

Points saillants des examens

Service canadien du renseignement de sécurité

4. Au cours de l'année 2020, l'OSSNR a réalisé deux examens qui ont permis d'approfondir sa connaissance d'importants secteurs d'activité du SCRS :

    - L'examen des mesures de réduction de la menace (MRM) du SCRS a révélé que ce dernier s'est acquitté de ses obligations en vertu des directives ministérielles. Toutefois, dans un nombre limité de cas, les MRM du SCRS n'étaient pas « justes et adaptées ».
    - L'examen de l'échange de renseignements entre le SCRS et la GRC sous l'angle d'une enquête en cours a permis de mettre en lumière une importante question non résolue du cadre de la sécurité nationale du Canada : les limites de l'utilisation des renseignements du SCRS à l'appui des enquêtes criminelles de la GRC, concept connu sous le nom de dilemme du « renseignement à la preuve ».

Centre de la sécurité des télécommunications

5. L'OSSNR a effectué trois examens des activités du CST en 2020, notamment :

    - la communication d'information nominative sur un Canadien (INC) par le CST aux ministères du gouvernement du Canada, qui a conclu que 28 % des demandes de divulgation n'étaient pas suffisamment justifiées pour permettre la communication d'INC;
    - les autorisations ministérielles et les arrêtés ministériels en vertu de la Loi sur le CST, qui permettent au CST de mener des activités nécessaires à l'exécution de son mandat qui autrement seraient illégales;
    - les politiques et les procédures de conservation des données relatives au renseignement d'origine électromagnétique (SIGINT) du CST, afin de mieux comprendre le processus de gestion du cycle de vie du SIGINT et la conformité aux limites légales de conservation des données et aux politiques gouvernementales et internes connexes.

Ministère de la Défense nationale et Forces armées canadiennes

6. En 2020, l'OSSNR a effectué un examen du MDN et des FAC, lequel portait sur la façon dont l'Unité nationale de contre-ingérence des Forces canadiennes (UNCIFC) mène ses activités de collecte relative à la contre-ingérence, en mettant particulièrement l'accent sur la façon dont les activités de l'unité s'inscrivent dans les cadres juridiques et de gouvernance.

Affaires mondiales Canada

7. En 2020, l'OSSNR a effectué son premier examen d'AMC qui était axé sur l'un de ses programmes.

Autres examens ministériels

8. L'OSSNR a également entrepris des examens concernant une unité spécialisée de renseignement de la GRC, des examens en vue de mieux comprendre le rôle et les responsabilités en matière de sécurité nationale d'IRCC, ainsi qu'un examen du ciblage des passagers aériens à l'ASFC.

Examens interministériels

9. L'OSSNR a effectué deux examens interministériels obligatoires en 2020 :

    - un examen des directives établies concernant la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*(LCMTIEE);
    - un examen de la communication d'information au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC);

10. L'OSSNR a également entamé un autre examen interministériel en 2020 :

    - un examen visant à répertorier la collecte et l'utilisation des données biométriques dans l'ensemble du gouvernement fédéral dans le cadre des activités relatives à la sécurité et au renseignement.

Points saillants des enquêtes

11. En 2020, l'OSSNR a réformé et modernisé son processus de traitement des plaintes afin d'en favoriser l'efficacité et la transparence. Deux priorités ont guidé ce processus de modernisation, à savoir promouvoir l'accès à la justice pour les plaignants non représentés et la mise en place de procédures plus simples et moins formelles.

12. Dans le cadre de cette réforme, l'OSSNR a créé de nouvelles règles de procédure; pour ce faire, l'OSSNR a mené un vaste exercice de consultation auprès des intervenants des secteurs public et privé afin d'obtenir un produit final aussi efficace et mûrement réfléchi que possible. Les nouvelles règles sont entrées en vigueur le 19 juillet 2021.

13. En 2020, l'OSSNR a également élaboré un nouvel énoncé de politique dans lequel il s'engage à publier des rapports d'enquête caviardés et dépersonnalisés afin de promouvoir et d'améliorer la transparence de ses enquêtes.

01 //

Introduction

1.1 Qui nous sommes

1. Créé en juillet 2019, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) est un organisme indépendant qui relève du Parlement. Avant la création de l'OSSNR, il existait plusieurs lacunes dans le cadre de responsabilisation en matière de sécurité nationale du Canada. Notamment, les organismes d'examen qui ont précédé l'OSSNR n'avaient pas la capacité de collaborer ou d'échanger leur information classifiée; ils pouvaient seulement effectuer des examens pour un ministère ou un organisme donné.
2. En revanche, l'OSSNR a le pouvoir de surveiller de manière intégrée toutes les activités en matière de sécurité nationale et de renseignement au sein du gouvernement du Canada. Comme l'a souligné le rapport annuel 2019 de l'organisme, grâce au rôle élargi de l'OSSNR, le Canada dispose maintenant de l'un des systèmes d'examen indépendant de la sécurité nationale les plus complets au monde[1].

1.2 Mandat

3. L'OSSNR a le double mandat de mener des examens et des enquêtes sur les activités en matière de sécurité nationale et de renseignement du Canada. L'annexe B contient un aperçu financier et administratif de l'OSSNR.

Examens

4. Le mandat d'examen de l'OSSNR est vaste, comme le stipule le paragraphe 8(1) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (Loi sur l'OSSNR)[2]. Il comprend l'examen des activités du Service canadien du renseignement de sécurité (SCRS) et du Centre de la sécurité des télécommunications (CST), ainsi que des activités liées à la sécurité nationale ou au renseignement de tous les autres ministères et organismes fédéraux. Cela comprend, sans toutefois s'y limiter, les activités en matière de sécurité nationale ou de renseignement de la Gendarmerie royale du Canada (GRC), de l'Agence des services

frontaliers du Canada (ASFC), du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC), d'Affaires mondiales Canada (AMC) et du ministère de la Justice. De plus, l'OSSNR examine toute question liée à la sécurité nationale ou au renseignement dont l'OSSNR est saisi par un ministre de la Couronne. L'annexe C décrit le cadre d'examen de l'OSSNR.

5. Les examens de l'OSSNR ont pour but de déterminer si les activités du Canada en matière de sécurité nationale et de renseignement sont conformes aux lois et aux directives ministérielles applicables et si elles sont raisonnables et nécessaires. Dans le cadre de ses examens, l'OSSNR peut formuler toute conclusion ou recommandation qu'il juge appropriée.

6. Les examens du SCRS et du CST demeureront toujours au cœur des efforts de l'OSSNR, puisque la mission de ces organisations consiste entièrement à traiter des questions liées à la sécurité nationale et au renseignement. Toutefois, contrairement aux organismes d'examen qui l'ont précédé, l'OSSNR a un mandat d'examen dont la portée est globale. L'OSSNR continuera aussi de considérer comme une priorité l'examen des autres ministères qui participent à des activités de sécurité nationale et de renseignement pour vérifier s'ils respectent leurs obligations. Les examens de l'OSSNR contribuent à tenir le Parlement et la population canadienne au fait du caractère licite et raisonnable des activités du Canada en matière de sécurité nationale et de renseignement.

Enquêtes

7. En plus de son mandat d'examen, l'OSSNR a la responsabilité d'enquêter sur les plaintes liées à la sécurité nationale ou au renseignement. Cette obligation est énoncée à l'alinéa 8(1)d) de la Loi sur l'OSSNR et consiste à enquêter sur les plaintes concernant :

    - les activités du SCRS ou du CST;
    - les décisions de refuser ou de révoquer certaines habilitations de sécurité du gouvernement fédéral;
    - les rapports ministériels présentés en vertu de la *Loi sur la citoyenneté* qui recommandent le refus de certaines demandes de citoyenneté.

8. Ce mandat consiste également à enquêter sur les plaintes relatives à la sécurité nationale transmises par la Commission civile d'examen et de traitement des plaintes relatives à la GRC (le mécanisme de traitement des plaintes de la GRC)[3] et la Commission canadienne des droits de la personne.

1.3 Rapports annuels au Parlement

9. Chaque année civile, l'OSSNR a l'obligation légale de présenter au premier ministre un rapport sur ses activités de l'année précédente, ainsi que ses constatations et recommandations[4].

Rapport annuel 2019

10. Le premier rapport annuel de l'OSSNR (Rapport annuel 2019) couvrait la période de six mois allant de la création de l'OSSNR en juillet 2019 à la fin de 2019. Dans ce rapport, l'OSSNR a discuté des examens et des enquêtes qu'il avait réalisés ou entamés en 2019, ainsi que de ses constatations et recommandations connexes. L'OSSNR a également publié les résultats d'examens qui n'avaient pas encore été rendus publics par les organismes qui l'ont précédé, soit le Comité de surveillance des activités de renseignement de sécurité (CSARS) et le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST)[5].

11. Le *Rapport annuel 2019* a également présenté les constatations de l'OSSNR selon un nouveau cadre appelé le « continuum de l'information ». Étant donné la portée globale et exhaustive du mandat d'examen de l'OSSNR, ce cadre offre une optique qui aide à comprendre les principaux thèmes, tendances et défis liés à la sécurité nationale et au renseignement qu'ont en commun les ministères et organismes du gouvernement fédéral. Cette optique permet de discuter des préoccupations communes en ce qui concerne l'architecture globale de sécurité et de renseignement du Canada, d'éclairer les priorités des examens futurs et de formuler des recommandations visant à régler les problèmes. Le continuum de l'information est abordé plus en détail à la section 2.1[6].

Rapport annuel 2020

12. En réponse aux commentaires reçus de différents intervenants, le deuxième rapport annuel de l'OSSNR regroupe les résumés d'examens par ministère, ainsi que pour le SCRS et le CST. Néanmoins, l'OSSNR reste déterminé à présenter des thèmes et des observations d'ordre plus général concernant la responsabilisation en matière de sécurité nationale et de renseignement dans l'ensemble du Canada.

13. Dans le *Rapport annuel 2020*, nous présentons donc :

- l'approche « faire confiance, mais vérifier » de l'OSSNR, mise au point pour garantir que l'OSSNR a accès en temps opportun à toute l'information pertinente lors de l'examen des ministères et des organismes;
- une mise à jour concernant les plans de l'OSSNR visant à poursuivre la présentation des analyses d'examens dans l'optique du « continuum de l'information »;
- des résumés des examens de l'OSSNR portant sur le SCRS, le CST et d'autres ministères et organismes réalisés en 2020 ou toujours en cours, dont le contexte est présenté dans la section suivante et résumé à l'annexe D, ainsi que des constatations et des recommandations détaillées à l'annexe E[7];
- des données sur le CST et liées à la conformité de ses activités afin de favoriser une plus grande transparence en la matière;
- les prochains examens de ministères et d'organismes prévus par l'OSSNR, notamment pour éclairer l'examen parlementaire triennal de la *Loi de 2017 sur la sécurité nationale*, qui devrait commencer en 2022;
- des résumés des enquêtes sur les plaintes réalisées en 2020 ou toujours en cours;
- un aperçu du nouveau processus modernisé de l'OSSNR de traitement des plaintes, résultat d'un vaste projet de réforme;
- les statistiques concernant les enquêtes de l'OSSNR sur les plaintes en 2020 figurent à l'annexe F.

1.4 Valeurs et objectifs

14. L'OSSNR s'engage à :

- faire preuve d'ouverture et de transparence pour tenir les Canadiens au fait du caractère licite et raisonnable des activités de notre pays en matière de sécurité nationale et de renseignement;
- prévoir les différents risques qui font partie du mandat de chacune des entités examinées;
- être objectif et indépendant, et être perçu comme tel;
- maintenir l'excellence des méthodes pour assurer la rigueur et la qualité de l'approche de l'OSSNR;
- mobiliser régulièrement les partenaires, les intervenants et les membres de l'appareil;
- favoriser la réflexion prospective et la pensée novatrice pour se tenir au courant et, idéalement, demeurer à l'avant-garde des nouvelles technologies et d'un environnement de sécurité nationale en constante évolution.

15. Dans le cadre de son engagement envers l'excellence des méthodes, l'OSSNR a mis au point l'approche « faire confiance, mais vérifier » (présentée ci-dessous), élaborée pour permettre à l'OSSNR d'avoir un niveau élevé de confiance en l'exhaustivité de l'information reçue des ministères et des organismes.

16. En 2020, le Secrétariat de l'OSSNR a également débuté l'élaboration d'un code de conduite pour tous les employés, qui a été achevé en juin 2021. Le code énonce les valeurs organisationnelles qui orientent les activités et les fonctions de l'effectif ainsi que les normes qu'une personne doit respecter pendant et après son emploi au Secrétariat de l'OSSNR[8].

17. L'annexe G contient des renseignements supplémentaires sur les valeurs et les objectifs de l'OSSNR liés à la transparence, à l'anticipation des risques, à l'objectivité et à l'indépendance, à l'excellence des méthodes, à la mobilisation des intervenants et des membres de l'appareil ainsi qu'à la réflexion prospective et à la pensée innovatrice.

1.5 Faire confiance, mais vérifier

18. La Loi sur l'OSSNR accorde à l'OSSNR des droits d'accès étendus à l'information : à l'exception des documents confidentiels du Cabinet, l'OSSNR a le droit d'avoir accès en temps opportun à tout renseignement en la possession ou sous le contrôle d'un ministère. Lorsque l'OSSNR mène des examens et des enquêtes, il a besoin d'accéder rapidement à un large éventail d'information, de personnes et d'actifs. Pour ce faire, il faut le soutien régulier d'unités de liaison spécialisées qui peuvent fournir des documents, organiser des séances d'information, répondre à des questions et, de façon générale, orienter et mettre en œuvre les exigences de l'OSSNR en matière d'accès. Les retards dans la réception de l'information peuvent nuire à la capacité de l'OSSNR de mener à bien son mandat.

19. En tant qu'organisme d'examen, l'OSSNR doit pouvoir garantir au Parlement – et par son entremise, aux Canadiens – son niveau élevé de confiance en l'exhaustivité de l'information reçue des ministères et des organismes et, par conséquent, en la fiabilité de ses constatations. L'approche « faire confiance, mais vérifier » est un outil essentiel pour atteindre cet objectif.

20. L'OSSNR reconnaît, d'une part, que le principe de la confiance exige que chaque partie comprenne et apprécie le mandat de l'autre et ait confiance en son intégrité. Bien sûr, dans un contexte d'examen, il y aura nécessairement des tensions saines découlant de différences de points de vue.

21. D'autre part, la vérification est une condition indispensable à la crédibilité de tout examen. L'OSSNR doit être en mesure de vérifier de façon indépendante l'exhaustivité de l'information qu'il reçoit.

22. À l'avenir, l'OSSNR mettra en œuvre un processus d'« accès sur mesure » pour la vérification. L'accès sur mesure consiste à déterminer les besoins en matière d'accès à l'information en fonction de l'examen ou de l'enquête à effectuer, et à collaborer avec les ministères et les organismes afin de déterminer quels sont les différents types d'accès qui constitueront la meilleure façon d'obtenir cette information. Le processus d'accès sur mesure peut inclure un accès ciblé aux réseaux et aux renseignements informatiques, un accès par la voie d'un intermédiaire, un espace de bureau réservé et l'accès au matériel de formation.

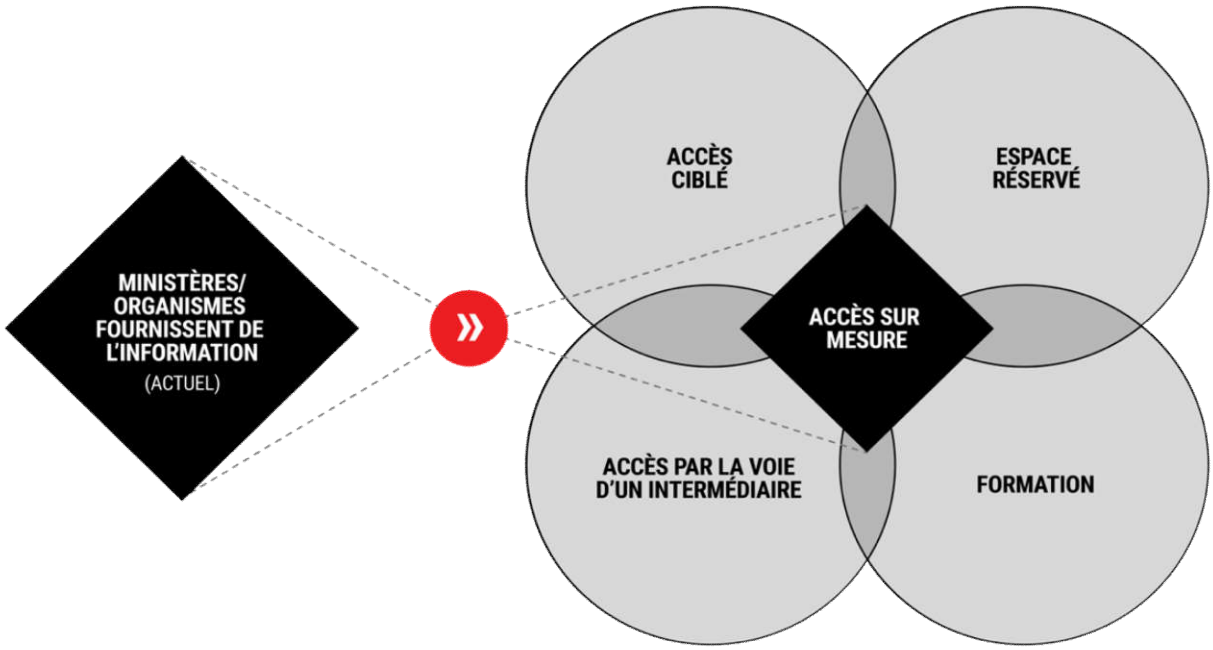
    - L'accès ciblé permet d'avoir directement accès aux réseaux informatiques ou à l'information de nature délicate d'un ministère ou d'un organisme. L'accès ciblé est la méthode par excellence pour garantir une vérification robuste de l'information reçue dans le cadre de l'approche « faire confiance, mais vérifier ».
    - L'accès par la voie d'un intermédiaire fait intervenir l'intermédiaire d'un ministère ou d'un organisme qui accède aux dépôts centraux des sources d'information en présence du personnel de l'OSSNR, qui peut alors examiner l'information pertinente telle qu'elle apparaît dans le système.
    - Le fait d'avoir un espace réservé dans les bureaux des ministères ou des organismes, de façon temporaire ou permanente, permet d'échanger de l'information plus rapidement et sécuritairement.
    - L'accès au matériel de formation implique d'accéder aux modules de formation des ministères ou des organismes portant sur des politiques organisationnelles pertinentes et d'autres sujets pour que l'OSSNR puisse acquérir des connaissances particulières.

23. Les processus d'accès sur mesure peuvent imposer des contraintes sur le plan de la logistique et des ressources aux ministères et aux organismes qui doivent les mettre en œuvre et peuvent nécessiter un changement de culture. Dans l'ensemble, cependant, l'accès sur mesure est mutuellement avantageux pour les parties. Les processus d'accès sur mesure peuvent accroître la transparence et la responsabilisation de toutes les parties, permettre d'accéder à l'information de façon sécuritaire et rapide, favoriser des interactions professionnelles positives, améliorer l'expertise globale et renforcer les constatations et les recommandations fondées sur des données probantes. De plus, l'OSSNR croit que l'accès sur mesure permettra, au fil du temps, de réduire la charge de travail du personnel de liaison des ministères et des organismes visés par un examen.

24. L'approche « faire confiance, mais vérifier » n'est pas nouvelle. L'OSSNR et son prédécesseur, le CSARS, ont déjà eu des ententes d'accès sur mesure de longue date avec le SCRS qui permettaient d'avoir un accès ciblé (direct) aux réseaux informatiques et à l'information de nature délicate du SCRS.

25. Le principe « faire confiance, mais vérifier » est un aspect essentiel du maintien de l'intégrité et de la crédibilité des examens effectués par l'OSSNR. Conformément à l'engagement de l'OSSNR envers la transparence et la rigueur méthodologique, ses examens contiendront un « énoncé de confiance » pour indiquer le niveau de confiance de l'OSSNR en l'exhaustivité de l'information sur laquelle ses constatations s'appuient, compte tenu de la capacité de l'OSSNR à la vérifier. L'énoncé de confiance est un outil important pour informer les ministres, le Parlement et les membres du public de la mesure dans laquelle l'OSSNR a pu accéder à toute l'information pertinente.

Fig. 1 Accès sur mesure



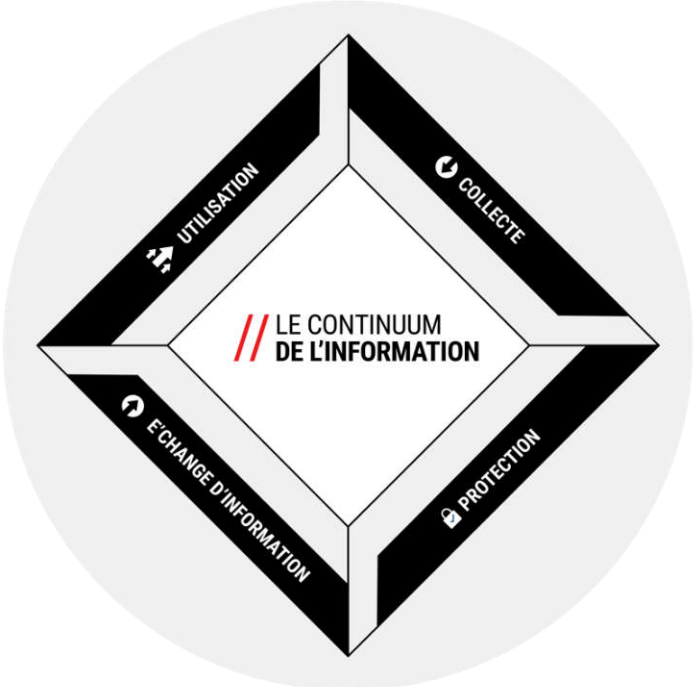
02 //

Examen

2.1 Le continuum de l'information

1. Comme il a été mentionné précédemment, le mandat d'examen de l'OSSNR s'étend à l'ensemble du gouvernement fédéral. La compétence élargie de l'OSSNR lui permet non seulement d'examiner les activités de sécurité nationale et de renseignement d'une organisation donnée, mais aussi de cerner les thèmes communs qui ressortent à l'échelle du gouvernement.
2. Dans le *Rapport annuel 2019*, l'OSSNR a présenté un cadre pour appuyer la discussion de ces tendances et leur analyse. Le « continuum de l'information » identifie quatre étapes principales au cours desquelles des problèmes peuvent survenir dans le cycle de vie de l'information sur la sécurité nationale et le renseignement: la collecte, la protection, l'échange d'information et l'utilisation de l'information à des fins concrètes[9].

Fig. 2 Le continuum de l'information



3. Dans un environnement en constante évolution, y compris le développement rapide de nouvelles technologies, chaque étape présente des défis potentiels pour les ministères et les organismes qui participent à des activités liées à la sécurité nationale et au renseignement. Malgré ces défis, toutes les activités en matière de sécurité nationale et de renseignement doivent être conformes aux lois et aux directives ministérielles applicables et satisfaire aux critères de la raisonnabilité et de la nécessité.

4. Le *Rapport annuel 2019* a également établi un certain nombre de priorités à venir pour lesquelles une analyse dans l'optique du continuum de l'information serait utile. Pour atteindre ces buts, l'OSSNR a promis d'investir dans le développement d'une expertise technologique interne, de collaborer avec les organismes de responsabilisation alliés à travers de sa collaboration avec le Conseil de surveillance et d'examen des activités de renseignement du Groupe des cinq, et de chercher à se tenir à jour en ce qui concerne les technologies nouvelles et émergentes, tels l'intelligence artificielle, l'apprentissage machine, l'informatique quantique et les « mégadonnées ».

5. L'OSSNR s'est également engagé à continuer de travailler de concert 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 afin de s'assurer que le plus vaste éventail de perspectives soient pris en compte.

6. L'OSSNR continue d'examiner les activités liées à la sécurité nationale et au renseignement dans l'optique du continuum de l'information et prévoit présenter les travaux sur son site Web à l'aide de cette approche afin d'aider à situer les thèmes horizontaux aux fins des examens en matière de sécurité nationale. Toutefois, pour 2020, ce rapport s'appuie sur des commentaires que l'OSSNR a reçus concernant le rapport annuel de l'année dernière et utilise une approche plus institutionnelle comme trame narrative[10].

2.2 Réalité de la surveillance en situation de pandémie

7. Tel que noté dans le *Rapport annuel 2019*, le personnel de l'OSSNR a continué de travailler à distance en 2020, ce qui a impliqué un accès limité au bureau et, par conséquent, un accès minimal aux documents classifiés physiques et électroniques qui doivent être sauvegardés dans un espace sécurisé et qui sont essentiels au travail de l'Office de surveillance. L'OSSNR a dû s'adapter aux réalités de la pandémie, comme toutes les organisations. L'OSSNR a revu ses plans d'examen et a établi des

horaires rotatifs stricts afin de permettre un accès limité au bureau pour le travail classifié, de manière à continuer de respecter en toute sécurité ses obligations législatives et ses engagements envers les Canadiens.

2.3 Examen parlementaire de la *Loi de 2017 sur la sécurité nationale*

8. La *Loi de 2017 sur la sécurité nationale*, qui a constitué l'OSSNR et apporté des modifications majeures au cadre de la sécurité nationale du Canada, contient des dispositions qui exigent un examen approfondi au cours de la quatrième année du fonctionnement de l'OSSNR, qui sera en 2022. Cet examen approfondi obligera le Parlement à évaluer les effets de la *Loi de 2017 sur la sécurité nationale* sur les opérations du Service canadien du renseignement de sécurité (SCRS), de la Gendarmerie royale du Canada (GRC) et du Centre de la sécurité des télécommunications (CST) liées à la sécurité nationale, au partage d'information et à l'interaction de ces organisations avec l'OSSNR, le Bureau du commissaire au renseignement et le CPSNR[11].

9. L'OSSNR a structuré et ordonné son plan d'examen afin d'éclairer l'examen parlementaire des nouveaux pouvoirs accordés aux organismes de sécurité en vertu de la *Loi de 2017 sur la sécurité nationale*. Ces nouveaux pouvoirs seront examinés au cours de 2021 et au début de 2022 afin de déterminer si leur exercice était conforme à la loi et aux directives ministérielles et s'il était raisonnable et nécessaire.

2.4 Examens visant le SCRS

Aperçu

10. En vertu de la Loi sur l'OSSNR, l'OSSNR a le mandat d'examiner toute activité du SCRS. La Loi sur l'OSSNR exige que l'OSSNR présente au ministre de la Sécurité publique et de la Protection civile un rapport annuel sur les activités du SCRS pour chaque année civile qui porte notamment sur le respect par le SCRS de la loi et des directives ministérielles applicables ainsi que sur le caractère raisonnable et la nécessité de l'exercice par celui-ci de ses pouvoirs[12].

11. En 2020, l'OSSNR a complété deux examens visant le SCRS, qui sont résumés ci-dessous. L'OSSNR a également commencé deux autres examens : un examen des programmes technologiques et des techniques de collecte de renseignement du

SCRS et un examen de l'obligation de franchise que le SCRS et le ministère de la Justice doivent respecter dans le cadre des procédures de mandat devant la Cour fédérale. D'autres examens en cours de l'OSSNR, y compris les examens de multiples organismes, comportent un volet lié au SCRS.

Mesures de réduction de la menace

12. En vertu de la *Loi antiterroriste* (2015), le SCRS s'est vu conférer le pouvoir de prendre des mesures de réduction de la menace (MRM). L'OSSNR est tenu d'examiner, annuellement, au moins un aspect de la prise, par le SCRS, de mesures pour réduire les menaces envers la sécurité du Canada[13].

13. Il s'agissait du premier examen de l'OSSNR portant sur le mandat du SCRS en matière de réduction de la menace. Il comprenait un examen détaillé de la conformité au droit d'un échantillon de MRM prises en 2019. L'examen comprenait également une analyse générale de la prise de MRM par le SCRS au cours des cinq dernières années afin de cerner les tendances et d'éclairer le choix de l'OSSNR quant aux sujets des examens futurs.

14. L'échantillon examiné par l'OSSNR était constitué de MRM qui avaient été employées pour contrer les menaces visant les institutions démocratiques canadiennes dans le cadre des élections fédérales de 2019. L'OSSNR a évalué les mesures en fonction des exigences législatives et des politiques, ainsi qu'en fonction des directives ministérielles.

15. Pour toutes les mesures examinées, l'OSSNR a constaté que le SCRS avait rempli ses obligations en vertu des directives ministérielles; notamment, le SCRS a consulté ses partenaires gouvernementaux et a complété une évaluation des risques opérationnels, politiques, juridiques et en matière de relations étrangères pour chaque MRM.

16. Pour la plupart des mesures prises par le SCRS, l'OSSNR a noté que ces mesures respectaient les exigences de la *Loi sur le Service canadien du renseignement de sécurité* (Loi sur le SCRS). Toutefois, l'OSSNR a également observé que, dans un nombre limité de cas, le SCRS a choisi d'inclure des individus dans une MRM sans qu'il y ait de lien rationnel entre la personne choisie et la menace. Par conséquent, ces mesures n'étaient pas « justes et adaptées » comme l'exige la Loi sur le SCRS[14].

17. Il y a un type de MRM examiné par l'OSSNR pour lequel le SCRS a jugé qu'un mandat n'était pas nécessaire. L'OSSNR est préoccupé par les facteurs qui exigerait que le SCRS tienne pleinement compte des répercussions de la *Charte canadienne des droits*

et libertés sur ces mesures, et pourrait exiger du SCRS qu'il obtienne des mandats avant de prendre certaines mesures.

18. Enfin, l'OSSNR a relevé certaines incohérences dans le type d'information fournie aux décideurs du SCRS dans les demandes d'approbation internes. De plus, l'OSSNR a également constaté des lacunes et des incohérences dans la documentation du SCRS, qui ont nui à l'examen de la conformité. Par conséquent, l'OSSNR a recommandé l'élaboration de processus officiels et documentés pour la gestion de toute l'information liée aux MRM. L'OSSNR a également recommandé que tous les faits pertinents relatifs aux MRM soient officiellement remis au Groupe litiges et conseils en sécurité nationale (GLCSN), lequel fait partie du Ministère de la Justice, afin de s'assurer que ce dernier dispose de l'information nécessaire pour fournir des avis juridiques éclairés.

19. Les questions juridiques soulevées dans le cadre de cet examen, ainsi que l'analyse des tendances au cours des cinq dernières années, tracent la voie à suivre pour les prochains examens de l'OSSNR. Plus précisément, l'OSSNR a été frappé par le potentiel d'une classe de MRMs à affecter les droits et libertés protégés par la *Charte*. À l'avenir, l'OSSNR accordera une attention particulière à cette catégorie de MRM et aux risques juridiques connexes. L'OSSNR note également que le SCRS n'a pas encore pris de MRM sous l'autorisation d'un mandat émis par la Cour. Si le SCRS obtient un mandat de MRM, l'OSSNR l'examinera en priorité.

Réponse aux recommandations de l'OSSNR

20. Les recommandations de l'OSSNR, la réponse de la direction du SCRS et d'autres détails concernant cet examen figurent à l'annexe E du présent rapport.

Relation entre le SCRS et la GRC dans une région du Canada dans l'optique d'une enquête en cours

21. Le SCRS et la GRC doivent collaborer et échanger des renseignements pour contrer efficacement les menaces à la sécurité nationale[15]. L'OSSNR a examiné l'état de la relation entre le SCRS et la GRC dans l'optique d'une enquête en cours dans une région donnée du Canada. L'OSSNR a entrepris une étude approfondie des activités des deux organismes, en portant une attention particulière à la façon dont ils ont collaboré à cette enquête au cours des dernières années, tant dans la région donnée qu'à l'échelle de l'administration centrale. Bien que les constatations de cet examen soient propres à l'enquête en question, l'OSSNR n'a aucune raison de croire que

l'enquête en question est atypique, et par conséquent, cet examen donne un aperçu de l'état plus général de la relation entre les deux organismes.

22. En ce qui concerne l'enquête du SCRS en particulier, l'OSSNR a observé que le SCRS dépendait de renseignements limités et qu'il était donc vulnérable et que des facteurs externes sont apparus, limitant fortement la capacité du SCRS à recueillir des renseignements sur la menace en question, ce qui a entraîné des lacunes en matière de collecte.

23. L'OSSNR a constaté que dans la région en question, le SCRS et la GRC ont établi une relation solide qui a favorisé l'efficacité de l'harmonisation tactique des activités opérationnelles. Néanmoins, des contraintes technologiques ont rendu l'harmonisation des activités entre le SCRS et la GRC dans la région excessivement lourde et chronophage.

24. L'utilisation par la GRC d'information transmise par le SCRS à l'appui de poursuites criminelles est depuis longtemps limitée par les risques perçus d'impliquer le SCRS ou son information dans une poursuite. À ce sujet, l'OSSNR a constaté une réticence générale de la part du SCRS et de la GRC à lier l'information du SCRS à une enquête de la GRC. Dans le cas de l'enquête régionale en question, les renseignements du SCRS n'avaient pas été communiqués ni utilisés d'une manière contribuant à faire progresser de façon importante les enquêtes de la GRC.

25. Dans l'ensemble, l'OSSNR a constaté que le SCRS et la GRC avaient fait peu de progrès pour contrer la menace visée par l'enquête. De plus, le SCRS et la GRC n'avaient pas de stratégie complémentaire pour lutter contre cette menace.

26. L'OSSNR a le pouvoir légal d'évaluer les activités conjointes du SCRS et de la GRC de la perspective des deux parties, et n'est pas limité à celle du SCRS, comme c'était le cas pour le Comité de surveillance des activités de renseignement de sécurité (CSARS). Cet examen régional a révélé un problème important dans le cadre de la sécurité nationale du Canada qui n'est toujours pas réglé : les limites de l'utilisation des renseignements du SCRS à l'appui des enquêtes criminelles de la GRC, concept souvent appelé le dilemme du « renseignement à la preuve ». Étant donné la place centrale qu'occupe la relation entre le SCRS et la GRC dans l'architecture de sécurité nationale du Canada, l'OSSNR se penchera à nouveau sur ce sujet dans les années à venir.

Réponse aux recommandations de l'OSSNR

27. Les recommandations de l'OSSNR, la réponse de la direction du SCRS et d'autres détails concernant cet examen figurent à l'annexe E du présent rapport.

Statistiques et données

28. Pour accroître la responsabilisation à l'égard du public, l'OSSNR demande au SCRS de publier des statistiques et des données liées aux aspects d'intérêt public et à la conformité de ses activités. L'OSSNR est d'avis que les statistiques suivantes permettront de renseigner le public sur la portée et l'ampleur des opérations du SCRS, ainsi que sur l'évolution des activités d'une année à l'autre.

    Le nombre de demandes de mandat en vertu de l'article 21 a) approuvées et b) rejetées; chaque catégorie est ensuite ventilée afin d'indiquer s'il s'agit d'une nouvelle demande, d'une demande de remplacement ou bien d'une demande supplémentaire.

    - Nombre de demandes de mandat en vertu de l'article 21 approuvées : 15
    - Nouvelles demandes : 2
    - Demandes de remplacement : 8
    - Demandes supplémentaires : 5
    - Nombre de demandes de mandat en vertu de l'article 21 rejetées : 0

    Le nombre de demandes de mandat en vertu de l'article 21.1 a) approuvées et b) rejetées; chaque catégorie est ensuite ventilée afin d'indiquer s'il s'agit d'une nouvelle demande, d'une demande de remplacement ou bien d'une demande supplémentaire.

    - Aucune demande de mandat en vertu de l'article 21.1 n'a été faite.

    Le nombre de cibles du SCRS

    - 360 cibles

    Le nombre d'ensembles de données accessibles au public a) évalués et b) conservés.

    - Six ensembles de données accessibles au public ont été évalués et conservés en vertu des articles 11.07 et 11.11.

    **Il convient de noter que l'un d'entre eux a été recueilli à la fin de 2019, mais qu'il a été évalué en 2020.*

Le nombre d'ensembles de données canadiens a) évalués et b) conservés après avoir reçu l'autorisation de la Cour, et le nombre de demandes de ce type rejetées.

- Aucun ensemble de données canadien n'a été évalué, ni fait l'objet d'une demande, ni conservé au cours de l'année civile 2020.

Le nombre d'ensembles de données étrangers a) évalués et b) conservés après avoir reçu l'autorisation du ministre et du commissaire au renseignement, et le nombre de demandes de ce type rejetées (soit par le ministre ou le commissaire au renseignement).

- Aucun ensemble de données étranger n'a été évalué au cours de l'année civile 2020. (Toutes les demandes en attente ont été évaluées en 2019.)
- Un ensemble de données étranger a été conservé au cours de l'année civile 2020 après avoir reçu l'autorisation du ministre (autorisation déléguée au Directeur du SCRS comme personne désignée) le 18 novembre 2020 et approuvé par le commissaire au renseignement (16 décembre 2020). (La demande a été évaluée en 2019.)
- Aucune demande d'ensemble de données étranger n'a été rejetée par le ministre ou le commissaire au renseignement au cours de l'année civile 2020.

Le nombre de MRM a) approuvées et b) exécutées.

- Approuvées : 11
- Exécutées : 8

Le nombre a) d'approbations et b) d'invocations en vertu du cadre de justification.

- Désignations en situation d'urgence en vertu du paragraphe 20.1(8) : 0
- Autorisations données en vertu du paragraphe 20.1(12) : 147
- Rapports écrits soumis en vertu du paragraphe 20.1(23) : 123 (ce chiffre comprend 39 commissions par des employés et 84 directives)

Le nombre d'incidents de conformité internes du SCRS.

- En 2020, la Direction de l'examen externe et de la conformité a traité 50 incidents de conformité. Parmi ceux-ci, 29 ont été considérés comme étant d'ordre administratif, 14 étaient liés aux conditions des mandats et 7 étaient liés aux politiques, procédures ou directives internes.

Difficultés générales en matière de conformité : politiques opérationnelles désuètes

29. En raison de l'évolution des environnements juridique et opérationnel au fil des années, l'ensemble des politiques et des procédures internes régissant les opérations du SCRS est devenu désuet. Ces politiques et procédures opérationnelles sont le moyen par lequel les limites imposées aux activités du SCRS par la loi et les directives ministérielles sont transposées dans la pratique quotidienne.

30. L'OSSNR, et auparavant le CSARS, ont tous deux exprimé des préoccupations au sujet des politiques et des procédures désuètes dans leurs rapports et les examens au fil des ans. Le SCRS reconnaît également ces préoccupations, mais a eu du mal à affecter les ressources nécessaires et à accorder de la priorité au renouvellement de l'ensemble de ses politiques opérationnelles. Il en résulte un ensemble confus d'anciennes et de nouvelles politiques et de directives particulières qui n'ont pas encore été intégrées aux politiques. Au cours des deux dernières années, le SCRS a signalé que plus de 150 de ses documents reliés aux politiques opérationnelles devaient être étoffés, mis à jour ou révisés en profondeur.

31. Les politiques et les procédures écrites qui ne reflètent pas les réalités opérationnelles et les obligations légales – ou qui sont simplement incohérentes entre elles – augmentent le risque que le SCRS ne respectera pas les lois et les directives ministérielles. Les employés du SCRS devraient toujours disposer d'un ensemble de politiques et de procédures claires, uniformes et à jour qui facilitent la conformité.

32. L'OSSNR est au courant des efforts soutenus du SCRS pour réviser et organiser l'ensemble de ses politiques et procédures opérationnelles. Comme l'arriéré perdure depuis des années, il est difficile de déterminer si les récents efforts de renouvellement sont assortis de ressources suffisantes pour vraiment remédier à la situation en temps opportun.

Conformité interne et divulgation proactive à l'OSSNR

En 2020, le SCRS a divulgué de façon proactive à l'OSSNR un problème de conformité lié à certaines activités opérationnelles. Après que ses employés ont exprimé des préoccupations au sujet d'un programme opérationnel, le SCRS a effectué un examen interne de la conformité. L'examen initial portait sur le respect des politiques et des procédures du SCRS, mais alors qu'il étudiait la question, le SCRS a décidé de mener une évaluation juridique. Depuis, le SCRS a pris diverses mesures pour remédier aux lacunes qu'il a relevées, notamment l'amélioration de la gouvernance opérationnelle et de la responsabilisation de la gestion. L'OSSNR a eu droit à une séance d'information complète sur la question au début de 2021; de plus, le SCRS fournit – et s'est engagé à continuer de fournir – à l'OSSNR l'ensemble des documents internes pertinents. L'OSSNR examine ces documents avec intérêt et assurera un suivi auprès du SCRS, au besoin.

Cet incident illustre la façon dont les mécanismes de conformité ministériels et le mandat d'examen externe de l'OSSNR peuvent se compléter. Nous encourageons le SCRS à continuer de faire appel à l'OSSNR lorsque des problèmes notables de conformité interne sont constatés.

Plan d'examen du SCRS de 2021

33. En 2021, l'OSSNR entreprendra ou mènera trois examens consacrés exclusivement au SCRS, un examen consacré au SCRS et au ministère de la Justice, et quelques examens interorganismes comportant un volet lié au SCRS. Ces examens sont résumés ci-dessous.

34. En plus des deux examens obligatoires de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) et de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, l'OSSNR a entrepris ou prévoit réaliser les examens suivants sur le SCRS, qui devraient être achevés en 2021 :

Étude des nouveaux programmes technologiques et des nouvelles techniques de collecte de renseignements

Cet examen, entrepris en 2020, comprend une vaste étude sur les programmes technologiques et les techniques de collecte de renseignements du SCRS, avec une emphase particulière sur ceux qui nécessitent un mandat de la Cour. L'examen permettra de cerner des technologies ou des

techniques d'enquête précises qui méritent d'être examinées ultérieurement en raison de leur nouveauté, de leur caractère potentiellement intrusif ou des risques potentiels qu'elles posent en matière de conformité. Une fois cernées, ces technologies ou ces techniques seront examinées au cours des années suivantes afin de s'assurer qu'elles sont conformes aux lois.

Examen découlant de la décision de la Cour fédérale dans 2020 CF 616

Cet examen découle de la décision de la Cour fédérale dans *2020 CF 616*[16]. Afin de bien cerner les lacunes et les défaillances systémiques, culturelles et relatives à la gouvernance qui pourraient être à l'origine du manquement constaté par la Cour, l'OSSNR a entrepris un vaste programme d'examen des documents et de séances d'information avec le SCRS et le ministère de la Justice. L'OSSNR mène également des entrevues confidentielles avec des employés du SCRS et du ministère de la Justice, à divers niveaux, afin de mieux comprendre la dynamique qui oriente la prise de décisions dans les deux ministères et les interactions entre eux. De plus, l'OSSNR a consulté des experts externes dans la mesure du possible. Cet examen est différent des autres que l'OSSNR a effectués, puisqu'il est mené par deux membres de l'OSSNR : Marie Deschamps et Craig Forcese. Le rapport définitif devrait être achevé à la fin de 2021 ou au début de 2022.

35. Après 2021, l'OSSNR a l'intention d'étudier, dans ses examens du SCRS, des sujets tels que :

- la directive ministérielle établie à l'intention du SCRS;
- la collecte de renseignements du SCRS sur l'ingérence étrangère;
- les ensembles de données du SCRS;
- le régime de justification du SCRS pour les activités de collecte de renseignements.

Accès

36. L'éventail d'information que le SCRS doit fournir de façon proactive à l'OSSNR s'est élargi en vertu des modifications apportées à la Loi sur le SCRS. L'OSSNR doit être informé des questions concernant l'utilisation d'ensembles de données par le SCRS, les mesures de réduction de la menace, la communication d'information et le nouveau cadre de justification des activités par ailleurs illégales. Étant donné que ces exigences sont intégrées à la Loi sur le SCRS[17], l'OSSNR croit comprendre que le Parlement prévoyait que l'OSSNR se tienne continuellement au courant de ces activités. À cette fin, l'OSSNR surveillera systématiquement l'information reçue du SCRS pour vérifier sa conformité à la loi ainsi que le caractère raisonnable et la nécessité de ces activités.

37. Toutefois, l'OSSNR estime qu'il est essentiel que le SCRS le tienne également informé des activités autres que celles que le SCRS est explicitement tenu de porter à son attention. L'OSSNR travaille avec le SCRS en vue d'établir un processus qui s'appuie sur l'accès direct existant de l'OSSNR aux principales bases de données du SCRS. Ce processus permettra à l'OSSNR d'obtenir de l'information complémentaire à celle que le SCRS est tenu de lui communiquer.

38. Cette initiative permettra non seulement d'enrichir le contenu des rapports publics annuels de l'OSSNR, mais aussi d'éclairer davantage le rapport classifié sur le SCRS que l'OSSNR doit présenter annuellement au ministre de la Sécurité publique et de la Protection civile[18].

39. Le SCRS est soumis à des examens indépendants depuis sa création en 1984. Afin de gérer ses relations avec les organismes de surveillance externes, le SCRS a depuis longtemps été doté d'un secrétariat consacré aux examens, qui est actuellement rattaché à sa Direction de l'examen externe et de la conformité. Ce secrétariat a amélioré la capacité du SCRS de respecter son obligation légale de fournir à l'OSSNR un accès en temps opportun à l'information que l'OSSNR juge pertinente. En 2020, l'OSSNR était généralement satisfait de son accès au SCRS.

40. Au cours de la période visée par le présent rapport, le personnel du SCRS s'est montré coopératif et disponible dans la mesure du possible et, à plusieurs reprises en 2020, il a déployé des efforts exceptionnels pour aider l'OSSNR à achever des examens dont les échéanciers avaient eux-mêmes été perturbés par la pandémie de COVID-19. Bien que le SCRS et l'OSSNR soient en désaccord sur certains points – comme on peut s'y attendre dans une relation avec un organisme de surveillance externe – l'OSSNR est d'avis que la coopération continue du personnel du SCRS dans ces circonstances difficiles reflète une profonde compréhension et un respect du rôle de l'examen indépendant au sein du SCRS.

2.5 Examens du CST

Aperçu

41. Conformément à la Loi sur l'OSSNR, l'OSSNR a le mandat d'examiner toute activité du CST. En vertu de la Loi sur l'OSSNR, l'OSSNR doit également présenter au ministre de la Défense nationale un rapport annuel sur les activités du CST, portant notamment sur le respect par le CST de la loi et des directives ministérielles applicables, ainsi que sur le caractère raisonnable et la nécessité de l'exercice des pouvoirs du CST[19].

42. En 2020, l'OSSNR a réalisé trois examens du CST. Le présent rapport fait également état des résultats d'un examen de 2019 que l'OSSNR n'a pas été en mesure de communiquer dans son *Rapport annuel 2019*. L'OSSNR a également entrepris trois examens, qui sont présentés ci-après.

43. Lors de réunions avec des représentants de la société civile canadienne et du milieu universitaire, certains intervenants ont exprimé le souhait de recevoir de l'information de suivi concernant les examens réalisés sous la direction de l'ancien Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST)[20]. L'OSSNR maintient son engagement à caviarder, à traduire et à publier les examens historiques du BCCST, selon les ressources disponibles. Toutefois, bon nombre des examens du BCCST ne sont plus pertinents à la lumière des modifications législatives apportées en 2019 par la *Loi de 2017 sur la sécurité nationale*. Bon nombre des recommandations du BCCST ont également été mises en œuvre, puisqu'elles prévoyaient l'apport de modifications à la loi qui ont par la suite été prises en compte dans la *Loi de 2017 sur la sécurité nationale*. De plus, les directives ministérielles et autres instruments délivrés en vertu du cadre juridique précédent pour le CST (*Loi de 2017 sur la sécurité nationale*) sont maintenant désuets, ayant été délivrés de nouveau en vertu des nouvelles autorisations.

Communication d'information nominative sur un Canadien aux partenaires canadiens

44. Le 18 juin 2021, l'OSSNR a publié un résumé public de son examen des communications d'information nominative sur un Canadien (INC) par le CST[21]. Lorsque le CST procède à la collecte de renseignements électromagnétiques étrangers (SIGINT), il supprime toute INC recueillie fortuitement dans ses rapports de renseignements afin de protéger la vie privée des Canadiens et des personnes au Canada[22]. Néanmoins, le gouvernement du Canada et les destinataires étrangers de ces rapports de renseignements peuvent demander les détails de cette information, y compris les noms, les adresses de courriel et les adresses IP, s'ils ont l'autorisation légale et la justification opérationnelle de les recevoir.

45. En 2020, l'OSSNR a examiné le caractère licite et approprié de la communication d'INC par le CST, en mettant l'accent sur la communication d'INC par le CST à d'autres ministères du gouvernement du Canada[23]. Cet examen a porté sur un échantillon de communications d'INC par le CST au cours de la période du 1er juillet 2015 au 31 juillet 2019 contenant 2 351 cas d'INC, y compris dans le contexte de l'assistance

prêtée à la collecte de renseignements étrangers par le SCRS en vertu de l'article 16 de la Loi sur le SCRS[24].

46. L'OSSNR a constaté que bien que le CST ait approuvé 99 % des demandes de communication d'INC provenant de ses partenaires nationaux, 28 % de toutes les demandes étaient insuffisamment justifiées pour légitimer la communication de l'INC. Par conséquent, l'OSSNR a conclu que la mise en œuvre par le CST du régime de communication d'INC manquait de rigueur et pourrait ne pas être conforme à ses responsabilités en vertu de la *Loi sur la protection des renseignements personnels*. Ce rapport constituait donc un rapport de conformité en vertu de l'article 35 de la Loi sur l'OSSNR et a été présenté au ministre de la Défense nationale le 25 novembre 2020[25].

47. De plus, l'OSSNR a conclu que les communications par le CST d'INC recueillie en vertu de l'article 16 de la Loi sur le SCRS ont été effectuées d'une manière qui n'aurait probablement pas été communiquée à la Cour fédérale par le SCRS. Le SCRS avait fourni à la Cour fédérale un témoignage sur la façon dont elle traite l'information sur les Canadiens recueillie conformément à l'article 16 de la Loi sur le SCRS. Pourtant, lorsque l'OSSNR a comparé ce témoignage à la façon dont le CST traitait l'information sur les Canadiens recueillie en prêtant assistance au SCRS relativement à l'article 16, l'OSSNR a constaté des divergences notables dans les normes communiquées à la Cour fédérale. Le SCRS n'a pas participé à l'évaluation ou à la diffusion des communications qui suscitaient des préoccupations chez l'OSSNR; ces communications ont été traitées uniquement par le CST.

Réponse aux recommandations de l'OSSNR

48. Tel qu'il est indiqué à l'annexe E du présent rapport, le CST a accepté l'ensemble des 11 recommandations de l'OSSNR. Le CST a procédé à une évaluation des facteurs relatifs à la vie privée de son régime de communication d'INC et a informé l'OSSNR qu'il en est aux dernières étapes de la mise en œuvre d'une version mise à jour de son logiciel de demande d'INC, qui vise à faire en sorte que toute l'information nécessaire liée à la justification opérationnelle et à l'autorisation légale soit saisie avant qu'une communication n'ait lieu. Le CST a également cessé de communiquer l'INC recueillie en vertu de l'article 16 de la Loi sur le SCRS jusqu'à ce que la Cour fédérale soit pleinement informée de la communication d'information par le CST découlant de la collecte d'information aux termes de mandats en vertu de l'article 16.

Autorisations ministérielles et arrêtés ministériels en vertu de la *Loi sur le CST*

49. Après l'entrée en vigueur de la Loi sur le CST en 2019, le CST a reçu une nouvelle série d'autorisations ministérielles. Ces documents, délivrés par le ministre de la Défense nationale, autorisent le CST à se livrer à des activités qui risquent de contrevenir à une « [loi fédérale ou de porter] atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada[26] ». À titre d'exemple, de telles activités pourraient comprendre l'interception fortuite de communications privées dans le cadre des activités du CST en matière de collecte de renseignements étrangers.

50. La Loi sur le CST a également créé l'autorisation législative permettant au ministre de « désigner comme étant importante[s] pour le gouvernement fédéral de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information[27] » au moyen d'un arrêté ministériel. La désignation d'infrastructures comme étant importantes pour le gouvernement du Canada permet au CST de communiquer certains types de renseignements et de prêter une assistance directe.

51. En 2019, le ministre de la Défense nationale a émis sept autorisations ministérielles et trois arrêtés ministériels en vertu de la Loi sur le CST. L'OSSNR a reçu des documents d'information exhaustifs sur les activités autorisées par chaque autorisation ministérielle et arrêté ministériel. Selon les documents fournis par le CST, l'OSSNR estime que le CST a fait preuve d'une grande rigueur dans le processus de demande d'autorisations ministérielles. L'OSSNR a conclu que les demandes d'autorisations ministérielles du CST contenaient suffisamment d'information et fournissaient plus d'information que les demandes précédentes en vertu de la loi habilitante du CST avant la Loi sur le CST, soit la *Loi sur la défense nationale*, permettant ainsi une meilleure transparence des activités du CST.

52. Toutefois, l'OSSNR a constaté que le CST n'a pas pleinement évalué les répercussions juridiques de certaines activités autorisées depuis l'entrée en vigueur de la Loi sur le CST, qui n'ont pas encore eu lieu, mais qui sont permises conformément à un type particulier d'autorisation ministérielle. L'OSSNR a également constaté que le CST n'était pas en mesure de fournir une évaluation de ses obligations en vertu du droit international en ce qui concerne la réalisation de cyberopérations actives.

53. Les documents d'information du CST sur ces questions ont permis d'orienter le plan d'examen triennal de l'OSSNR. Plus particulièrement, cet examen a mis en lumière la

nécessité immédiate pour l'OSSNR de mettre l'accent sur les cyberopérations actives (CA) et les cyberopérations défensives (CD) du CST, étant donné que le commissaire au renseignement n'assure pas l'approbation de ces activités et que le CST n'a aucune obligation prévue par la loi d'aviser l'OSSNR lorsqu'il entreprend ces activités. Les CA et les CD représentent un nouveau volet du mandat du CST, et l'OSSNR examinera de près les politiques et les procédures de gouvernance touchant ces activités, de même que les opérations elles-mêmes.

Réponse aux recommandations de l'OSSNR

54. Tel qu'il est indiqué à l'annexe E, le CST a généralement accepté les recommandations de l'OSSNR relativement à cet examen. Le CST convient que ses activités devraient être évaluées en fonction de leur conformité au droit international, mais il continue de contester l'affirmation de l'OSSNR selon laquelle il n'a pas été en mesure de fournir une évaluation de ses obligations en vertu du droit international[28].

Politiques et procédures de conservation des données relatives au renseignement électromagnétique

55. S'inspirant d'un examen semblable effectué par l'inspecteur général de la National Security Agency des États-Unis, l'OSSNR a réalisé un examen des politiques et des procédures de conservation des données relatives au SIGINT du CST en décembre 2020. Cet examen visait à comprendre le processus de gestion du cycle de vie du SIGINT et à en savoir plus sur la conformité avec les limites légales de conservation des données, ainsi qu'avec les politiques gouvernementales et internes. La non-conformité avec ces limites pourrait porter atteinte aux libertés civiles et à la protection de la vie privée. L'OSSNR a terminé son examen et utilisera l'information qu'il en a tirée comme fondement d'un futur examen.

Dossier relatif aux incidents liés à la vie privée (2019)

56. Le 4 mars 2021, l'OSSNR a publié son premier examen du CST, qui était un examen du Dossier relatif aux incidents liés à la vie privée du CST de 2019[29]. Un incident lié à la vie privée 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 DIVP de 2019 de l'OSSNR, y compris les constatations et les recommandations, a été abordé à l'annexe A du *Rapport annuel 2019*. L'OSSNR n'a

pas été en mesure de publier les réponses du CST aux recommandations de l'OSSNR à temps pour ce rapport. Nous avons donc inclus ces réponses à l'annexe E du présent rapport annuel.

Réponse aux recommandations de l'OSSNR

57. Le CST a accepté l'ensemble des cinq recommandations de l'OSSNR concernant l'examen du DIVP de 2019. Le CST s'emploie à mettre en place un mécanisme normalisé pour déceler les incidents liés à la vie privée et en rendre compte, et étudie des façons de produire des rapports plus simplifiés et uniformes entre les équipes responsables de la conformité opérationnelle. Le CST s'est engagé à normaliser sa politique sur la façon d'évaluer si un incident lié à la vie privée constitue une atteinte substantielle à la vie privée, de même qu'à réexaminer ses méthodes d'évaluation pour veiller à ce qu'elles soient efficaces et raisonnables. En novembre 2019, le CST a également aboli une pratique particulière à l'égard de laquelle l'OSSNR avait soulevé des préoccupations.

Statistiques et données

58. Afin d'accroître la responsabilité à l'égard du public, l'OSSNR demande au CST de publier davantage de statistiques et de données sur l'intérêt public et les aspects liés à la conformité de ses activités. La présente section présente certaines de ces données du CST[30].

59. L'OSSNR a l'intention de fournir des données annuellement afin d'établir des points de référence et de permettre la comparaison. Cela dit, il convient de signaler que, sans une analyse approfondie et un contexte complet, certaines données du CST sont difficiles à interpréter et peuvent ne pas forcément indiquer des pratiques ou des faits nouveaux particuliers.

60. En 2020, le CST a fourni des rapports sur le renseignement étranger à plus de 2100 clients au sein de plus de 25 ministères et organismes du gouvernement du Canada en réponse à un éventail de priorités liées aux affaires internationales, à la défense et à la sécurité. À titre d'exemple, le CST estime que ses propres rapports sur le renseignement ont contribué à contrecarrer ou à contrer les cybermenaces étrangères, ont appuyé les opérations militaires du Canada, ont protégé les forces déployées, ont permis de relever les activités des États hostiles et ont donné un aperçu des événements et des crises à l'échelle mondiale afin d'éclairer les politiques et la prise de décisions du gouvernement du Canada[31].

61. Au cours de l'année civile 2020, le CST a reçu 24 demandes d'assistance du SCRS, de la GRC et du ministère de la Défense nationale et a traité 23 de ces demandes.

62. Également en 2020, le CST a enregistré un total de 81 incidents dans son DIVP, son Dossier relatif aux incidents liés aux alliés et son Dossier des erreurs de procédure mineures.

63. Au cours de l'année civile 2020, le CST s'est vu délivrer six autorisations ministérielles. Le tableau ci-dessous présente une ventilation de ces autorisations ministérielles, ainsi que des autorisations ministérielles de l'année civile 2019, que l'OSSNR n'a pas été en mesure de publier dans son rapport annuel de 2019. L'OSSNR continuera d'établir des points de référence pour ces statistiques et d'autres statistiques de même que de les comparer chaque année.

Autorisations ministérielles du CST, 2020

Type d'autorisation ministérielle	Article habilitant de la Loi sur le CST	Nombre d'autorisations délivrées
Renseignement étranger	26(1)	3
Cybersécurité — infrastructures fédérales et non fédérales	27(1) et 27(2)	1
Cyberopérations défensives	29(1)	1
Cyberopérations actives	30(1)	1

Autorisations ministérielles du CST, 2019

Type d'autorisation ministérielle	Article habilitant de la Loi sur le CST	Nombre d'autorisations délivrées
Renseignement étranger	26(1)	3
Cybersécurité — infrastructures fédérales et non fédérales	27(1) et 27(2)	2
Cyberopérations défensives	29(1)	1
Cyberopérations actives	30(1)	1

* Il convient de noter que les tableaux ci-dessus renvoient aux autorisations ministérielles qui ont été *délivrées* au cours des années civiles données et ne reflètent peut-être pas forcément les autorisations ministérielles qui étaient *en vigueur*. À titre d'exemple, si une autorisation ministérielle a

été délivrée à la fin de 2019 et est demeurée en vigueur au cours d'une partie de l'année 2020, elle est considérée comme une autorisation ministérielle de 2019 uniquement.

64. En juin 2021, le CST a confirmé dans son rapport annuel public de 2020-2021 qu'il a mené des cyberopérations étrangères[32]. Le CST a informé l'OSSNR qu'il n'est pas prêt à communiquer de l'information précise concernant les cyberopérations étrangères, car il s'agirait d'informations opérationnelles spéciales qui, si elles étaient divulguées, pourraient être préjudiciables aux relations internationales, à la défense nationale ou à la sécurité nationale du Canada.

Programmes de conformité internes

65. En plus de l'examen de l'OSSNR à titre d'expert indépendant, les fonctions du CST font également l'objet de ses propres programmes de conformité internes. Pour les besoins du présent rapport annuel, l'OSSNR a demandé au CST de fournir de l'information sur certains de ses programmes de conformité internes. Le programme interne de conformité des opérations du CST est responsable des activités du Centre canadien pour la cybersécurité (CCC)[33], tandis que la conformité des activités relatives au SIGINT est supervisée par la section responsable de la conformité du SIGINT.

66. Contrairement à certains de ses homologues internationaux[34], l'OSSNR n'évalue pas actuellement l'efficacité des programmes de conformité internes des ministères et organismes. Toutefois, l'OSSNR reconnaît que l'évaluation de tels programmes serait un élément important de son mandat d'examen, et il a l'intention de renforcer ses capacités dans ce domaine. Entre-temps, il est néanmoins utile de publier l'information accessible sur la conformité interne afin de mieux comprendre les politiques du CST à cet égard. L'information fournie dans la présente section ne devrait pas être considérée comme une évaluation indépendante.

Programme interne de conformité des opérations

67. Le personnel du programme interne de conformité des opérations est chargé d'offrir un soutien en matière de gestion des missions et d'opérationnaliser le programme de conformité interne du CCC, qui comprend trois piliers fondamentaux en matière de responsabilisation :

    - favoriser la conformité (sensibilisation, prévention et collaboration);
    - vérification et assurance de la conformité (surveillance, examen et audit);
    - gestion des incidents de conformité (analyse, atténuation et rapports).

68. Selon le CST, la capacité du CCC de démontrer sa conformité avec les obligations juridiques, ministérielles et stratégiques dans le cadre de ses activités de cybersécurité est un élément clé de son « permis d'exploitation ». Le CST considère que ces valeurs de responsabilisation et de transparence sont au cœur des opérations du CCC; elles sont considérées comme constituant le fondement du maintien de la confiance des Canadiens dans les activités du CCC.

69. Le CST a également soutenu qu'en plus de procéder annuellement à la surveillance de la conformité des activités de cybersécurité et d'assurance de l'information, le personnel du programme interne de conformité des opérations collabore avec les secteurs opérationnels du CCC pour promouvoir une « conception destinée à assurer la conformité », aux termes de laquelle les mécanismes de contrôle et les mesures de protection de la vie privée sont destinés à être intégrés de façon proactive aux systèmes, aux outils et aux processus opérationnels.

Conformité du SIGINT

70. Selon le CST, il est de la plus haute importance pour le SIGINT de veiller à la conformité des activités, ce qui est essentiel au maintien de la conformité du CST. La section chargée de la conformité du SIGINT travaille de concert avec les employés pour clarifier leurs rôles en matière de conformité, notamment au moyen de la mobilisation des employés, de la gestion des incidents, de la formation annuelle sur l'accréditation en matière de conformité et des conseils relatifs à la conformité au sujet des initiatives de SIGINT nouvelles et établies. La section s'emploie à élaborer et à tenir à jour un cadre d'examen de la conformité fondé sur la Loi sur le CST et d'autres lois applicables, ainsi que des instruments de politique interne du CST.

71. Selon le CST, ce cadre d'examen de la conformité prévoit les examens de la conformité internes que le groupe doit effectuer chaque année sur une période de trois ans. En outre, le groupe responsable de la conformité du SIGINT a pour but d'examiner les activités liées au SIGINT tout au long du cycle de vie de la production de renseignements, et ce, de l'acquisition de données au traitement, à l'analyse et à la diffusion des produits finaux. Au besoin, ces examens contiennent les mesures requises que les employés de certains secteurs d'activité doivent prendre pour maintenir ou améliorer la conformité. Ces mesures requises doivent faire l'objet d'un suivi et être mises à jour régulièrement par le groupe responsable de la conformité, de même que la haute direction.

72. L'OSSNR comprend que la transparence liée à la conformité n'est pas réalisée du jour au lendemain et que les efforts du CST en matière de transparence sont, comme l'a

dit le CST à l'OSSNR, toujours en cours. L'OSSNR peut aider le CST dans ces efforts, notamment en fournissant de l'information au public canadien sur le respect de la loi par le CST, sa conformité et ses fonctions de façon plus générale.

Erreurs de conformité internes signalées à l'OSSNR

Le CST affirme qu'il favorise une culture de conformité et encourage le signalement volontaire des incidents de conformité potentiels. En 2019-2020, le CST s'est dit préoccupé par le fait qu'il aurait peut-être reçu de l'information en dehors d'une période d'autorisation ministérielle valide relativement aux activités de cybersécurité touchant un certain type d'infrastructure.

Le CST a finalement avisé le propriétaire de l'infrastructure, a éliminé l'information reçue par inadvertance de ses systèmes conformément aux mesures de protection de la vie privée normalisées et a lancé un examen de l'incident afin d'établir et de mettre en œuvre des mesures de protection de la vie privée supplémentaires. Le CST a également mobilisé de façon proactive le ministre de la Défense nationale et l'OSSNR à des fins de transparence et de responsabilisation.

L'OSSNR est reconnaissant du fait que le CST lui ait signalé cet incident. Nous n'avons pas considéré l'incident comme soulevant une préoccupation importante, mais estimons que l'avis proactif et volontaire qu'a donné le CST concernant l'incident constitue une réussite clé de la relation entre l'OSSNR et le CST. L'OSSNR estime que la réponse du CST à cet incident est de bon augure pour une communication et une collaboration efficaces et honnêtes dans l'avenir.

Plan d'examen du CST de 2021

73. En général, l'OSSNR établit l'ordre de priorité de ses examens du CST en fonction des exigences législatives, ainsi que des risques. Dans le cas des risques, l'OSSNR cherche à déterminer les activités qui pourraient présenter des risques plus élevés de non-conformité juridique, souvent parce que ces activités sont nouvelles et non mises à l'essai, ou sont menées en vertu des autorisations mises à jour de la Loi sur le CST. L'OSSNR collabore également avec divers intervenants, de l'intérieur et de l'extérieur du Gouvernement du Canada, afin d'examiner les préoccupations liées au CST qui devraient être examinées[35].

74. Au cours des années à venir, l'OSSNR mettra l'accent sur les nouveaux aspects du mandat du CST ainsi que sur l'utilisation par le CST de certaines nouvelles technologies, y compris l'intelligence artificielle. Plus particulièrement, l'OSSNR a pris connaissance de diverses préoccupations exprimées par les intervenants canadiens au sujet du nouveau mandat du CST touchant les cyberopérations étrangères. L'OSSNR examine de près les cyberopérations étrangères du CST, y compris dans le cadre de deux examens en cours, et l'OSSNR continuera d'examiner ces types d'opérations dans l'avenir. L'OSSNR continuera également d'examiner les activités spécifiques du CST liées à la cybersécurité et au SIGINT en fonction des risques qui leurs sont associés.

75. En plus des deux examens de l'OSSNR prévus par la loi visant la Loi sur la communication d'information ayant trait à la sécurité du Canada (LCISC) et la Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères (LCMTIEE), l'OSSNR a entrepris ou prévoit réaliser les examens suivants du CST, dont l'achèvement est prévu en 2021 :

Examen de l'utilisation et de l'échange d'information entre les volets des mandats du CST

Cet examen porte sur la façon dont le CST garantit la conformité avec ses autorisations et ses restrictions prévues par la loi lorsqu'il échange de l'information entre les différents volets de ses mandats. L'échange d'information entre les volets a lieu, par exemple, si le CST recueille de l'information au titre du volet touchant le renseignement étranger, puis communique cette information à ceux menant des activités dans le cadre du volet touchant la cybersécurité. Cet examen porte sur la façon dont le CST utilise cette information entre différents volets afin de garantir la conformité avec la Loi sur le CST. Cet examen a été amorcé en janvier 2020, mais a été différé.

Examen des cyberopérations actives et des cyberopérations défensives du CST, partie 1 : gouvernance

Cet examen porte sur les nouveaux pouvoirs du CST touchant les cyberopérations actives et les cyberopérations défensives en vertu de la Loi sur le CST afin de garantir le respect de la loi. Il porte sur le cadre stratégique et juridique pour la réalisation de ces activités dans le cadre des autorisations ministérielles de 2019-2020. Cet examen a été amorcé en août 2020, mais a été différé.

Examen d'une activité réalisée en vertu de l'autorisation ministérielle du CST touchant le renseignement étranger

Cet examen porte sur une activité réalisée en vertu de l'autorisation ministérielle du CST touchant le renseignement étranger afin d'étudier les politiques et les procédures du CST. Cette activité n'a pas fait l'objet d'une évaluation, d'un audit ou d'un examen de la conformité externes ou internes, et l'OSSNR a ainsi l'occasion d'effectuer le tout premier examen de cette activité du CST. Le CST a présenté un document d'information préliminaire sur ce sujet à l'OSSNR au début de 2021, mais cet examen a été différé.

Étude ministérielle en vertu de l'article 31 de la Loi sur l'OSSNR

En vertu de l'article 31 de la Loi sur l'OSSNR, l'OSSNR peut faire effectuer par le CST une étude de ses activités qui sont liées à la sécurité nationale et au renseignement afin de s'assurer que ces activités respectent la loi et les directives ministérielles applicables et qu'elles sont raisonnables et nécessaires. Une fois l'étude terminée, le CST doit présenter un exemplaire du rapport au ministre de la Défense nationale et à l'OSSNR. À la suite de l'examen réalisé par l'OSSNR des communications d'INC par le CST, l'OSSNR a conclu que la mise en œuvre par le CST de son régime de communication en vertu de la *Loi sur la défense nationale* pourrait ne pas avoir respecté les exigences prévues par la *Loi sur la protection des renseignements personnels*. Étant donné la modification de la loi habilitante du CST en 2019, l'OSSNR a demandé au CST d'examiner ses communications aux partenaires du gouvernement du Canada ainsi qu'aux partenaires étrangers afin d'en garantir la conformité avec l'article 43 de la Loi sur le CST[36].

76. Au-delà de 2021, l'OSSNR a l'intention d'explorer les examens du CST portant notamment sur les sujets suivants :

- *les cyberopérations actives et les cyberopérations défensives, partie 2 : opérations;*
- *la protection des renseignements de nature délicate, y compris l'utilisation du polygraphe;*
- *l'assistance prêtée au SCRS;*
- *une activité de cybersécurité particulière énoncée dans une autorisation ministérielle;*
- *le Cadre de gestion du partage des nouvelles capacités associées à une vulnérabilité;*
- *l'utilisation de nouvelles technologies, y compris l'intelligence artificielle;*
- *un programme de collecte de SIGINT étrangers mené en vertu d'une autorisation ministérielle;*
- *les pratiques de conservation de SIGINT*.

77. Le mandat de l'OSSNR lui permet de réaliser des examens interministériels (également appelés examens qui « suivent le fil »), et l'OSSNR a l'intention de procéder ainsi dans le cadre de plusieurs examens en cours et prévus du CST. Réalisé en collaboration avec divers ministères et organismes fédéraux, l'examen des

communications d'INC du CST a été le premier examen dans le cadre duquel l'OSSNR a suivi le fil.

Accès

78. En 2020, l'équipe d'examen du CST de l'OSSNR a aménagé des locaux à bureaux à l'administration centrale du CST. Ces locaux à bureaux, au sein desquels on a commencé à mener partiellement des activités en 2020, comprennent neuf postes de travail et offrent à l'OSSNR un meilleur accès à ses homologues du CST. L'accès aux locaux à bureaux du CST de l'OSSNR est restreint et des mesures de protection appropriées sont en place pour assurer l'indépendance de l'OSSNR.

79. L'absence d'un accès complet et vérifiable de façon indépendante au référentiel d'information du CST constitue un défi important en ce qui a trait à l'examen du CST par l'OSSNR[37]. D'une part, afin de relever les défis en matière d'accès, l'OSSNR étudie des options visant à faire en sorte que le CST communique régulièrement et de manière proactive des catégories spécifiques d'information. Cette information serait utilisée à la fois pour assurer la conformité des activités et pour étayer les conclusions que l'OSSNR fournit dans son rapport annuel classifié à l'intention du ministre[38].

80. D'autre part, afin de relever les défis en matière d'accès, l'OSSNR étudie aussi certaines options avec le CST dans le but de mettre en œuvre l'approche d'« accès sur mesure » décrite à la section 1.5 du présent rapport. La mise en œuvre d'un accès sur mesure permettrait de maintenir la confiance entre les deux organisations, et ce, tout en garantissant que l'OSSNR a la capacité de vérifier de manière indépendante l'information reçue dans le cadre de son examen. Il convient également de noter que la vitesse à laquelle l'OSSNR reçoit l'information avant l'étape des vérifications demeure importante, car tout retard dans la réception d'information est susceptible de nuire à la capacité de l'OSSNR de s'acquitter de son mandat.

81. Afin d'encourager une plus grande responsabilisation au cours de l'année à venir, l'OSSNR entend établir des lignes directrices plus officielles pour la communication d'information par les ministères et les organismes, y compris des objectifs pour la rapidité des réponses aux demandes d'information, et un cadre pour la production de rapports publics sur ce qui précède.

Conclusion

82. En tant que nouvelle organisation, l'OSSNR a continué de doter son équipe d'examen du CST en 2020[39], en plus d'améliorer sa compréhension globale des attributions du CST. L'OSSNR reconnaît la nécessité de continuer à renforcer sa connaissance et son expertise du CST et de divers aspects liés aux fonctions de ce dernier. De même, le CST, qui a établi une relation étroite avec le BCCST au cours de quelque 23 années d'examen, est en voie de se familiariser avec l'OSSNR et son mandat. L'OSSNR reconnaît également que les examens des fonctions du CST peuvent être de nature tout particulièrement délicate, notamment en raison du volume élevé de contenu d'information spéciale hautement classifiée.

83. L'OSSNR remercie le CST de l'aide qu'il a apportée en temps opportun pour ce qui est de fournir des informations accessibles au public pour les besoins du présent rapport annuel, dont bon nombre n'ont pas été rendues publiques auparavant. L'OSSNR estime que cela reflète les mesures prises par le CST en vue d'accroître la transparence pour les Canadiens. En outre, l'OSSNR est reconnaissant de l'aide régulièrement fournie par les services de technologie de l'information du CST afin de l'aider à communiquer de façon sécurisée.

2.6 Autres ministères gouvernementaux

Aperçu

84. L'une des principales raisons de la création de l'OSSNR était d'assurer l'examen des organismes et ministères canadiens de la sécurité nationale et du renseignement qui n'avaient pas déjà des organismes d'examen spécialisés. À cette fin, la Loi sur l'OSSNR prévoit le fondement juridique afin « d'examiner l'exercice par les ministères de leurs activités liées à la sécurité nationale ou au renseignement »[40]. Comme on peut s'y attendre, la sélection des ministères et organismes qui ne font pas partie du SCRS et du CST et doivent être examinés est complexe et doit être mise à jour continuellement, et ce, parallèlement au contexte de la sécurité nationale en évolution constante.

85. En plus de sélectionner des ministères en particulier aux fins d'examen, l'OSSNR s'emploie à élaborer un cadre d'examen intégré qui porte sur les questions générales touchant la sécurité nationale et le renseignement, tant horizontalement que verticalement, dans l'ensemble des ministères et des organismes. Cela s'ajoute aux

examens annuels de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) et de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* (LCMTIEE), qui, lorsqu'ils sont considérés cumulativement, offrent la possibilité de couvrir l'ensemble de l'appareil.

86. Tel qu'il est mentionné précédemment à la section 1 du présent rapport, l'OSSNR travaille de concert avec les ministères et les organismes de l'ensemble du gouvernement à la conception d'un processus dans le cadre duquel l'information fournie pour les besoins d'un examen est corroborée et vérifiée aux fins d'exhaustivité. L'OSSNR appelle cela le principe « faire confiance, mais vérifier » : l'OSSNR se fie aux ministères pour lui donner accès à l'information, aux personnes et aux actifs en temps opportun, tout en ayant des mécanismes en place pour permettre à l'OSSNR de vérifier de façon indépendante l'intégralité de l'accès.

87. Il est également important de noter que l'OSSNR travaille en étroite collaboration avec le CPSNR et le CPVP pour échanger des plans d'examen et régler les conflits lorsque les examens portent sur des sujets semblables.

88. En plus du SCRS et du CST, l'OSSNR a entrepris des examens auprès des ministères et organismes suivants en 2020 :

- le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC);
- Affaires mondiales Canada (AMC);
- la GRC;
- Immigration, Réfugiés et Citoyenneté Canada (IRCC);
- l'Agence des services frontaliers du Canada (ASFC);
- Transports Canada;
- l'Agence de la santé publique du Canada.

89. Par ailleurs, dans le cadre des examens annuels de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) et de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* (LCMTIEE), l'OSSNR a collaboré avec tous les ministères et organismes qui composent l'appareil canadien de la sécurité nationale et du renseignement.

90. Les sections qui suivent présentent les examens réalisés ou amorcés en 2020 par ministère ou organisme, ainsi que certains examens futurs prévus.

Ministère de la Défense nationale et Forces armées canadiennes

Unité nationale de contre-ingérence des Forces canadiennes

91. L'Unité nationale de contre-ingérence des Forces canadiennes (UNCIFC) relève du Groupe du renseignement des Forces canadiennes au sein du Commandement du renseignement des Forces canadiennes et est organisée selon les détachements régionaux. Les activités de l'UNCIFC comprennent la réalisation d'enquêtes sur les menaces liées à la contre-ingérence qui présentent un risque pour la sécurité du MDN et des FAC, ainsi que le signalement de telles menaces, le soutien des opérations des FAC visant à améliorer la posture des forces et la sécurité opérationnelle, la coordination des échanges d'information sur les menaces avec les partenaires de sécurité et la communication d'une pré-alerte. La principale responsabilité de l'UNCIFC consiste à recueillir des renseignements de sécurité aux fins d'intégration aux évaluations des menaces nationales ou locales.

92. Le cadre d'enquête de l'UNCIFC est unique en ce sens qu'il couvre un large éventail de préoccupations en matière de renseignement de sécurité semblables à celles du SCRS, mais sa portée d'enquête se limite à l'information, aux personnes et aux actifs du MDN et des FAC (c.-à-d. ayant un lien avec le MDN et les FAC). Contrairement au SCRS, l'UNCIFC ne recueille pas d'informations détaillées sur les menaces, étant donné la nécessité d'un lien; et contrairement à un agent de sécurité du Ministère, l'UNCIFC ne mène pas d'enquêtes sur des questions concernant la conformité avec les politiques ou des questions de sécurité mettant en cause des comportements inadéquats de la part d'employés qui n'indiquent pas une menace évidente. En outre, l'UNCIFC n'est responsable ni du filtrage de sécurité ni des enquêtes criminelles. Il est donc plus facile de comprendre que le champ d'enquête de l'UNCIFC occupe une place très restreinte au-dessus de ceux liés aux mesures disciplinaires et au filtrage de sécurité, tout en se situant en deçà des seuils criminels.

93. Cet examen a porté sur les efforts déployés à l'échelle nationale par l'UNCIFC pour enquêter sur les menaces liées à la contre-ingérence pour le MDN et les FAC, sur la justification utilisée par l'UNCIFC pour justifier les enquêtes et sur les activités d'enquête connexes qui suivent. Dans ce contexte, l'examen visait expressément à fournir un portrait préliminaire du cadre de gouvernance du MDN et des FAC, ainsi que de la façon dont l'UNCIFC perçoit les menaces, recueille des renseignements, collabore et met en application les analyses. Une attention particulière a été accordée aux fondements juridiques, aux processus et aux procédures de l'UNCIFC, ainsi qu'à la façon dont ils contribuent à la protection contre les scénarios de menace interne[41].

L'OSSNR a également examiné la façon dont les renseignements tirés des enquêtes ont été transmis aux décideurs du MDN et des FAC. On procède actuellement au caviardage de l'examen complet et celui-ci devrait être publié sur le site Web de l'OSSNR sous peu.

94. L'OSSNR a constaté que l'UNCIFC et d'autres composantes de sécurité du MDN et des FAC ont été organisées de manière à former des cloisonnements verticaux à objectif restreint qui ne sont pas intégrés. L'UNCIFC respectait les politiques internes utilisées pour lancer des enquêtes, mais n'avait pas de processus officiel pour orienter l'établissement des priorités en matière d'enquête en fonction des critères pertinents. Il était également évident que l'UNCIFC avait besoin de clarté en ce qui a trait à ses pouvoirs juridiques afin d'assurer l'échange adéquat d'information à l'appui des processus administratifs et criminels.

95. L'OSSNR a en outre souligné la nécessité pour le MDN et les FAC de permettre à l'UNCIFC de tirer pleinement parti de ses capacités d'enquête pour réduire la durée des enquêtes, un problème qui, selon l'OSSNR, va à l'encontre des saines pratiques de protection de l'information, des personnes et des actifs du MDN et des FAC.

96. De plus, l'examen de l'OSSNR a révélé que l'UNCIFC n'a pas tenu compte de manière adéquate de l'effet cumulatif de ses activités relatives à la contre-ingérence en ce qui a trait à la protection des renseignements personnels du sujet d'une enquête, soulevant ainsi des questions quant au caractère adéquat des efforts de l'UNCIFC visant à assurer l'équité procédurale et incitant l'OSSNR à recommander que l'UNCIFC demande conseil au CPVP. L'OSSNR a également observé que le régime d'échange de renseignements de l'UNCIFC n'était pas conforme aux politiques du gouvernement du Canada en matière de protection de l'information, des personnes et des actifs.

97. La présence de la suprématie blanche au sein des Forces canadiennes est bien documentée. Les groupes militant pour la suprématie blanche cherchent activement des personnes possédant déjà une formation et une expérience militaires antérieures ou, inversement, encouragent les gens à s'enrôler afin d'avoir accès à une formation, à des tactiques et à de l'équipement spécialisés. Bien que l'OSSNR reconnaisse que la responsabilité de contrer cette menace ne peut pas relever exclusivement de l'UNCIFC, les multiples constatations découlant de l'examen font craindre que l'UNCIFC ne soit pas pleinement mise à contribution pour identifier de façon proactive les suprématistes blancs dans l'ensemble du MDN et des FAC. Après l'examen des études de cas et des entrevues menées avec des enquêteurs de l'UNCIFC, l'équipe responsable de l'examen a constaté que la suprématie blanche présente une menace

active liée à la contre-ingérence pour le MDN et les FAC et que le mandat de l'UNCIFC consistant à déceler cette menace de façon proactive est limité.

98. Enfin, à la suite de certaines préoccupations soulevées lors des dernières étapes de cet examen, l'OSSNR réalisera en 2021 une étude de cas sur les recherches informatiques et les processus d'entrevue de l'UNCIFC afin d'évaluer si ces activités étaient conformes à la *Charte*.

Réponse du MDN et des FAC aux recommandations de l'OSSNR

99. Le MDN et les FAC ont souscrit aux recommandations de l'OSSNR et ont déclaré qu'ils approuvent le rapport d'examen. Le MDN et les FAC ont convenu que des mesures seront prises aux niveaux appropriés conjointement avec les experts et les bureaux compétents, soulignant que des travaux ont été amorcés à cet égard et que certaines des recommandations de l'OSSNR sont déjà en cours de mise en œuvre. À titre d'exemple, le MDN et les FAC travaillent à la réalisation d'une évaluation des facteurs relatifs à la vie privée touchant les activités de renseignement de défense, et ils feront appel au CPVP pour obtenir ses commentaires une fois cette évaluation terminée.

Examens en cours

100. L'OSSNR a lancé un examen de l'entreprise du renseignement de défense afin de schématiser la collecte de renseignements et d'obtenir de l'information sur les cadres de gouvernance, les pouvoirs et les structures du renseignement de défense en vue d'appuyer la planification de futurs examens. Cette information a été complétée par un examen corollaire de la surveillance, de l'examen et de la conformité du renseignement au sein du système de renseignement de défense du MDN et des FAC. Bien qu'aucune constatation ou recommandation ne découle de ces enquêtes, les membres de l'OSSNR recevront une note d'information et une présentation du personnel de l'OSSNR sur les principales observations tirées de ce processus. L'achèvement de cet examen est prévu à l'automne 2021.

101. L'OSSNR a également commencé à assurer le suivi des questions soulevées lors de l'examen de l'UNCIFC de l'an dernier. L'examen portant sur la collecte opérationnelle liée à la contre-ingérence et la protection de la vie privée de l'OSSNR permettra d'examiner de façon plus approfondie les pratiques de l'UNCIFC concernant les entrevues de sujets et l'accès aux bases de données des systèmes de gestion de l'information et de technologie de l'information; cette dernière évaluation nécessitera que le personnel de l'OSSNR accède aux réseaux informatiques du MDN et des FAC

afin de valider l'utilisation de ces systèmes lors des enquêtes liées à la contre-ingérence.

102. L'OSSNR a également entrepris un examen des capacités relatives au renseignement d'origine humaine (ROHUM) du MDN et des FAC, essentiellement par l'examen de la gouvernance de cette activité de collecte spécialisée. L'examen portera sur l'évolution du ROHUM au sein du MDN et des FAC, y compris l'examen des récentes initiatives internes visant à améliorer la gouvernance et l'orientation relatives au ROHUM. À l'automne 2021, le personnel de l'OSSNR se rendra au centre de formation sur le ROHUM du MDN et des FAC et mènera des entrevues de grande envergure auprès des cadres supérieurs, des formateurs et des praticiens du domaine du ROHUM. Cet examen jettera les fondements d'un examen opérationnel complet des sources de ROHUM dans divers théâtres d'opérations.

103. À la suite des récentes communications du MDN et des FAC dans le cadre de l'examen de la portée de l'entreprise du renseignement de défense, l'OSSNR examinera également les activités de collecte de renseignement de source ouverte et de renseignement médical du MDN et des FAC à compter de la fin de 2021. Cet examen permettra d'évaluer la gouvernance et la conformité de ces activités.

104. La COVID-19 a eu une incidence considérable sur les échéanciers et les calendriers, entraînant ainsi des retards pouvant aller jusqu'à six mois. Bien que la COVID-19 ait présenté des difficultés ayant une incidence sur les échéanciers et les travaux d'examen, le MDN et les FAC ainsi que le Secrétariat de la coordination de l'examen et de la surveillance de la sécurité nationale et du renseignement ont été soucieux des demandes de l'OSSNR, lui offrant l'accès nécessaire à l'information, aux personnes et aux actifs, au besoin.

Affaires mondiales Canada

105. L'OSSNR a réalisé son premier examen consacré à un programme d'AMC. La période visée par l'examen s'est échelonnée du 1er janvier 2017 au 31 décembre 2019, mais des informations ne faisant pas partie de cette période ont également servi à la réalisation d'une évaluation complète d'aspects précis de ce programme. Les difficultés liées à la COVID-19 ont entraîné des rajustements méthodologiques, comme l'utilisation de la vidéoconférence sécurisée au lieu d'entrevues en personne pour certains employés.

106. Bien que les clients du programme le trouvent à la fois unique et précieux pour le gouvernement du Canada, l'examen a permis de relever plusieurs aspects à améliorer.

L'OSSNR a formulé un certain nombre de recommandations visant à améliorer ce programme. AMC a accepté de donner suite de façon positive à toutes les recommandations et s'est engagée à répondre à l'OSSNR dans un proche avenir. En raison de la nature très délicate de cet examen, l'OSSNR ne publiera rien de plus pour le moment.

Gendarmerie royale du Canada

107. En 2021, l'OSSNR terminera l'examen d'une unité spécialisée de renseignement de la GRC et lancera un examen des activités de sources humaines du Programme de sécurité nationale de la GRC. L'OSSNR prévoit augmenter le nombre d'examens auxquels participe la GRC. À titre d'exemple, l'OSSNR examinera la façon dont la GRC et le SCRS ont réagi à la menace que présentent les extrémismes violents motivés par des raisons idéologiques.

Immigration, Réfugiés et Citoyenneté Canada

108. L'OSSNR procède actuellement à un examen de la portée d'IRCC afin de définir son rôle et ses responsabilités en matière de sécurité nationale. Bien que ce ministère ne dispose d'aucun programme de collecte de renseignement, IRCC a un mandat complexe comportant des autorisations législatives partagées et des responsabilités opérationnelles pour ce qui est d'assurer l'intégrité du système d'immigration et d'atténuer les menaces pour la sécurité nationale provenant de l'étranger.

Agence des services frontaliers du Canada

109. L'OSSNR a lancé son plan visant à mener des examens approfondis des activités de sécurité et de renseignement les plus délicates de l'ASFC, tel qu'il a été déterminé par le CPSNR : ciblage fondé sur des scénarios, surveillance, sources humaines confidentielles, avis de surveillance et opérations policières conjointes. Un examen du ciblage des voyageurs aériens est en cours, lequel met l'accent sur la façon dont l'ASFC utilise les analyses prévisionnelles, y compris ce que l'on appelle le « ciblage fondé sur des scénarios », pour sélectionner les voyageurs aériens entrant au pays aux fins d'examen plus approfondi en ce qui a trait aux menaces pour la sécurité nationale. Les examens de l'utilisation par l'ASFC de sources humaines confidentielles et des activités de surveillance devraient être achevés en 2022.

Examens interministériels

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

110. Le 4 septembre 2019, la gouverneure en conseil a publié des directives écrites à l'intention des administrateurs généraux de 12 ministères et organismes en vertu de la nouvelle *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* (LCMTIEE). Cette loi et ses directives connexes visent à prévenir les mauvais traitements infligés à une personne en raison d'informations échangées entre un ministère du gouvernement du Canada et une entité étrangère. Au cœur des directives se trouve la prise en compte du risque sérieux et de la question de savoir si ce risque, s'il est présent, peut ou non être atténué. Pour ce faire, la LCMTIEE et les directives énoncent une série d'exigences qui doivent être respectées ou mises en œuvre par les ministères lorsqu'il s'agit de traiter de l'information. En vertu du paragraphe 8(2.2) de la Loi sur l'OSSNR, l'OSSNR est tenu d'examiner chaque année la mise en œuvre de toutes les directives données aux ministères et organismes.

111. Même s'il s'agissait de l'examen annuel inaugural effectué en vertu de la Loi sur l'OSSNR, il prend appui sur les travaux antérieurs entrepris dans ce domaine par l'OSSNR et son prédécesseur, le CSARS. L'examen de l'OSSNR concernant l'instruction du ministre de 2017 sur l'échange d'information avec des organismes étrangers en est un exemple. L'OSSNR prend appui sur cet examen antérieur et soutient fermement les constatations et les recommandations qu'il renferme. Il était essentiel de veiller à ce que l'OSSNR et les ministères faisant l'objet d'un examen respectent leurs obligations en vertu de la LCMTIEE et de la Loi sur l'OSSNR. L'approche employée pour recueillir de l'information lors d'une pandémie mondiale a été conçue à dessein pour cette première période d'examen unique. L'OSSNR a procédé au caviardage de l'ensemble de l'examen de 2019 de la Loi visant à éviter la complicité et celui-ci a été publié sur le site Web de l'OSSNR[42].

112. Pour obtenir un aperçu complet de la mise en œuvre au sein des ministères, l'OSSNR a demandé de l'information directement liée aux obligations particulières de chaque ministère en vertu de la LCMTIEE et des directives. Les réponses et les informations connexes ont permis de saisir les activités ministérielles liées à la LCMTIEE au cours de la période d'examen, ainsi que les procédures, les politiques, les outils et autres instruments (cadres) dont on a tiré parti à l'appui de ces activités. Aucune étude de cas n'a été réalisée pour cet examen. Toutefois, l'information recueillie a permis

d'établir une base de référence pour les questions globales auxquelles fait face l'appareil. En prenant appui sur cette base de référence, on commencera, dans le cadre d'examens futurs, à étudier les défis et les questions propres au cadre d'échange et à étudier de façon approfondie des cas particuliers et des avis juridiques ministériels pour orienter les constatations des examens.

113. L'OSSNR a été satisfait des efforts considérables déployés par de nombreux ministères nouvellement visés par la LCMTIEE en vue d'élaborer leurs cadres de soutien, mais il était clair au cours de cet examen que les ministères utilisaient des approches très différentes pour orienter leurs activités de traitement de l'information. Les réponses reçues démontrent diverses incohérences dans l'ensemble des ministères. L'adoption d'une approche uniforme et coordonnée pour donner suite aux préoccupations liées à la LCMTIEE n'est pas une exigence de mise en œuvre; toutefois, l'OSSNR estime qu'une telle approche s'avère utile.

114. De plus, étant donné que les directives données en vertu de la LCMTIEE ne décrivent pas les moyens précis par lesquels les ministères les « mettent en œuvre », il incombe aux organismes et aux ministères de veiller à ce qu'ils mettent en place des cadres et des programmes suffisamment solides pour appuyer pleinement une affirmation de mise en œuvre. Par conséquent, l'information recueillie dans le cadre de cet examen ne se limitait pas à une évaluation stricte de la mise en œuvre et prenait également en compte les aspects nécessaires pour mieux appuyer cette mise en œuvre. À l'avenir, cette approche permettra de jeter les fondements d'examens ultérieurs. En s'appuyant sur les constatations et les préoccupations soulevées dans le présent document, l'OSSNR continuera d'examiner les aspects qui, au bout du compte, amélioreront les cadres sous-jacents, favorisant ainsi une meilleure mise en œuvre de la LCMTIEE dans l'ensemble de l'appareil.

Communication d'information en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*

115. Adoptée en 2019, la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) a pour objet d'encourager les institutions fédérales à communiquer entre elles de l'information et de faciliter une telle communication, afin de protéger le Canada contre des activités portant atteinte à la sécurité du Canada. L'OSSNR a l'obligation légale de réaliser un examen annuel des communications faites en vertu de la LCISC.

116. En 2020, l'OSSNR a produit le Rapport annuel de 2019 sur la communication d'information au titre de la Loi sur la communication d'information ayant trait à la

sécurité du Canada[43]. Ce rapport porte sur la période allant de l'entrée en vigueur de la LCISC le 21 juin 2019 au 31 décembre de la même année. Au cours de la période de référence, les institutions fédérales ont fait 114 communications d'information en vertu de la LCISC. Le rapport révèle que les institutions ont réalisé des progrès satisfaisants au chapitre de l'institutionnalisation de cette nouvelle loi. Le rapport fournit des renseignements historiques et contextuels sur la LCISC et sur la place qu'elle occupe aux côtés d'autres mécanismes juridiques pour l'échange d'information. Le rapport comprend également des exemples de scénarios anonymisés de communications faites en vertu de la LCISC, de même que des critères d'évaluation future. L'OSSNR a l'intention de travailler en étroite collaboration avec le CPVP dans le cadre de la production des prochaines versions de ce rapport. Les résultats de l'examen ultérieur des communications faites au titre de la LCISC seront examinés dans le rapport annuel de 2020 sur la communication d'information au titre de la LCISC.

Biométrie

117. L'OSSNR a fait progresser son engagement pris l'an dernier pour ce qui est de répertorier 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. Un examen horizontal des données biométriques dans le continuum frontalier est en cours, portant sur les activités menées par l'ASFC, IRCC et Transports Canada. Les activités à l'étude comprennent la délivrance et la vérification de documents de voyage – en mettant l'accent sur les voyages aériens – et le filtrage de sécurité des étrangers cherchant à entrer au Canada. Un examen ultérieur portera sur l'utilisation des données biométriques dans le cadre des activités de maintien de l'ordre relatives au renseignement de sécurité et à la sécurité nationale.

Conclusion

118. Compte tenu de la pandémie en cours et à la lumière des leçons tirées des examens actuels, dans certains cas, l'OSSNR a modifié le plan présenté dans son *Rapport annuel 2019*. En effet, le travail de l'OSSNR sur la sécurité économique, par exemple, a bénéficié d'un exercice d'établissement de la portée faisant intervenir plusieurs ministères pour l'aider à mieux comprendre les pouvoirs octroyés dans ce domaine, et pour l'aider à déterminer s'il doit poursuivre ses travaux sur cette question. Dans le même ordre d'idées, à la suite d'un exercice d'établissement de la portée, l'OSSNR attendait de prendre connaissance des conclusions d'un rapport indépendant

commandé par le ministre de la Santé dans ce domaine avant de décider s'il doit examiner ou non le renseignement sur la santé publique, qui a désormais été déposé.

119. Au cours de l'année à venir, l'OSSNR continuera de collaborer avec les ministères et les organismes au moyen d'examens ciblés. Certains de ces examens seront organisés en fonction de grands thèmes horizontaux pouvant comprendre de nombreux ministères, nécessitant ainsi une approche coordonnée. L'OSSNR s'engage à travailler en collaboration avec les ministères, plus particulièrement en ce qui concerne l'établissement d'un régime d'accès qui appuie la vérification indépendante et la responsabilisation.

03 //

Enquêtes sur les plaintes

3.1 Défis de 2020

1. La pandémie a eu une incidence défavorable sur la réalisation en temps opportun des enquêtes de l'OSSNR. En date de mars 2020, des retards inévitables ont découlé des décrets ordonnant de rester à domicile et des lignes directrices en matière de santé publique provinciale qui ont été adoptées. Tout comme l'OSSNR a dû composer avec un accès limité aux documents classifiés, les parties du gouvernement fédéral aux enquêtes qui sont tenues de fournir des renseignements à l'OSSNR ont aussi dû faire face à cette réalité. Par conséquent, dans plusieurs affaires en cours, l'OSSNR a accordé des ajournements et des prorogations des délais pour les étapes de la procédure, y compris le dépôt des observations et des éléments de preuve. Bien que cela soit regrettable, l'OSSNR s'est adapté aux circonstances difficiles de la pandémie du mieux possible et a fait progresser les procédures d'enquête de manière novatrice, dans la mesure du possible, notamment en menant certaines instances par écrit et en organisant des réunions et des conférences de gestion de cas virtuelles.
2. Malgré les revers procéduraux en 2020, l'OSSNR a été en mesure de mener une enquête sur une plainte et de produire un rapport définitif. L'OSSNR a également rendu des décisions officielles en vue de clore trois autres dossiers. De plus, l'OSSNR a réussi à mener à bien une initiative complexe de réforme des processus qui permettra de moderniser et de simplifier le processus d'enquête.

3.2 Processus d'enquête sur les plaintes : réforme et prochaines étapes

3. Bien que la pandémie ait eu une incidence sur les enquêtes sur les plaintes, l'OSSNR a réalisé des progrès considérables au chapitre de la réforme des processus régissant ces enquêtes. Au cours de l'année, l'OSSNR a entrepris une initiative de réforme des processus visant à moderniser le modèle d'enquête sur les plaintes afin d'atteindre son objectif consistant à assurer l'efficacité et la transparence. Deux priorités ont

orienté la modernisation du processus, à savoir l'accès à la justice pour les plaignants non représentés et la création d'étapes procédurales simplifiées et moins formelles.

4. L'OSSNR a créé de nouvelles Règles de procédure pour refléter ce nouveau modèle et a procédé à un vaste exercice de consultation auprès des intervenants des secteurs public et privé afin d'obtenir le produit final le plus efficace et le plus réfléchi. Ces nouvelles Règles de procédure sont en vigueur depuis juillet 2021.

5. L'OSSNR a également mis en œuvre un nouvel énoncé de politique qui prévoit un engagement envers le public en vue d'accroître la transparence de ses enquêtes en publiant les versions non classifiées et dépersonnalisées des rapports d'enquête finaux[44].

6. Au cours de l'année à venir, l'OSSNR mettra à jour son site Web afin d'y ajouter des directives procédurales améliorées pour informer les membres du public sur la façon de déposer des plaintes et de s'orienter dans le processus d'enquête. Une partie de la mise à jour du site Web de l'OSSNR consistera à mettre en place un portail sécurisé pour le dépôt en ligne des plaintes et les communications protégées afin de faciliter la gestion efficace de la charge de travail liée aux plaintes de l'OSSNR.

7. Dans l'avenir, l'OSSNR prévoit également mener une analyse des tendances en ce qui concerne les plaintes, ce qui comportera une vaste initiative visant à recueillir de façon appropriée des données démographiques sur la race et autres données démographiques. Cette initiative vise à améliorer l'accès à la justice en renforçant la connaissance et la compréhension du processus d'enquête. L'objectif général est de consigner les différents groupes parmi les plaignants civils et de déterminer la fréquence des plaintes qui comprennent des allégations de préjugés raciaux ou autres types de préjugés ainsi que d'établir s'il y a des disparités, s'il y a des différences quant aux types de plaintes déposées contre des membres d'organismes de sécurité nationale et du renseignement en fonction de différents groupes, si les résultats des enquêtes sur les plaintes varient selon le groupe, ainsi que si la satisfaction des civils à l'égard du processus d'enquête de l'OSSNR varie selon le groupe.

Volume de dossiers d'enquête de l'OSSNR pour l'année à venir

8. À la conclusion des efforts visant à gérer les dossiers d'enquêtes en cours de l'OSSNR dans le contexte des défis présentés par la pandémie en 2020, l'OSSNR entreprendra au cours de l'année à venir une réforme du processus d'enquête qui facilitera la mise en œuvre de procédures modernes et équitables qui permettront de faire progresser

ces dossiers, le tout complété par un site Web amélioré qui favorisera l'accès et la transparence dans le cadre du processus d'enquête.

9. En 2021, le volume de dossiers de l'OSSNR augmentera considérablement en raison de l'ajout de près d'une soixantaine de nouvelles enquêtes à son inventaire actuel. Ces plaintes ont été transmises à l'OSSNR en avril 2021 par la Commission canadienne des droits de la personne en vertu du paragraphe 45(2) de la *Loi canadienne sur les droits de la personne*. Ce volume élevé de dossiers présentera un défi important sur le plan de la gestion des cas de l'OSSNR. L'OSSNR mettra en œuvre des mesures d'efficacité procédurale autant que possible tout en respectant les exigences en matière d'équité procédurale.

3.3 Plaintes en 2020

Résumé du rapport définitif

Allégations relatives au rôle du Service canadien du renseignement de sécurité dans l'annulation ou le refus de l'autorisation d'accès aux sites

Contexte

10. Le plaignant a déposé une plainte contre le SCRS pour demander une enquête sur le rôle du SCRS ou sa participation en ce qui a trait à l'annulation ou au refus de demandes de contrôle d'accès aux sites se rattachant à un emploi auprès d'une entreprise privée dans un édifice gouvernemental.

Allégation

11. Le plaignant a allégué que le SCRS a utilisé de façon inadéquate l'information recueillie et a conclu de manière inadéquate qu'il y avait une menace pour la sécurité, ce qui a donné lieu au refus d'une autorisation d'accès aux sites.

Enquête

12. L'OSSNR a examiné les éléments de preuve présentés par les témoins convoqués, les documents présentés par les parties ainsi que d'autres documents pertinents mis à sa disposition dans le cadre de l'enquête sur la plainte, y compris les documents classifiés communiqués à l'OSSNR par le SCRS. L'OSSNR a également entendu le témoignage du plaignant.

13. Les articles 13 et 15 de la Loi sur le SCRS confèrent au SCRS le pouvoir de fournir des évaluations de sécurité aux ministères du gouvernement du Canada et de mener des enquêtes, au besoin. Le SCRS reçoit des demandes des ministères concernant des personnes qui demandent une autorisation de sécurité ou une autorisation d'accès aux sites et leur rôle est défini à l'article 2 de la Loi sur le SCRS. Le SCRS a présenté des éléments de preuve sur les étapes suivies dans le cadre du processus du Service, la Norme sur le filtrage de sécurité du Secrétariat du Conseil du Trésor et le fait que le ministère client décide d'accorder ou non une autorisation. Ainsi, le SCRS ne fournit que de l'information générale et une évaluation du point de vue de la sécurité nationale afin que les ministères disposent de l'information dont ils ont besoin pour prendre une décision éclairée.

14. L'OSSNR a également entendu des témoignages du SCRS concernant certaines informations communiquées au ministère client qui a demandé l'autorisation d'accès aux sites et la façon dont le tout se rattachait à la fois à la fiabilité et à la loyauté. Le SCRS a reconnu que l'échange de certaines informations avec le ministère client s'est déroulé dans un cadre informel et que cela n'aurait pas dû se produire ainsi. Il a été souligné qu'après la communication d'informations de source ouverte, le ministère client a annulé sa demande et le SCRS a fermé son dossier.

15. Le plaignant était convaincu que le SCRS était responsable du refus de sa demande d'autorisation d'accès au site.

16. L'OSSNR a reconnu la perception du plaignant selon laquelle le SCRS a refusé sa demande d'autorisation d'accès au site, mais la preuve a démontré que le SCRS n'avait pas pris cette décision. Cette décision a été prise par le ministère en question et le SCRS n'a eu aucun autre rôle à jouer dans cette affaire.

Constatations

17. L'OSSNR a constaté les faits suivants :

    - le SCRS n'a pas utilisé de façon inadéquate les informations de source ouverte qui ont été communiquées;
    - le SCRS reconnaît que l'échange d'informations n'aurait pas été approuvé par la direction;
    - le SCRS n'a pas refusé la demande du plaignant visant à obtenir une autorisation d'accès au site, mais c'est plutôt le ministère qui a pris la décision d'annuler la demande.

Conclusion

18. L'OSSNR a déterminé que la plainte était non fondée.

Résumés des plaintes jugées abandonnées

Allégations contre le SCRS concernant la communication d'information à des autorités étrangères et l'incidence sur le passage de la frontière

19. Le plaignant a déposé une plainte contre le SCRS concernant la communication d'information à des autorités étrangères ayant compliqué le passage de la frontière. L'OSSNR a commencé son enquête et a tenu une conférence informelle de gestion des cas avec les parties afin de régler la plainte. À la suite de cette réunion de résolution, le plaignant s'est engagé à prendre des mesures pour régler tout problème en cours. L'OSSNR a tenté de communiquer avec le plaignant à plusieurs reprises pour déterminer si les problèmes en cours avaient été réglés. L'OSSNR a conclu que des efforts raisonnables avaient été déployés pour communiquer avec le plaignant et a communiqué les motifs pour lesquels la plainte était réputée avoir fait l'objet d'un désistement conformément aux Règles de procédure de l'OSSNR. Le dossier d'enquête sur la plainte a été fermé.

Allégations concernant le rôle du SCRS dans le retard de l'évaluation de sécurité concernant une demande de résidence permanente

20. Le plaignant a déposé une plainte contre le SCRS alléguant qu'il a causé un retard important dans la présentation de l'évaluation de sécurité pour une demande de résidence permanente. Dans le cadre de son enquête, l'OSSNR a tenté à plusieurs reprises de communiquer avec le plaignant au sujet de la possibilité de mener des discussions informelles en vue de parvenir à une résolution avec le SCRS. L'OSSNR a conclu que des efforts raisonnables avaient été déployés pour communiquer avec le plaignant et a communiqué les motifs pour lesquels la plainte était réputée avoir fait l'objet d'un désistement conformément aux Règles de procédure de l'OSSNR. Le dossier d'enquête sur la plainte a été fermé.

Allégations contre la GRC pour mauvaise conduite pendant l'arrestation

21. La Commission civile d'examen et de traitement des plaintes relatives à la GRC (CCETP) a renvoyé cette plainte à l'OSSNR en vertu du paragraphe 45.53(4.1) de la Loi sur la GRC. La plainte alléguait que les membres de la GRC n'avaient pas

informé le plaignant de ses droits et obligations lors d'une interaction qui s'est produite la veille d'une arrestation pour incitation à craindre des activités terroristes et méfait public, l'usage de la force excessive et d'autres allégations. Dans le cadre du lancement de son enquête, l'OSSNR a tenté à plusieurs reprises de communiquer avec le plaignant. L'OSSNR a conclu que des efforts raisonnables avaient été déployés pour communiquer avec le plaignant et que toutes les options avaient été épuisées. Par conséquent, l'OSSNR a communiqué les motifs pour lesquels la plainte était réputée avoir fait l'objet d'un désistement conformément aux Règles de procédure de l'OSSNR. Le dossier d'enquête sur la plainte a été fermé.

04 //

Conclusion

1. En 2020, les équipes de l'OSSNR ont travaillé dans des conditions exigeantes et ont pourtant réussi à se surpasser. L'OSSNR leur est reconnaissant d'avoir mené les examens de manière efficace. Comme il est mentionné dans le présent rapport annuel, l'OSSNR a des projets ambitieux pour les travaux en cours et futurs, et ce, tout en continuant d'accroître sa capacité et de renforcer ses relations avec les ministères et organismes visés par ses examens. En 2020, l'effectif de l'OSSNR est passé de 30 à 58 personnes, son équipe d'examen du CST a commencé à travailler dans les bureaux du CST et l'OSSNR a presque achevé l'aménagement d'une nouvelle installation pour son personnel, tout en s'adaptant soigneusement et de façon responsable aux défis de la pandémie.
2. Dans un esprit de coordination et de complémentarité avec d'autres entités d'examen et de surveillance, l'OSSNR a continué de renforcer ses relations avec divers homologues, dont le Conseil de surveillance et d'examen du renseignement du Groupe des cinq, le Comité des parlementaires sur la sécurité nationale et le renseignement et le Commissariat à la protection de la vie privée du Canada. L'OSSNR se consacre également à entretenir une relation solide et mutuellement bénéfique avec les intervenants non gouvernementaux. L'OSSNR espère faire connaître son mandat à diverses communautés, y compris aux étudiants, de même que recevoir des commentaires pour l'aider à poursuivre son travail et à améliorer son programme. L'OSSNR vous encourage fortement à formuler une rétroaction et des commentaires et espère que vous avez trouvé le présent rapport utile. Quels que soient vos antécédents, veuillez communiquer avec nous et nous faire part de vos réflexions au sujet du présent rapport, ainsi que des activités d'examen et de traitement des plaintes de l'OSSNR.
3. L'OSSNR est très reconnaissant de la persévérance, de la diligence et de la passion dont fait preuve son personnel, qui continue de réaliser des travaux significatifs et d'obtenir des résultats importants malgré les défis que pose la pandémie en 2020. À mesure que l'OSSNR évolue en tant qu'organisation, notamment en ce qui a trait à l'augmentation de son effectif, son personnel se réjouit à l'idée de promouvoir la responsabilisation au sein de l'appareil canadien de la sécurité et du renseignement.

05 //

Annexes

Annexe A : Liste des abréviations

Abréviation	Nom complet
AM	Autorisation ministérielle
ASFC	Agence des services frontaliers du Canada
BCCST	Bureau du commissaire du Centre de la sécurité des télécommunications
CSARS	Comité de surveillance des activités de renseignement de sécurité
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement
CPVP	Commissariat à la protection de la vie privée du Canada
CST	Centre de la sécurité des télécommunications
FAC	Forces armées canadiennes
FIORC	Conseil de surveillance et d'examen du renseignement du Groupe des cinq
GRC	Gendarmerie royale du Canada
LCISC	*Loi sur la communication d'information ayant trait à la sécurité du Canada*
LCMTIEE	*Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*
MDN	Ministère de la Défense nationale
MRM	Mesures de réduction de la menace
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement
ROHUM	Renseignement d'origine humaine
SCRS	Service canadien du renseignement de sécurité

SIGINT	Renseignement d’origine électromagnétique
UNCIFC	Unité nationale de contre-ingérence des Forces canadiennes

Annexe B : Aperçu financier et administratif

Aperçu financier

1. L'OSSNR est organisé selon trois principaux secteurs d'activité : les services juridiques, les examens et les services internes. Le tableau ci-dessous présente une comparaison des dépenses effectuées en 2019 et en 2020 pour chacun des trois secteurs d'activité susmentionnés.

(en dollars)	Dépenses (2020)	Dépenses (2019)
Services juridiques et enquêtes sur les plaintes	1 859 924	1 042 117
Examens	3 094 323	1 726 218
Services internes	4 625 860	2 820 115
Total	**9 580 107**	**5 588 450**

2. Au cours de l'année civile 2020, les dépenses de l'OSSNR se sont élevées à 9,6 millions de dollars, ce qui représente une augmentation de 4,0 millions de dollars (82 %) par rapport aux 5,6 millions de dollars dépensés en 2019. Cette augmentation des dépenses est principalement attribuable à la croissance de l'effectif de l'OSSNR, à l'aménagement d'installations sécurisées afin qu'elles puissent accueillir un plus grand nombre d'employés, et à des investissements dans les infrastructures de gestion de l'information et de technologie de l'information, notamment afin de permettre l'accès aux réseaux classifiés, aux vidéoconférences sécurisées ainsi qu'à l'équipement permettant au personnel de l'OSSNR de travailler à distance.

Dotation

3. Au cours de l'année, l'OSSNR a réalisé d'importants progrès sur le plan de la dotation en personnel. En effet, l'OSSNR a vu son effectif passer de 30 à 58 personnes, ce qui représente une augmentation nette de 28 employés (93 %). Cette augmentation a été rendue possible par la mise en œuvre de stratégies, de procédures et de pratiques de dotation modernes et souples. Lors de l'exécution de ses activités de dotation, l'OSSNR a eu recours à des pratiques exemplaires pour favoriser l'inclusion et la diversité ainsi que pour respecter les impératifs liés à la représentation des langues officielles.

4. En 2021 et par la suite, l'OSSNR poursuivra ses efforts pour embaucher des personnes talentueuses et dévouées afin de pouvoir remplir son mandat. Pour appuyer ces efforts, l'OSSNR met en place des programmes d'intégration des employés, de gestion des talents et de bien-être visant à attirer et à maintenir en poste ses employés ainsi qu'à soutenir leur perfectionnement. Au fur et à mesure que l'OSSNR prend de l'expansion pour atteindre un effectif complet de 100 employés, il continuera à faire des investissements importants dans l'infrastructure technologique et à s'assurer que ses employés offrent un bon rendement, tout en pouvant compter sur le plein soutien des fonctions des services internes.

Pandémie

5. Comme indiqué tout au long du présent rapport, la pandémie a continué à avoir des conséquences importantes sur les opérations et les activités de l'OSSNR en 2020. Le Secrétariat de l'OSSNR a réagi rapidement en élaborant et en mettant en œuvre de nouveaux protocoles pour que l'OSSNR puisse continuer à déployer des efforts dans un contexte où la crise de santé publique est en constante évolution.
6. Compte tenu de l'importance de l'accès aux installations de l'OSSNR pour que ce dernier puisse mener à bien son mandat, le Secrétariat a pris des mesures efficaces en temps opportun pour permettre aux employés de l'OSSNR d'accéder de manière contrôlée, sécuritaire et rapide à leurs bureaux. Les résultats du plus récent Sondage auprès des fonctionnaires fédéraux confirment que les employés se sentent en confiance avec l'approche adoptée par l'OSSNR en ce qui concerne la protection de la santé et de la sécurité des employés. En 2021, l'OSSNR entend continuer à améliorer ses pratiques en matière de santé et de sécurité en écoutant les préoccupations des employés et en prenant des mesures en temps opportun pour répondre aux préoccupations en matière de santé et de sécurité.
7. Pour remédier à certains des effets néfastes de la pandémie, tels que l'isolement, le manque de contacts humains ou la capacité restreinte de créer des liens avec les nouveaux employés, l'OSSNR a axé ses efforts sur l'augmentation des communications numériques et des contacts virtuels avec le personnel en publiant des bulletins, en faisant le point sur la pandémie, en organisant des réunions virtuelles et en faisant la promotion de programmes d'aide aux employés régulièrement.
8. Toutefois, les décrets ordonnant de rester à domicile et l'accès restreint aux bureaux ont rendu inévitables certains retards dans l'avancement des examens et des enquêtes sur les plaintes, étant donné que la capacité de récupérer des documents

classifiés et d'en discuter dans un environnement sécurisé est essentielle au travail de l'OSSNR. Un grand nombre de ministères et d'organismes qui ont répondu aux demandes de l'OSSNR liées à des examens et à des enquêtes ont également dû faire face à des défis similaires, notamment des effectifs réduits et un accès limité à leurs lieux de travail, ce qui a contribué aux retards pris par l'OSSNR.

Cyberincident

9. En mars 2021, l'OSSNR a été victime d'un cyberincident. En effet, un accès non autorisé a été détecté dans le réseau externe de l'OSSNR, ce qui a contribué à retarder davantage l'exécution de ses travaux. Ce réseau externe abrite uniquement des informations non classifiées et protégées, et il n'était pas utilisé pour stocker de l'information de niveau Secret ou Très secret. Grâce à l'aide de ses partenaires fédéraux et, en particulier, aux efforts du Bureau du Conseil privé, du Centre canadien pour la cybersécurité et de Services partagés Canada, l'OSSNR a pu régler le problème et reprendre ses activités normales en temps opportun.

10. L'OSSNR a collaboré avec le Commissariat à la protection de la vie privée du Canada (CPVP) et le Secrétariat du Conseil du Trésor du Canada afin de régler un cas de violation de la vie privée ayant découlé du cyberincident. L'OSSNR a informé ses partenaires, a avisé le public par l'intermédiaire de son site Web et de ses comptes de médias sociaux, et a publié des avis directs conformément aux exigences et aux recommandations du CPVP. L'OSSNR a pour principales priorités d'assurer la protection de la vie privée des Canadiens et de protéger l'information en sa possession.

Initiatives fondamentales

11. Compte tenu de la croissance actuelle et prévue des effectifs et des exigences en matière de distanciation physique en vigueur durant la pandémie, pour que l'organisation connaisse du succès, il est crucial que ses employés aient accès à des locaux sécurisés pour effectuer des travaux de nature classifiée. En 2020, l'OSSNR a renforcé sa stratégie relative à ses locaux, a accru son financement et a réalisé des progrès considérables en ce qui a trait à l'aménagement à court terme de ses locaux. Bien que les projets de construction de locaux à long terme aient été touchés par la pandémie, l'OSSNR élabore actuellement des stratégies visant à inciter ses employés à travailler à domicile lorsque cela est possible et productif.

12. La contribution des employés de l'OSSNR, leur perfectionnement et leur bien-être ainsi que le développement d'une culture qui soutient son important mandat sont des éléments cruciaux du succès de l'OSSNR. En tant que nouvel organisme et employeur distinct, l'OSSNR a établi, après avoir consulté ses employés, les fondements de sa philosophie en matière de gestion des ressources humaines en élaborant et en mettant en œuvre une politique de gestion des ressources humaines moderne et cohérente ainsi qu'en mettant en place les conditions d'emploi qui s'y rattachent.

13. De la même manière, l'OSSNR a élaboré des politiques en matière de santé et de sécurité au travail, de prévention du harcèlement et de la violence au travail, et ce, en plus de mettre sur pied un programme de récompenses et de reconnaissance ainsi qu'un code de conduite pour ses employés et un plan d'action triennal sur les langues officielles. L'OSSNR s'est également associé à Santé Canada pour offrir des services d'aide aux employés et à d'autres organisations dans le but de maintenir des relations solides entre les employés et les employeurs.

14. Les employés et les membres de la direction de l'OSSNR ont participé à des discussions sur les obstacles systémiques à l'inclusion et à la diversité et sur la façon dont, grâce à son mandat, l'OSSNR pourrait tirer profit de son rôle afin de devenir un agent de changement dans l'appareil de la sécurité nationale et du renseignement. Au cours de l'année 2021, un plan d'action à cet effet sera officialisé et présenté au greffier du Conseil privé.

Ce que nous réserve l'avenir

15. En 2021, l'OSSNR entend continuer à mettre au point des politiques et des outils ainsi qu'à mettre en œuvre des initiatives qui favorisent une culture de l'excellence, de la transparence, du respect et de l'innovation.

16. À court terme, l'OSSNR mettra en œuvre des politiques, des outils et des programmes pour attirer, maintenir en poste et perfectionner davantage les gens de talent; s'efforcera de soutenir ses engagements et ceux du gouvernement du Canada à l'égard de la diversité et de l'inclusion; prendra des mesures pour répondre aux préoccupations des employés soulevées dans le cadre du Sondage auprès des fonctionnaires fédéraux de 2020; achèvera la mise en place des activités qui peuvent être mieux exécutées par l'OSSNR (comme la gestion des finances et des ressources humaines) ainsi que la recherche de soutien des ministères partenaires pour les activités qui peuvent être mieux exécutées par des organisations de plus grande taille (comme certaines d'entre elles ont trait à la technologie de l'information et aux

fonctions de sécurité); poursuivra les travaux pour renforcer sa position en ce qui concerne la sécurité, la technologie de l'information et la gestion de l'information; obtiendra un accès accru aux installations sécurisées pour ses employés.

Annexe C : Cadre d'examen de l'OSSNR

1. L'OSSNR élabore présentement un cadre d'examen qui lui permettra de s'assurer que ses examens sont exécutés d'une manière uniforme. Ce cadre vise à fournir une orientation systématique concernant le processus et l'approche de l'OSSNR à l'égard des examens, du début à la fin. Le cadre d'examen de l'OSSNR comprend les types d'examens ainsi que les phases et les étapes du processus d'examen.

Phases et étapes d'examen

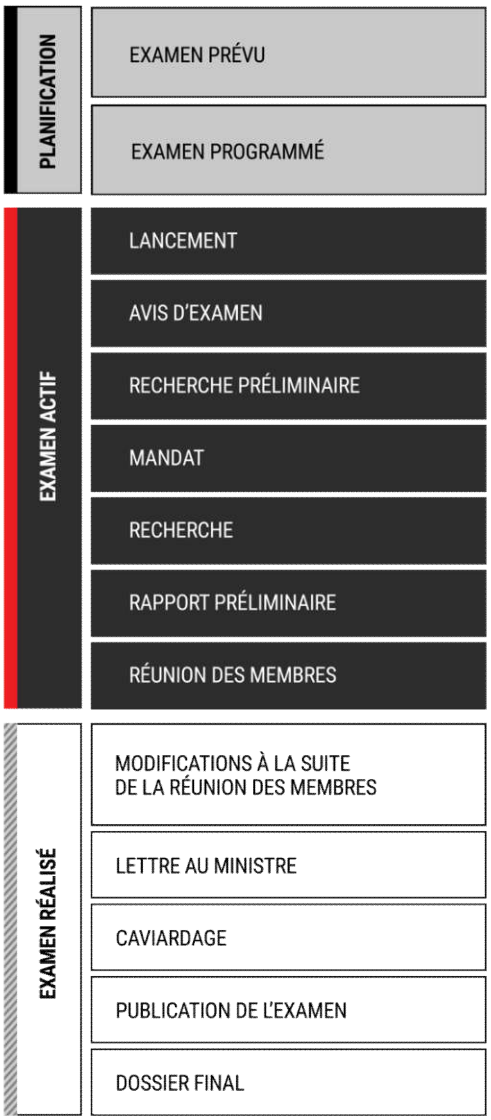
2. Un examen comporte trois grandes phases. Les phases d'examen couvrent l'ensemble du cycle de vie de l'examen, du début à la fin. Il s'agit des phases « planification de l'examen », « examen actif » et « examen réalisé ». Les étapes d'examen représentent le processus chronologique à suivre. La figure 2 illustre les différentes phases d'examen et les étapes d'examen correspondantes.

Processus d'examen

3. Bien que les étapes du processus d'examen doivent être suivies chronologiquement, certaines d'entre elles peuvent se chevaucher. Par exemple, si la recherche préliminaire peut commencer à l'étape de lancement, elle peut chevaucher l'étape de recherche principale, ou la rédaction du rapport peut commencer à une étape antérieure du processus global.

4. Chaque étape du processus d'examen intègre une multitude d'éléments supplémentaires nécessaires à la réalisation d'un examen. L'OSSNR a pour objectif d'affiner et d'améliorer continuellement son processus d'examen afin de produire les examens les plus cohérents, objectifs et rigoureux possible.

Fig. 2 Processus d'examen de l'OSSNR : Phases et étapes



Annexe D : Coup d'œil sur les examens de 2020

5. La présente annexe dresse une liste succincte des examens que l'OSSNR a achevés, lancés ou menés en 2020. Dans les tableaux ci-dessous, la « date de début » renvoie au mois auquel l'OSSNR a finalisé son mandat pour un examen donné, tandis que la « date d'achèvement » renvoie au mois auquel le rapport définitif d'un examen a été approuvé par les membres de l'OSSNR[45].

Examens achevés en 2020

Nom de l'examen	Date de début	Date d'achèvement
Examens visant le Service canadien du renseignement de sécurité (SCRS)		
Relation entre le SCRS et la GRC dans une région du Canada dans l'optique d'une enquête en cours	10/2019	12/2020
Activités de réduction de la menace	07/2020	12/2020
Examens visant le Centre de la sécurité des télécommunications (CST)		
Communication d'information nominative sur un Canadien aux partenaires canadiens	09/2019	10/2020
Autorisations ministérielles et arrêtés ministériels en vertu de la Loi sur le CST	12/2019	10/2020
Politiques et procédures de conservation des données relatives au renseignement électromagnétique	07/2020	12/2020
Examens visant d'autres ministères		
Unité nationale de contre-ingérence des Forces canadiennes	12/2019	12/2020
Examen visant Affaires mondiales Canada	02/2020	12/2020
Examens interministériels		
Mise en œuvre de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* pour 2019	08/2020	12/2020
Communication d'information en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*	03/2019	11/2020

Annexe E : Constatations et recommandations formulées dans le cadre des examens

La présente annexe énumère les constatations et les recommandations formulées par l'OSSNR pour les examens dont il est question dans le présent rapport annuel, ainsi que les réponses de la direction des entités examinées à ses recommandations, dans la mesure du possible au moment de la publication du présent rapport[46]. L'OSSNR a l'intention de publier cette information et d'en assurer le suivi pour tous les examens publiés sur son site Web.

Examens visant le Service canadien du renseignement de sécurité

Examen de la relation entre le Service canadien du renseignement de sécurité et la Gendarmerie royale du Canada dans une région du Canada dans l'optique d'une enquête en cours

Constatations de l'OSSNR

1. Depuis 2019, on constate qu'il y a des lacunes dans la collecte de renseignements par le SCRS concernant une menace en particulier.
2. La dépendance à l'égard d'un éventail restreint d'information a créé des lacunes dans l'enquête sur la menace en question.
3. Le manque d'outils de communication sécurisés utilisables et compatibles rend la coordination des activités du SCRS et de la GRC dans la région excessivement lourde et chronophage.
4. Malgré les défis persistants liés à l'échange d'information et aux structures de gouvernance, le SCRS et la GRC ont établi une relation solide qui a favorisé l'efficacité de la coordination tactique dans la région.
5. Les questions fondamentales liées au problème du passage du renseignement à la preuve ne sont toujours pas résolues. Dans l'enquête régionale en question, malgré les fréquentes communications verbales d'information entre le SCRS et la Direction générale de la GRC, les communications officielles d'information par le SCRS ont été limitées et pas toujours utiles. Les renseignements du SCRS n'ont pas été échangés ou utilisés d'une manière qui a fait avancer de façon significative les enquêtes de la GRC.

6. L'Examen relatif à l'amélioration opérationnelle a reçu l'appui de la haute direction du SCRS et de la GRC et des travaux sont en cours pour évaluer et mettre en œuvre ses recommandations.

Recommandations de l'OSSNR et réponse du SCRS et de la GRC

Recommandations	Réponse du SCRS et de la GRC (juin 2021)
L'OSSNR recommande que le SCRS investisse les ressources nécessaires afin de mettre au point un plus large éventail d'information afin d'éviter que l'enquête examinée ne subisse d'autres préjudices graves.	En raison de la variété de facteurs qui entrent en jeu dans chaque enquête, le Service tente toujours de trouver les meilleurs moyens de recueillir de l'information et d'atténuer les menaces à l'aide de divers outils et ressources, selon la situation, conformément à la *Loi sur le SCRS* et aux instructions du ministre.
L'OSSNR recommande au SCRS et à la GRC d'accorder la priorité au déploiement de systèmes de communication sécurisés utilisables et compatibles afin de rendre plus efficace la coordination à l'échelle régionale.	Le SCRS et la GRC priorisent la mise en œuvre de moyens de communication sécuritaires et compatibles. Le directeur du SCRS et la commissaire de la GRC ont approuvé la Stratégie de communication sécuritaire du SCRS et de la GRC, maintenant en cours d'exécution.
L'OSSNR recommande au SCRS et à la GRC de continuer à accorder la priorité à une mise en œuvre rapide des recommandations formulées dans le cadre de l'Examen relatif à l'amélioration opérationnelle afin d'aider à combler les lacunes opérationnelles signalées par l'Examen relatif à l'amélioration opérationnelle et illustrées plus en détail dans le présent examen.	Le SCRS et la GRC réitèrent leur engagement concernant la mise en œuvre des recommandations résultant du PAO et leur volonté d'aller de l'avant avec le projet Une vision 3.0. Le PAO est à l'origine de 76 recommandations, dont certaines visant à parfaire la collaboration et la communication d'informations dans le cadre des enquêtes liées à la sécurité nationale, à fournir plus de formation aux membres du personnel chargé de la sécurité nationale et à améliorer le traitement et la communication d'informations sensibles et classifiées. Beaucoup de travail a été fait pour s'assurer que les recommandations soient adoptées et mises en œuvre dans les deux organisations. Les premières réalisations

	incluent le projet pilote portant sur les pistes d'enquête qui a contribué à améliorer l'harmonisation des opérations liées à la sécurité nationale du SCRS et de la GRC. La GRC et le SCRS continuent d'appuyer pleinement la mise en œuvre de ces changements nécessaires au sein de leurs organisations. Grâce à ce travail et aux efforts de la communauté du renseignement, le Gouvernement du Canada s'assurera d'avoir une assise solide pour une collaboration renforcée et de meilleurs outils pour atténuer les menaces et assurer la sécurité publique. Toutefois, ce travail complexe est toujours en cours et il reste des défis à surmonter, surtout sur le plan du renseignement et de la preuve. Ces défis importants nécessiteront une démarche pangouvernementale pour être résolus.
L'OSSNR recommande que le SCRS et la GRC élaborent une stratégie complémentaire dotée de ressources suffisantes pour faire face à la menace examinée dans le présent rapport. Conformément à la vision énoncée dans l'Examen relatif à l'amélioration opérationnelle, la stratégie devrait tenir compte de toute la gamme d'outils dont disposent les deux organismes.	Le SCRS et la GRC se coordonnent et collaborent lorsqu'il est question des menaces à la sécurité nationale et utilisent les stratégies et les ressources qui conviennent le mieux à chaque opération. Grâce aux mesures mises en place à la suite du PAO, le SCRS et la GRC sont davantage en contact et collaborent plus tôt dans les processus d'enquête, ce qui a réduit le chevauchement des efforts.

Examen des activités de réduction de la menace du SCRS

Constatations

1. En ce qui concerne les types de mesures de réduction de la menace (MRM) examinées, l'OSSNR a constaté que le SCRS a satisfait aux exigences énoncées dans les directives ministérielles, telles qu'elles sont décrites dans les politiques et procédures du SCRS.

2. L'OSSNR a constaté que le SCRS a mené un petit nombre d'entrevues d'une manière qui n'était pas juste et adaptée, comme l'exige le paragraphe 12.1(2) de la Loi sur le SCRS.
3. Pour une MRM en particulier, l'OSSNR a constaté que la méthode utilisée par le SCRS pour sélectionner les individus à inclure dans la MRM traduisait un lien rationnel fort entre la menace et la mesure.
4. L'OSSNR a constaté que le SCRS ne dispose pas d'un processus officiel et documenté orientant l'identification et la sélection des sujets à inclure dans les MRM qui assure une reddition de comptes adéquate pour ces activités.
5. L'OSSNR estime que la mise en œuvre de certaines MRM était le résultat de circonstances particulières.
6. Pour un certain type de MRM, l'OSSNR estime que les exigences énoncées dans l'instruction ministérielle ont été respectées.
7. L'OSSNR a constaté que le SCRS ne s'est pas suffisamment penché sur la question de savoir si un droit garanti par la *Charte* serait limité par la MRM examinée.
8. *Cette constatation ne peut être divulguée dans un rapport public.*
9. *Cette constatation ne peut être divulguée dans un rapport public.*

Recommandations de l'OSSNR et réponse du SCRS

Recommandations	Réponse du SCRS (août 2021)
L'OSSNR recommande que le SCRS crée un cadre de responsabilisation pour l'information liée aux MRM, et que cette information soit documentée et conservée dans un endroit central où il est facile de la récupérer.	Le cadre de gouvernance rigoureux du SCRS qui a trait à l'autorisation des mesures de réduction de la menace (MRM) a fait l'objet d'un examen par le Comité de surveillance des activités de renseignement de sécurité (CSARS) et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). Suite à ces examens, des modifications considérables ont été apportées aux directives qui régissent les MRM. Le SCRS est en train d'élaborer un outil plus perfectionné de gestion des dossiers organisationnels. En attendant, le Service prend des mesures temporaires pour

	appliquer les recommandations de l'OSSNR. Enfin, il emploie des méthodes de communication additionnelles pour bien faire connaître les exigences relatives aux MRM.
L'OSSNR recommande que le SCRS crée un processus officiel et documenté qui garantit que les faits pertinents concernant les personnes visées par les MRM sont fournis au Groupe litiges et conseils en sécurité nationale (GLCSN) afin qu'il dispose des renseignements nécessaires pour fournir un avis juridique réfléchi sur l'identification et la sélection des personnes interrogées à inclure dans les MRM.	Le SCRS et le ministère de la Justice ont une relation de collaboration qui favorise la discussion et permet un dialogue permanent. Quand la législation a confié au SCRS la mission de réduire la menace, le SCRS a travaillé étroitement avec le ministère de la Justice pour mettre en place un cadre de gouvernance adapté et rigoureux. Ce cadre comprend un processus officiel et étayé d'évaluation du risque juridique, ainsi que des directives pratiques concernant la pertinence de l'information et le niveau de détail requis dans les demandes d'approbation des mesures de réduction de la menace (MRM). Le SCRS fait appel au ministère de la Justice pour vérifier que toutes les exigences inscrites dans la *Loi sur le SCRS* soient respectées, notamment le fait que les mesures en question doivent être justes et adaptées aux circonstances et qu'il faut demander des mandats au besoin. Le Service s'assure que ces conseils soient appliqués pour que les MRM soient légales et conformes à toutes les lois canadiennes, y compris la *Charte canadienne des droits et libertés*.
L'OSSNR recommande que le SCRS élabore un cadre de responsabilisation pour le respect des avis juridiques sur les MRM, y compris la documentation des cas où les avis juridiques n'ont pas été suivis et des raisons pour lesquelles ils ne l'ont pas été.	Le cadre de conformité du SCRS permet de signaler les cas possibles de non-conformité aux directives ministérielles, aux politiques et procédures internes, et à la loi. Quand de tels cas se présentent, l'équipe du programme de la conformité du SCRS est en mesure d'effectuer les enquêtes nécessaires et de consulter le ministère de la Justice.

	Le ministère de la Justice formule des avis pour que les mesures de réduction de la menace (MRM) respectent la législation et les droits de la population canadienne. Le SCRS applique rigoureusement les principes et les conseils obtenus dans l'exécution de toutes les MRM. Bien que le ministère de la Justice ne donne pas de directive tactique explicite sur la conduite de ces MRM dans ses avis, le SCRS tient compte de tous les conseils du ministère dans ses délibérations sur ses opérations.
L'OSSNR recommande que, lorsqu'il s'agit de déterminer si un droit garanti par la Charte est limité par une proposition de MRM, le GLCSN entreprenne une analyse au cas par cas qui évalue les facteurs identifiés dans notre rapport.	Le ministère de la Justice étudiera de façon plus approfondie cette recommandation et en tiendra compte dans ses travaux relatifs aux mesures de réduction de la menace (MRM) prises en vertu de la *Loi sur le SCRS*. Le SCRS et le ministère de la Justice continueront de renforcer leur collaboration établie depuis longtemps dans le but d'améliorer et de perfectionner la gouvernance applicable aux MRM.

Examens visant le Centre de la sécurité des télécommunications

Examen de la communication d'information nominative sur un Canadien aux partenaires canadiens par le CST

Constatations de l'OSSNR

1. L'OSSNR a constaté que les membres du personnel du CST chargés de la communication ne reçoivent pas suffisamment de formations et de directives écrites et qu'ils ne sont pas tenus de documenter les principales mesures qu'ils prennent et les évaluations qu'ils mettent en œuvre lorsqu'ils communiquent de l'INC.
2. L'OSSNR a constaté que le CST n'a pas évalué suffisamment en profondeur les pouvoirs légaux invoqués par ses clients.

3. L'OSSNR a constaté que la mise en œuvre par le CST de son régime de communication n'était peut-être pas conforme à ses obligations prévues par la *Loi sur la protection des renseignements personnels*.
4. L'OSSNR a constaté que la gestion du régime de communication d'INC du CST ne favorise pas un arrangement où ses clients peuvent assumer une responsabilité égale en matière de communication et de collecte des renseignements personnels concernant des Canadiens.
5. L'OSSNR a constaté que la Cour fédérale n'a pas été pleinement informée de la communication par le CST de renseignements personnels sur des Canadiens, particulièrement en ce qui a trait aux fonctionnaires canadiens, découlant des mandats qu'il délivre au SCRS en vertu de l'article 16 de la Loi sur le SCRS. L'OSSNR a constaté que les pratiques du CST en matière de communication contredisent les principes clés que le SCRS avait déjà exposés à la Cour.

Recommandations de l'OSSNR et réponse du CST

Recommandations	Réponse du CST (juin 2021)
Le CST devrait renforcer la rigueur de ses pratiques internes relatives à l'information nominative sur un Canadien (INC). Tout d'abord, le CST devrait actualiser ses politiques pour exiger de son personnel qu'il documente ses évaluations et les motifs pour lesquels il approuve ou refuse les demandes de communication.	Le CST accepte la recommandation. Le CST en est aux dernières étapes de la mise en œuvre d'une version actualisée de son logiciel de demande d'INC. Le nouveau logiciel nécessitera la saisie et la documentation des motifs des décisions relatives à la communication d'INC.
Le CST devrait améliorer davantage le système de demande d'INC pour faire en sorte que les clients soient obligés d'énoncer clairement leurs pouvoirs légaux en matière de collecte d'information et les justifications opérationnelles pour recueillir de l'INC.	Le CST accepte la recommandation. Le CST en est aux dernières étapes de la mise en œuvre d'une version actualisée de son logiciel de demande d'INC, qui garantira que les renseignements nécessaires sont obligatoirement saisis.
Le CST devrait veiller à ce que le rôle de ses agents des relations avec la clientèle se limite à faciliter la communication d'INC uniquement lorsque les clients le demandent explicitement.	Le CST accepte la recommandation. Les agents des relations avec la clientèle continueront à faciliter la communication d'INC uniquement en réponse aux demandes des clients. Une formation supplémentaire est en cours d'élaboration afin de garantir une documentation adéquate de ces demandes.

Le CST devrait former les analystes de la communication à évaluer le fond et la validité des demandes de communication d'INC. Plus particulièrement, le CST devrait donner de la formation aux analystes de la communication sur la législation et les politiques applicables en matière de protection de la vie privée ainsi que sur les limites associées à l'échange de renseignements personnels.	Le CST accepte la recommandation. Le CST, en collaboration avec les Services juridiques, a élaboré du matériel de formation supplémentaire pour améliorer le programme de formation existant des analystes de la communication. Cette formation supplémentaire sera mise en place au cours des prochaines semaines.
Le CST et ses clients du gouvernement du Canada qui demandent de l'INC devraient d'abord obtenir un avis juridique du ministère de la Justice concernant les pouvoirs de collecte d'information pouvant justifier la collecte de renseignements personnels.	Le CST accepte la recommandation. Le CST travaille actuellement à la révision de ses procédures normales d'exploitation, lesquelles seront éclairées par les réponses reçues par le CST à la correspondance envoyée relativement à la recommandation no 5.
Le CST devrait réviser ses procédures normales d'exploitation pour tenir compte des avis juridiques qu'il reçoit en réponse à la recommandation no 5.	Le CST accepte la recommandation. Le CST a envoyé une correspondance à ses ministères clients, soulignant les domaines de responsabilité et suggérant que le client, ainsi que ses propres services juridiques, confirme leur autorité légale de demander et de recevoir des INC.
L'OSSNR recommande que le CST cesse de communiquer de l'INC à des clients autres que le SCRS, la GRC et l'Agence des services frontaliers du Canada (ASFC) jusqu'à ce qu'il mette en œuvre les recommandations contenues dans le présent rapport.	Le CST accepte la recommandation. Les demandes adressées aux organismes autres que le SCRS, la GRC et l'ASFC sont traitées en collaboration avec le DLS afin d'examiner les autorisations fournies par les institutions requérantes.
L'OSSNR recommande que le CST collabore avec le ministère de la Justice, le Secrétariat du Conseil du Trésor du Canada et ses clients habituels du gouvernement du Canada afin de conclure des ententes sur l'échange d'information. Ces ententes devraient aborder clairement la question des rôles, des responsabilités et des pouvoirs légaux de chaque partie en matière de collecte et de communication d'INC, ainsi que la question des normes que chaque communication doit respecter.	Le CST accepte la recommandation. Le CST a déjà envoyé une correspondance à ses ministères clients soulignant les domaines de responsabilité et suggérant que le client, de concert avec les services juridiques de son propre ministère, confirme son pouvoir légal de demander et de recevoir de l'INC. Des discussions ont eu lieu avec le Secrétariat du Conseil du Trésor sur l'utilisation de l'INC avec les clients.

L'OSSNR recommande qu'une évaluation des facteurs relatifs à la vie privée soit entreprise en ce qui concerne le régime de communication d'INC du CST.	Le CST accepte la recommandation. Le CST a entamé une évaluation des facteurs relatifs à la vie privée.
Le SCRS, le CST et le procureur général du Canada devraient informer pleinement la Cour fédérale des pratiques du CST en matière de communication d'INC et des pratiques connexes découlant des mandats délivrés par la Cour.	Le CST accepte la recommandation. Le CST a travaillé étroitement de concert avec le SCRS pour fournir à la Cour fédérale les renseignements nécessaires.
L'OSSNR recommande que le CST cesse de communiquer de l'INC recueillie en vertu de l'article 16 de la Loi sur le SCRS jusqu'à ce que la Cour fédérale soit pleinement informée au sujet de la communication par le CST d'information provenant des mandats délivrés par le SCRS en vertu de l'article 16. D'ici là, le CST devrait inclure dans ses rapports de renseignements en vertu de l'article 16 un message aiguillant vers le SCRS les personnes demandant de l'INC.	Le CST accepte la recommandation. Toutes les demandes d'INC en vertu de l'article 16 de la Loi sur le SCRS sont examinées et approuvées par le SCRS.

Examen des autorisations ministérielles et des arrêtés ministériels du CST en vertu de la Loi sur le CST

Constatations de l'OSSNR

1. Les demandes d'autorisations ministérielles du chef du CST ont fourni au ministre suffisamment d'information pour satisfaire aux conditions prévues par le paragraphe 33(2) de la Loi sur le CST. Les nouvelles demandes fournissent plus d'information que les demandes précédentes en vertu de la *Loi sur la défense nationale*, et permettent de faire en sorte que les activités du CST soient plus transparentes.
2. Bien que ces activités n'aient pas encore eu lieu, rien n'indique que le CST ait pleinement évalué les ramifications – légales ou autres – des activités autorisées par un certain type d'autorisation.
3. Les lettres de 2019 relatives à la consultation du ministre de la Défense nationale avec le ministre des Affaires étrangères pour les cyberopérations actives et

défensives n'étaient pas datées. Cette activité de consultation spécifique avec AMC n'était pas suffisamment documentée.

4. Le CST n'a pas été en mesure de fournir une évaluation de ses obligations en vertu du droit international se rapportant à la réalisation de cyberopérations actives.
5. L'arrêté ministériel désignant les destinataires de l'information nominative sur un Canadien obtenue, utilisée et analysée en vertu d'une autorisation ministérielle relative au renseignement étranger n'était pas suffisamment détaillée.

Recommandations de l'OSSNR et réponse du CST

Recommandations	Réponse du CST (mai 2020)
Le CST devrait demander une évaluation juridique complète des activités autorisées par une autorisation de renseignement étranger spécifique avant d'entreprendre toute activité de collecte en vertu de cette autorisation ministérielle. L'avis juridique devrait aborder la question de savoir s'il existe un régime de justification implicite créé dans l'autorisation ministérielle.	Le CST accepte cette recommandation en principe. Le CST estime que toutes les activités autorisées par cette autorisation ministérielle ont une autorité explicite, comme le stipule l'article 3 de la *Loi sur le Centre de la sécurité des télécommunications* (Loi sur le CST), et que ces activités sont justes et adaptées, et relèvent d'une autorisation délivrée par le ministre et approuvée par le commissaire au renseignement. En outre, les évaluations juridiques font partie intégrante du processus d'élaboration de l'autorisation, l'avocat des Services juridiques faisant partie de l'équipe chargée de l'élaboration de l'autorisation.
Le CST devrait s'assurer que le processus de consultation relatif aux cyberopérations actives et aux cyberopérations défensives auprès d'AMC est documenté de manière aussi précise que possible afin de permettre une vérification facile de sa conformité à l'ordre requis par la Loi sur le CST.	Le CST prend acte de cette recommandation et la considère comme résolue.
Le CST devrait demander une évaluation juridique formelle du régime juridique international applicable à la réalisation de cyberopérations actives avant d'entreprendre de telles opérations.	Le CST n'accepte pas cette recommandation. Le CST convient que ses opérations devraient être évaluées du point de vue de la conformité au droit international, mais il continue de contester l'affirmation de l'OSSNR selon laquelle il n'a pas été en mesure de fournir une évaluation de ses obligations en vertu du droit international. Le CST continuera de travailler avec diligence avec le

	conseiller juridique du ministère de la Justice et AMC en ce qui concerne les cyberopérations étrangères.
Une ordonnance rendue en vertu de l'article 45 de la Loi sur le CST doit être aussi précise que possible en détaillant clairement la liste des personnes ou des catégories de personnes désignées pour recevoir de l'INC communiquée par le CST. Information disclosed by CSE.	Le CST accepte cette recommandation et note que les arrêtés ministériels actualisés du CST ont abordé cette question. Dans le but de promouvoir une transparence accrue et de faciliter les communications externes, les trois arrêtés ministériels du CST ont été remaniés en 2020 à un niveau de sécurité non classifié. Présentés au CST par le ministre en août 2020, les arrêtés ministériels du CST ont satisfait à l'objectif et à l'esprit de cette recommandation bien avant l'achèvement du rapport d'examen de l'OSSNR.

Examen du Dossier relatif aux incidents liés à la vie privée du CST (2019)

Il convient de noter que cet examen a porté sur le Dossier relatif aux incidents liés à la vie privée du CST en 2019, mais qu'il est inclus dans la présente annexe parce qu'il présente de l'information que l'OSSNR n'était pas en mesure de publier auparavant – à savoir les réponses du CST aux recommandations de l'OSSNR. Les conclusions de l'examen de 2019 du Dossier relatif aux incidents liés à la vie privée du CST sont publiées dans l'examen en ligne[47].

Recommandations de l'OSSNR et réponse du CST

Recommandations	Réponse du CST (mars 2020)
Le CST devrait examiner la totalité des incidents liés à la vie privée en vue de déterminer les tendances systémiques ou les points faibles des politiques ou des pratiques en place.	Le CST accepte la recommandation. Le CST s'efforcera de renforcer son utilisation du régime de gestion des incidents liés à la vie privée comme source d'information pour contribuer à l'élaboration de politiques et pour déterminer quelles améliorations il est possible d'apporter aux pratiques existantes.
Les équipes chargées de la conformité opérationnelle devraient s'inspirer des pratiques exemplaires de leurs homologues en matière de production de rapports uniformes sur les incidents liés à la vie privée, de sorte qu'un	Le CST accepte la recommandation. Le CST cherche à mettre en place un mécanisme normalisé pour la saisie, l'enregistrement et le signalement des incidents ayant des conséquences sur la vie privée. Le CST étudie une série de solutions

rapport d'incident soit rempli pour chaque incident ayant des conséquences sur la vie privée de Canadiens.	politiques, procédurales et techniques afin de parvenir à des rapports plus uniformes entre les secteurs d'activité, le cas échéant et au besoin. Un tel mécanisme tiendrait également compte des différences opérationnelles entre les activités liées aux renseignements électromagnétiques étrangers et celles du Centre canadien pour la cybersécurité.
Le CST devrait toujours examiner ce qui a déjà été fait avec l'information présentant un intérêt au chapitre de la vie privée de Canadiens, afin de déterminer si d'autres mesures d'atténuation sont justifiées dans les circonstances d'un incident spécifique lié à la vie privée.	Le CST accepte la recommandation. En évaluant la meilleure façon d'atteindre le résultat demandé dans cette recommandation, le CST étudie une série de solutions stratégiques, procédurales et techniques.
Le CST devrait normaliser la politique sur la manière d'évaluer si un incident lié à la vie privée constitue une atteinte substantielle à la vie privée. En outre, après une évaluation des renseignements personnels sensibles, le CST devrait élaborer des méthodes pour analyser si un préjudice ou un dommage important s'est produit, qui ne soit pas déclenché uniquement par le fait qu'une demande d'intervention a été traitée.	Le CST accepte la recommandation. Le CST cherchera à améliorer et à normaliser sa documentation permettant de déterminer si un incident lié à la vie privée constitue une atteinte importante à la vie privée. Le CST réexaminera également les éléments utilisés dans son évaluation pour s'assurer qu'ils sont efficaces et raisonnables.
Le CST devrait abolir une pratique spécifique. S'il devait continuer à utiliser cette pratique comme mesure d'atténuation, le CST devrait obtenir un avis juridique sur la légalité de cette pratique.	Le CST accepte la recommandation. Le CST a aboli cette pratique en novembre 2019.

Examens visant les autres ministères

Examen de l'Unité nationale de contre-ingérence des Forces canadiennes (UNCIFC)

Constatations de l'OSSNR

1. L'OSSNR a constaté que l'un des principaux obstacles à la viabilité de l'expertise de l'UNCIFC en matière d'enquête est le taux élevé de roulement du personnel et la dépendance excessive à l'égard du mentorat.

2. L’OSSNR a constaté que l’UNCIFC a respecté les politiques internes utilisées pour lancer des enquêtes, et que ces déterminations étaient raisonnables et nécessaires dans ces circonstances particulières.
3. L’OSSNR a constaté que l’UNCIFC ne dispose pas d’un processus officiel et documenté orientant l’établissement de l’ordre de priorité des enquêtes.
4. L’OSSNR a constaté que la structure institutionnelle et les décisions de gestion du MDN et des FAC ne permettent pas à l’UNCIFC d’utiliser pleinement ses capacités d’enquête prévues par la loi.
5. L’OSSNR a constaté que, lorsque l’UNCIFC examine la nature du droit à la vie privée d’un sujet, elle n’évalue pas adéquatement ses activités en tenant compte de l’ensemble des circonstances.
6. L’OSSNR a constaté que la durée des enquêtes va à l’encontre d’une saine protection de l’information, des personnes et des actifs du MDN et des FAC.
7. L’OSSNR a constaté que le régime d’échange d’information de l’UNCIFC n’est pas toujours conforme aux politiques du gouvernement du Canada ayant trait à la protection de l’information.
8. L’OSSNR a constaté que l’UNCIFC et d’autres composantes de sécurité du MDN et des FAC ont été organisés de manière à former des cloisonnements verticaux très ciblés qui ne sont pas conçus pour travailler de façon intégrée.
9. L’OSSNR a constaté que l’UNCIFC n’a pas clairement défini ses pouvoirs juridiques en matière d’échange d’information à l’appui des processus administratifs et liés aux activités criminelles.
10. L’OSSNR a constaté que le fait de ne pas transmettre de rapport définitif aux intervenants concernés n’assure pas une responsabilisation adéquate des activités d’enquête de l’UNCIFC.
11. L’OSSNR a constaté que les enquêtes de l’UNCIFC ne font pas l’objet d’une surveillance adéquate.
12. L’OSSNR a constaté que la suprématie blanche et l’extrémisme violent motivé par une idéologie constituent une menace active de contre-ingérence pour le MDN et les FAC et que le mandat de l’UNCIFC pour cerner de façon proactive cette menace est limité.

Recommandations de l'OSSNR

1. L'OSSNR recommande que l'UNCIFC crée un processus formel et documenté qui aide à établir l'ordre de priorité des enquêtes en fonction de critères pertinents (p. ex. les ressources, la valeur de l'enquête, les priorités institutionnelles ainsi que les préoccupations opérationnelles, juridiques et liées à la politique étrangère).
2. L'OSSNR recommande que le MDN et les FAC habilitent l'UNCIFC à utiliser pleinement ses capacités d'enquête légales, ce qui pourrait inclure des activités moins intrusives.
3. L'OSSNR recommande que l'UNCIFC demande conseil au CPVP pour s'assurer que les activités d'enquête respectent toutes les pratiques exemplaires en vigueur en matière de protection de la vie privée.
4. L'OSSNR recommande que les structures d'échange et de responsabilisation de l'UNCIFC soient conformes à la Politique sur la sécurité du gouvernement.
5. L'OSSNR recommande que les activités d'enquête de l'UNCIFC soient harmonisées aux efforts déployés dans le cadre des activités de filtrage de sécurité afin de réduire les redondances.
6. L'OSSNR recommande que l'UNCIFC demande des conseils sur les pouvoirs légaux d'échanger de l'information à l'appui des processus administratifs et liés aux activités criminelles.
7. L'OSSNR recommande que l'UNCIFC crée un cadre de responsabilisation qui comprend des produits écrits approuvés qui sont transmis aux intervenants concernés.
8. L'OSSNR recommande que l'UNCIFC actualise son mécanisme de surveillance pour s'assurer qu'il est indépendant, que ses responsables se réunissent régulièrement et qu'il est appuyé par un secrétariat qui consigne adéquatement l'information pertinente.
9. L'OSSNR recommande que le MDN et les FAC clarifient le rôle de l'UNCIFC dans le cadre de la stratégie globale du MDN et des FAC sur la lutte contre les comportements haineux et extrémistes.

Réponse du MDN et des FAC aux recommandations de l'OSSNR (juin 2021)

Voici la réponse du MDN et des FAC aux recommandations de l'OSSNR contenues dans l'examen :

« Le MDN et les FAC reconnaissent l'importance de l'examen et accueillent favorablement le rapport qui en découle. Le MDN et les FAC souscrivent aux recommandations du rapport et prennent des mesures pour y donner suite. Toutes les activités de l'UNCIFC doivent être conformes à toutes les lois canadiennes applicables et respecter les dispositions de la *Charte canadienne des droits et libertés*. Bien que l'UNCIFC n'ait actuellement aucun rôle à jouer en ce qui concerne la détection et l'élimination des comportements haineux, le MDN et les FAC ont adopté une approche robuste pour faire face aux comportements haineux, y compris une nouvelle politique des FAC qui nous permettra de mieux faire face à ce problème. Comme l'a recommandé l'OSSNR, le MDN et les FAC préciseront le rôle de l'UNCIFC dans le contexte de la réponse plus générale du MDN et des FAC à l'extrémisme violent motivé par une idéologie.

L'UNCIFC a pris des mesures au cours des dernières années pour renforcer ses capacités, dont certaines concernent directement le contenu du rapport. L'UNCIFC continue d'évoluer et de s'améliorer pour répondre aux exigences d'un environnement de sécurité international, national et lié aux FAC en constante évolution. Les recommandations formulées dans ce rapport vont de changements à l'échelle de l'UNCIFC à des considérations d'ordre institutionnel, et le MDN et les FAC conviennent que des mesures seront prises aux niveaux appropriés, conjointement avec les experts et les bureaux pertinents. Le MDN et les FAC ont commencé ce travail et plusieurs des recommandations de ce rapport sont déjà en voie d'être mises en œuvre, notamment un mécanisme de suivi provisoire pour la communication d'information ainsi qu'un examen des politiques et des procédures opérationnelles pertinentes. Par ailleurs, des travaux sont en cours pour réaliser une évaluation des facteurs relatifs à la vie privée sur les activités de renseignement de défense, y compris les enquêtes sur la contre-ingérence, qui permettra d'évaluer tout risque pour les renseignements personnels dans le cadre du processus d'enquête de l'UNCIFC et de proposer des mesures d'atténuation, le cas échéant. Le MDN et les FAC feront appel au CPVP une fois que l'évaluation des facteurs relatifs à la vie privée sera terminée pour obtenir des commentaires sur les considérations liées à la protection de la vie privée, s'il y a lieu. La mise en œuvre des recommandations de l'OSSNR permettra d'améliorer davantage nos pratiques.

L'UNCIFC est une unité du Groupe du renseignement des Forces canadiennes, qui relève du Commandement du renseignement des Forces canadiennes. Le mandat de l'UNCIFC est de fournir des renseignements de sécurité et de contre-ingérence au MDN et aux FAC, tant en ce qui concerne la situation au pays qu'à l'étranger. Le mandat de l'UNCIFC est axé sur les menaces à la sécurité dans les domaines du terrorisme, de l'espionnage, de la subversion, du sabotage et des menaces à la sécurité posées par le crime organisé. L'UNCIFC mène des enquêtes dans son optique particulière et fait partie du groupe plus large d'organismes d'enquête et de sécurité qui existent au sein du MDN et des FAC. L'UNCIFC n'est pas un

organisme d'application de la loi et n'a pas le pouvoir d'enquêter sur des infractions disciplinaires ou criminelles. Cependant, elle collabore souvent avec des organismes d'application de la loi comme la police militaire ou la GRC et prendra d'autres mesures pour améliorer cette collaboration. »

Examens interministériels

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

Constatations

1. L'OSSNR a constaté que plusieurs ministères, pour qui la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* (LCMTIEE) est une nouvelle loi dont ils doivent tenir compte, ont décrit les progrès considérables réalisés au cours de la période d'examen et, par la suite, concernant l'élaboration de cadres formels pour appuyer la mise en œuvre de cette loi.
2. L'OSSNR a constaté que les ministères qui échangent très peu d'information avec des entités étrangères n'ont pas encore pleinement pris conscience de l'importance de mettre en place un cadre officiel régissant l'échange d'information.
3. L'OSSNR a constaté que les différences et la variabilité des cadres ministériels témoignent d'un manque antérieur de coordination au sein de l'appareil de la sécurité nationale et du renseignement et de la nécessité de déterminer quelles sont les pratiques exemplaires qui doivent être adoptées.
4. L'OSSNR a constaté qu'il y a des incohérences dans l'application des cadres d'échange d'information existants entre les ministères, particulièrement en ce qui concerne les seuils d'évaluation de l'information et les décisions déléguées aux cadres supérieurs.
5. L'OSSNR a constaté un manque d'uniformité et de normalisation dans les évaluations des pays et des entités utilisées par les ministères, ce qui entraîne des incohérences dans l'approche et la position adoptée par l'appareil de la sécurité nationale et du renseignement lorsqu'il interagit avec des entités étrangères préoccupantes visées par la LCMTIEE.

Recommandations de l'OSSNR

1. L'OSSNR recommande que tous les ministères qui reçoivent des directives en vertu de la LCMTIEE disposent d'un cadre officiel leur permettant d'appuyer pleinement la mise en œuvre des directives.
2. L'OSSNR recommande que les ministères se coordonnent afin de déterminer quelles sont les pratiques exemplaires à adopter pour tous les éléments essentiels des cadres sur l'échange d'information et que le Groupe de coordination d'échange de renseignements soit mis à contribution pour s'assurer que ces pratiques sont diffusées dans la mesure du possible au sein de l'appareil de la sécurité nationale et du renseignement afin d'appuyer la mise en œuvre de la LCMTIEE.
3. L'OSSNR recommande que les ministères établissent des seuils cohérents pour les éléments déclencheurs dans leurs cadres sur l'échange d'information, y compris les évaluations initiales par rapport aux préoccupations soulevées par la LCMTIEE, le moment où un cas doit être acheminé à l'échelon supérieur dans le cadre du processus décisionnel et la façon dont tout cela est documenté.
4. L'OSSNR recommande aux ministères de trouver un moyen d'établir des outils uniformes et normalisés d'évaluation des risques liés aux pays et aux différentes entités afin d'appuyer une approche cohérente des ministères lorsqu'ils interagissent avec des entités étrangères préoccupantes en vertu de la LCMTIEE.

Réponse aux recommandations de l'OSSNR (juillet 2021)

Le gouvernement du Canada souscrit généralement au fond et à l'esprit des recommandations. Voici la réponse du gouvernement aux quatre recommandations contenues dans l'examen et une description de la façon dont les ministères et organismes concernés ont l'intention de mettre en œuvre ces recommandations au cours des prochains mois :

«Le gouvernement du Canada est d'accord avec la première recommandation du rapport selon laquelle tous les ministères qui reçoivent des directives en vertu de la Loi doivent avoir un cadre officiel en place pour s'assurer qu'ils peuvent pleinement appuyer la mise en oeuvre des directives. Comme le reconnaît le rapport, au cours des quatre premiers mois de l'entrée en vigueur de la Loi, les douze ministères et organismes concernés avaient mis en place des cadres. Ces cadres sont adaptés aux circonstances particulières de chaque ministère ou organisme. Comme le rapport souligne, il y a encore de la place pour que ces cadres mûrissent. À cette fin, les ministères et organismes concernés continueront de modifier et

d'officialiser leurs cadres respectifs au besoin pour tenir compte des constatations et soutenir la mise en oeuvre complète des orientations.

Le gouvernement du Canada est d'accord avec la deuxième recommandation du rapport et convient que les ministères devraient travailler ensemble pour identifier les meilleures pratiques pour tous les éléments essentiels des cadres de partage de l'information. Le Groupe de coordination du partage de l'information de Sécurité publique Canada continuera d'être un forum bien placé pour faciliter ce travail. La communauté de la sécurité et du renseignement continuera de tirer parti du Groupe de coordination du partage d'informations pour partager les meilleures pratiques, les leçons apprises et les interprétations communes afin d'améliorer davantage les pratiques de partage d'informations et de remplir les obligations en vertu des directives.

Le gouvernement du Canada n'est que partiellement d'accord avec les troisième et quatrième recommandations du rapport. Ces recommandations soulignent l'importance d'établir des approches cohérentes dans l'ensemble de la communauté de la sécurité et du renseignement. Le gouvernement du Canada comprend le point de vue selon lequel des approches cohérentes peuvent aider à assurer une mise en oeuvre fiable des orientations. De même, la normalisation des outils d'évaluation des risques des pays et des entités de la communauté favoriserait un point de départ cohérent pour évaluer le risque généralisé d'un pays ou d'une entité étranger, minimisant potentiellement la duplication des efforts entre les organisations. Les ministères et organismes concernés continueront de tirer parti du Groupe de coordination du partage de l'information pour déterminer où l'uniformité peut être établie dans leurs processus, conformément à votre deuxième recommandation. Les ministères et organismes s'efforceront davantage de déterminer où les outils d'évaluation des risques des pays et des entités peuvent être normalisés et veilleront à ce que toutes les organisations aient accès aux outils d'évaluation des risques de base.

Cela dit, les approches standardisées ne sont pas toujours réalisables dans la pratique. Cela est particulièrement vrai lorsqu'on applique une approche à douze ministères et organismes aux activités et mandats opérationnels divers. Les activités de partage d'informations de ces organisations servent toutes à des fins de renseignement, d'application de la loi ou administratives, chacune comportant des profils de risque, des problèmes de confidentialité et des autorités légales différents. Les ministères et organismes individuels sont responsables d'établir des seuils ou des déclencheurs spécifiques dans leurs cadres de partage de l'information qui conviennent à leurs contextes opérationnels.

Le gouvernement du Canada est de l’avis qu’il n'est pas nécessairement pratique ni essentiel d'appliquer le même seuil à toutes les organisations pour déclencher, évaluer et élever des

cas pour garantir que chaque ministère ou organisme fonctionne conformément à la Loi. De même, compte tenu de la variété des mandats légaux, des activités opérationnelles et de la sensibilité des informations disponibles pour certains ministères mais pas pour d'autres, il pourrait ne pas être possible de produire une suite entièrement normalisée d'outils d'évaluation des risques disponibles pour toutes les organisations en vertu de la Loi.»

Examen de la communication d'information en vertu de la Loi sur la communication d'information ayant trait à la sécurité du Canada

En 2020, l'OSSNR a terminé son Rapport annuel de 2019 sur la communication d'information au titre de la Loi sur la communication d'information ayant trait à la sécurité du Canada[48]. Ce premier rapport n'a formulé aucune conclusion ni recommandation, mais a établi des critères pour les évaluations futures.

Annexe F : Tableau statistique – Enquêtes sur les plaintes

Enquêtes sur les plaints : Statistiques finales

Du 1er janvier 2020 au 31 décembre 2020

Demandes de traitement de plaintes reçues	**69**	
Nombre de nouvelles plaintes déposées	**26**	
Article 16 de la Loi sur l'OSSNR (plaintes visant le SCRS)	15	
Article 17 de la Loi sur l'OSSNR (plaintes visant le CST)	1	
Article 18 de la Loi sur l'OSSNR (habilitations de sécurité)	8	
Article 19 de la Loi sur l'OSSNR (plaintes visant la GRC)	2	
Article 19 de la Loi sur l'OSSNR (Loi sur la citoyenneté)	0	
Article 45 de la Loi sur l'OSSNR (Loi canadienne sur les droits de la personne)	0	
Nombre de dossiers de plaintes pour lesquels l'OSSNR a décidé d'enquêter ou non	**24**	
	Acceptés :	**Rejetés :**
(SCRS)	Art. 16 : 3	Art. 16 : 10
(Habilitations de sécurité)	Art. 18 : 0	Art. 18 : 6
(GRC)	Art. 19 : 4	Art. 19 : 1
Enquêtes actives sur les plaintes pendant cette période	**19**	
Une fois que l'OSSNR a décidé de mener une enquête…		
Enquêtes sur les plaintes reportées de l'année civile précédente	**12**	
(SCRS)	Art. 16 : 9	
(habilitations de sécurité)	Art. 18 : 2	

(GRC)	Art. 19 : 1
Nombre total d'enquêtes sur des plaintes dont le dossier est clos	**5**
Plaintes retirées ou considérées comme abandonnées	3
Plainte réglée à l'amiable	1
Enquête terminée (rapport final produit)	1
(SCRS)	Art. 16 : 3
(habilitations de sécurité)	Art. 18 : 1
(GRC)	Art. 19 : 1
Enquêtes sur les plaintes qui seront reportées à l'année civile suivante	**14**
(SCRS)	Art. 16 : 9
(habilitations de sécurité)	Art. 18 : 1
(GRC)	Art. 19 : 4

Annexe G : Valeurs et objectifs

1. L'OSSNR s'engage à :

   - faire preuve d'ouverture et de transparence pour tenir les Canadiens au fait du caractère licite et raisonnable des activités du pays en matière de sécurité nationale et de renseignement;
   - maintenir l'excellence des méthodes pour assurer la rigueur et la qualité de son approche;
   - favoriser la réflexion prospective et la pensée novatrice pour se tenir au courant et, idéalement, demeurer à l'avant-garde des nouvelles technologies et d'un environnement de sécurité nationale en constante évolution;
   - mobiliser régulièrement les partenaires, les intervenants et les membres de l'appareil;
   - être objectif et indépendant, et être perçu comme tel.

   Au cours de sa première année complète d'activité, l'OSSNR a continué à faire des progrès dans la réalisation de ces objectifs et une description complète de ses valeurs et de ses objectifs se trouve dans le *Rapport annuel 2019*.

2. L'OSSNR souhaite que les Canadiens aient confiance que la légalité, le caractère raisonnable et la nécessité des activités de sécurité nationale et de renseignement du pays font l'objet d'un examen rigoureux.

Transparence

3. La *Loi de 2017 sur la sécurité nationale* stipule « que 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[49] ». L'OSSNR s'engage donc à tenir le public informé des résultats de ses examens, enquêtes et activités, tout en protégeant l'information sensible. L'OSSNR s'efforce notamment d'améliorer l'accès du public à ses rapports et de communiquer clairement sur la manière dont il remplit son mandat.

4. À cet effet, l'OSSNR continue de travailler avec les ministères et les organismes pour s'assurer que les versions non classifiées de ses rapports d'examen, comprenant ses constatations et ses recommandations, sont publiées et mises à la disposition du public. Certains des rapports d'examen de l'OSSNR peuvent maintenant être consultés sur son nouveau site Web remanié[50].

5. Depuis son dernier rapport annuel, l'OSSNR a publié de manière proactive des rapports d'examen non classifiés sur :

    - les erreurs de procédure et les incidents liés à la vie privée autosignalés par le CST;
    - la mise en œuvre par les ministères de mesures liées à la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* pour 2019;
    - l'échange d'information nominative sur un Canadien par le CST.

6. En outre, l'OSSNR a commencé à caviarder, à déclassifier et à publier les rapports antérieurs du Comité de surveillance des activités de renseignement de sécurité, l'ancien organe dédié à la surveillance des activités du Service canadien du renseignement de sécurité (SCRS). L'OSSNR a déjà publié l'équivalent d'une décennie d'examens et continue de collaborer avec le SCRS pour déclassifier les rapports restants et les publier dès qu'ils seront disponibles. L'OSSNR a toutefois connu des retards dans ces efforts en raison de la pandémie.

7. L'OSSNR prévoit lancer de nouveaux outils de recherche sur son site Web, qui héberge ces rapports, afin de faciliter la navigation dans ses bases de données en ligne contenant les publications et les examens récents et anciens. Son nouveau site Web vise également à mieux faire connaître l'OSSNR et son mandat, à expliquer son processus d'examen, à fournir un processus facile pour soumettre des plaintes en ligne et à encourager les intervenants à collaborer avec l'OSSNR. L'OSSNR s'est également créé un compte Twitter pour informer le public au sujet de ses activités.

8. Enfin, l'OSSNR a récemment publié une nouvelle politique sur la diffusion de versions non classifiées et dépersonnalisées des rapports d'enquête finaux[51]. L'objectif de cette politique est d'améliorer l'accès au processus d'enquête de l'OSSNR, renforçant ainsi son mandat de responsabilité publique. En rendant publics les rapports déclassifiés et dépersonnalisés, l'OSSNR espère encourager les discussions et les débats ouverts.

9. En plus de ses propres initiatives visant à renforcer la responsabilité et la transparence, l'OSSNR continuera d'encourager les ministères et les organismes à promouvoir la transparence de leurs activités de sécurité nationale et de renseignement, notamment pour respecter l'engagement de transparence en matière de sécurité nationale[52].

Anticipation du risque

10. En tant qu'organisme qui a récemment pris de l'expansion et embauché des personnes de talent provenant d'horizons divers, l'OSSNR a l'avantage de pouvoir influer sur les attitudes de ces derniers afin de développer une culture qui lui est propre. La diversité des origines, culturelles et professionnelles, des employés de l'OSSNR lui permet de jouir d'une pluralité d'expertises et d'expériences, donc d'un vaste éventail d'idées et d'opinions. Cet éventail d'expertises, d'expériences, d'idées et d'opinions est complété par la recherche de pratiques exemplaires en matière d'examen fondées sur les expériences d'autres pays et par le recours à une formation interne originale.

11. Ainsi, l'OSSNR dispose des outils nécessaires pour anticiper les différents risques qui sont couverts par le mandat de chacune des entités examinées. Les examinateurs peuvent poser les bonnes questions, ce qui leur permet de reconnaître les habitudes et les comportements systémiques des entités examinées et d'en rendre compte aux intervenants avec transparence et d'une manière conforme à leurs attentes. Plus précisément, pour ce faire, les examinateurs doivent non seulement avoir des attentes claires concernant les politiques et procédures que les entités devraient avoir adoptées et mises en œuvre, mais ils doivent également anticiper les risques auxquels les entités font face et ceux sur lesquels elles travaillent ou devraient travailler, que ce soit à des fins de renseignement ou de prévention. En d'autres termes, l'anticipation du risque fait partie de la culture de l'examinateur.

12. En résumé, la culture de l'anticipation est inhérente à la quête d'excellence méthodologique de l'OSSNR et à son programme de recrutement et de formation, et fait également partie de ses relations avec ses partenaires étrangers et les différents intervenants.

Objectivité et indépendance : une approche impartiale

13. L'objectif de l'OSSNR est d'aborder tous ses examens avec objectivité et de manière impartiale. L'OSSNR ne recherche pas un résultat particulier lorsqu'il effectue un examen; au contraire, il se préoccupe uniquement de la manière dont l'examen est mené et présenté. Cette « indifférence » professionnelle à l'égard des résultats signifie que l'OSSNR est libre de se concentrer sur l'information qu'il demande et évalue.

14. Chaque examen porte sur des questions spécifiques; l'information que l'OSSNR cherche à obtenir auprès des ministères et des organismes et à examiner l'aide à

trouver des réponses. L'OSSNR pose à la fois les questions que le public lui demande de poser et celles que l'OSSNR est tenu de poser en vertu des dispositions de son mandat. Le renforcement continu de son processus et de sa méthodologie d'examen garantira que cette approche est exécutée de la manière la plus cohérente possible dans tous ses examens.

15. Bien que la confiance du public et la transparence soient importantes, il est également primordial que les entités examinées soient convaincues que l'OSSNR collabore avec elles de manière impartiale; les entités examinées doivent être convaincues que lorsqu'elles soumettent leurs programmes et leurs activités à un examen minutieux, ces derniers feront l'objet d'une évaluation impartiale. Ce type de relation constitue la base d'un examen qui peut être utile à la fois pour le public et le gouvernement.

16. Dans ce sens, l'OSSNR croit qu'il y a autant de valeur dans un examen qui a des conclusions positives que dans un examen qui met en évidence des problèmes nécessitant une attention particulière.

17. Une approche véritablement impartiale va de pair avec des principes tels que l'indépendance, la transparence et la méthodologie « faire confiance, mais vérifier ». Il doit y avoir des obligations et des considérations des deux côtés de la relation d'examen et de surveillance si l'OSSNR souhaite maximiser la valeur et l'efficacité de ses examens. Le personnel de l'OSSNR est conscient de ses obligations à cet égard et continuera d'étudier les moyens d'améliorer et de mieux jouer son rôle dans cette relation vitale.

Excellence méthodologique

18. L'OSSNR souhaite améliorer la capacité de l'appareil de la sécurité nationale et du renseignement du Canada à mener ses activités d'une manière conforme à la loi, aux directives ministérielles et aux politiques opérationnelles appropriées. Pour ce faire, l'OSSNR doit :

    - avoir la compréhension requise de l'environnement opérationnel et des exigences légales applicables;
    - s'engager continuellement dans un apprentissage itératif;
    - s'assurer que ses processus d'examen et d'enquête sont transparents et clairs;
    - s'assurer que toute l'information pertinente est mise à disposition lors de la réalisation des examens;
    - faire preuve de clarté et de précision dans la formulation de ses constatations et de ses recommandations;

- surveiller, documenter et évaluer le suivi des recommandations par les ministères et les organismes.

19. Pour atteindre ces objectifs, l'OSSNR se concentre sur l'amélioration de l'expertise du personnel dans l'environnement opérationnel de la sécurité nationale, y compris les instruments juridiques et politiques pertinents, et sur le développement des connaissances par l'apprentissage itératif. À cette fin, l'OSSNR élabore un programme de formation structuré pour ses analystes d'examen, en mettant l'accent sur des principes méthodologiques solides et objectifs, et en établissant des réseaux d'experts.

20. L'OSSNR élabore également un cadre d'examen pour assurer la cohérence et la clarté de la façon dont il exécute ses examens. Ce cadre vise à fournir des orientations systématiques sur l'approche de l'OSSNR et à rendre ses processus aussi transparents que possible[53].

21. En 2020, l'OSSNR a également réformé son modèle d'enquête sur les plaintes afin de mieux répondre aux objectifs d'efficacité et de transparence. Deux priorités ont guidé ses efforts pour moderniser ce processus, à savoir l'accès à la justice pour les plaignants qui se représentent eux-mêmes et la création d'étapes procédurales simplifiées et moins formelles. L'OSSNR a créé de nouvelles règles de procédure pour tenir compte de ce nouveau modèle, à la suite de consultations approfondies avec les intervenants des secteurs public et privé. Ces nouvelles règles sont entrées en vigueur en juillet 2021.

Mobilisation des intervenants et des membres de la communauté

22. L'OSSNR collabore avec des experts, des universitaires et des intervenants de la collectivité pour faire connaître son mandat, recevoir des commentaires sur les rapports achevés et orienter les priorités futures, et créer une compréhension commune des pratiques exemplaires en matière d'examens et d'enquêtes. Cela dit, la pandémie a obligé l'OSSNR à repenser ses efforts de mobilisation. L'OSSNR cherche actuellement à élargir la portée de sa mobilisation du public avec divers intervenants non gouvernementaux, notamment pour recevoir des commentaires sur les sujets d'examen et les rapports, ainsi que pour diffuser l'information et faire de la sensibilisation.

23. L'OSSNR s'engage à coopérer avec d'autres organismes d'examen fédéraux dont les mandats ou les objectifs pourraient chevaucher les siens, à savoir le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) et la

Commission civile d'examen et de traitement des plaintes relatives à la GRC, comme le prévoit la Loi sur l'OSSNR. De plus, comme l'autorise la Loi sur l'OSSNR, l'Office s'engage à coordonner ses efforts avec le Commissariat à la protection de la vie privée du Canada (CPVP). Le personnel de l'OSSNR s'entretient régulièrement avec des fonctionnaires de tous les niveaux au sein de ces organismes afin d'éviter les chevauchements inutiles entre les mandats respectifs des différents organismes[54].

24. Par exemple, l'OSSNR a conclu un protocole d'entente avec le CPVP afin de coordonner les efforts et de définir les rôles, responsabilités et domaines d'expertise respectifs lorsque des activités sont susceptibles de se chevaucher. De même, l'OSSNR et le CPSNR ont convenu de s'échanger leurs informations respectives sur la planification des examens afin d'éviter les chevauchements. Dans le cadre de leurs examens respectifs de la GRC, le personnel de l'OSSNR et du CPSNR participe à des séances d'information conjointes afin de réduire le chevauchement des demandes à la GRC.

25. L'OSSNR et le CPSNR cherchent à harmoniser leurs approches à l'égard de leurs obligations distinctes d'informer les ministres du Cabinet lorsqu'ils soupçonnent que des activités liées à la sécurité nationale et au renseignement pourraient ne pas être conformes à la loi. Les lois qui régissent l'OSSNR et le CPSNR décrivent chacune une obligation de faire rapport ou d'informer en utilisant un langage très similaire. Afin de promouvoir la cohérence de leurs approches, l'OSSNR et le CPSNR ont convenu de travailler à l'élaboration d'une norme commune.

Réflexion prospective et pensée novatrice avec les entités homologues de l'OSSNR au sein du FIORC

26. Enfin, l'OSSNR participe également à des forums internationaux, dont le Conseil de surveillance et d'examen du renseignement du Groupe des cinq (FIORC). Le FIORC rassemble les organismes d'examen du Canada, de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis pour discuter des tendances internationales en matière de sécurité nationale et de renseignement et pour échanger des pratiques exemplaires dans le cadre de conversations non classifiées. Certaines de ces conversations ont lieu dans le cadre de réunions tenues au niveau multilatéral auxquelles participent tous les partenaires du FIORC, tandis que d'autres consistent en des conversations bilatérales sur des sujets d'intérêt commun.

27. L'OSSNR participe à trois groupes de travail thématiques du FIORC qui examinent des défis importants communs à ses membres. Le groupe de travail sur l'intelligence

artificielle examine les conséquences de l'intelligence artificielle dans le contexte de la sécurité nationale et ce que cela signifie pour les organismes qui examinent la manière dont ces technologies sont exploitées. Ce groupe de travail examine également si les organes d'examen eux-mêmes peuvent tirer parti des nouveaux outils d'intelligence artificielle pour améliorer leurs capacités d'examen.

28. Le groupe de travail sur les assurances en matière d'échange d'information examine les pratiques en place pour garantir que l'échange d'information n'entraîne pas un risque accru de mauvais traitements pour les sujets visés par l'information échangée.

29. Enfin, le groupe de travail sur les lacunes en matière de responsabilisation explore les lacunes législatives et pratiques qui subsistent dans les différentes administrations en ce qui concerne le mandat, les pouvoirs, l'accès et les ressources des organismes d'examen. L'OSSNR continuera de travailler avec ses partenaires du Groupe des cinq par l'intermédiaire du FIORC afin d'encourager la collaboration en matière de transparence et de responsabilité, et de combler les lacunes potentielles au chapitre de la responsabilité qui existent en ce qui a trait à la coopération internationale.

---

[1] Office de surveillance des activités en matière de sécurité nationale et de renseignement, *Rapport annuel 2019*, https://www.nsira-ossnr.gc.ca/wp-content/uploads/2020/12/AR-NSIRA-Fr-Final.pdf.

[2] *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (L.C. 2019, ch. 13, art. 2) (Loi sur l'OSSNR) : https://laws-lois.justice.gc.ca/fra/lois/n-16.62/page-1.html.

[3] Site Web de la Commission civile d'examen et de traitement des plaintes relatives à la GRC : https://www.crcc-ccetp.gc.ca/fr.

[4] Loi sur l'OSSNR, paragraphe 38(1).

[5] Rapport annuel de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement – OSSNR (nsira-ossnr.gc.ca).

[6] Voir aussi *Rapport annuel 2019*, p. 20 à 56.

[7] Les rapports complets sont disponibles sous forme caviardée sur le site Web de l'OSSNR : https://nsira-ossnr.gc.ca/fr/reviews.

[8] Cela comprend, sans s'y limiter : demeurer indépendant et objectif en tout temps pendant l'exécution des travaux du Secrétariat de l'OSSNR; être ouvert à la collaboration, aux nouvelles technologies et à l'apprentissage continu; s'efforcer de maintenir un niveau élevé de compétence professionnelle et d'expertise pour s'acquitter de ses fonctions et de ses responsabilités; traiter les membres du public, les employés d'autres ministères et les intervenants externes d'une manière respectueuse et professionnelle.

[9] Bien qu'elles soient présentées comme des segments d'un continuum, les étapes du cycle de l'information ne sont pas nécessairement distinctes ou unidirectionnelles. En réalité, elles se chevauchent et sont souvent interreliées. Ici, leur regroupement aide simplement à cerner et à analyser les thèmes communs qui pourraient ressortir à l'échelle du gouvernement.

[10] Dans le *Rapport annuel 2019*, nous avons indiqué qu'une structure différente du continuum de l'information pourrait être adoptée pour les futurs rapports annuels en fonction des recommandations que l'OSSNR reçoit et de l'information qu'il souhaite communiquer (voir p. 21).

[11] *Loi de 2017 sur la sécurité nationale*, L.C. 2019, ch. 13, art. 168.

[12] Loi sur l'OSSNR, art. 32.

[13] Loi sur l'OSSNR, paragr. 8(2).

[14] *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23 (Loi sur le SCRS), paragraphe 12.1(1).

[15] Un expert-conseil externe a effectué un examen externe de la relation opérationnelle entre le SCRS et la GRC, intitulé « Examen relatif à l'amélioration opérationnelle ». Cet examen présente des recommandations ambitieuses visant à améliorer la façon dont le SCRS et la GRC gèrent conjointement les menaces tout en gérant les risques liés à la communication d'information par le SCRS à la GRC. L'OSSNR recommande que le SCRS et la GRC continuent d'accorder la priorité à la mise en œuvre en temps opportun de ces recommandations, qui bénéficient du soutien de la haute direction des deux organisations. L'OSSNR entreprendra, au cours des prochaines années, un examen de la mise en œuvre des recommandations de l'Examen relatif à l'amélioration opérationnelle par le SCRS et la GRC afin d'évaluer les progrès et de faire le bilan des résultats.

[16] Dans sa décision rendue dans *2020 CF 616* et publiée le 16 juillet 2020, aux articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23, la Cour fédérale a constaté que le SCRS avait manqué à son obligation de franchise envers la Cour en omettant d'indiquer et de déclarer de façon proactive que l'information utilisée à l'appui des demandes de mandat provenait probablement d'activités illégales. À la suite de la recommandation de la Cour voulant que cette question fasse l'objet d'un examen indépendant plus poussé, les ministres de la Sécurité publique et de la Justice ont confié l'affaire à l'OSSNR. En réponse à la lettre de renvoi et conformément à son propre mandat d'examen, l'OSSNR a entrepris un examen du SCRS et du ministère de la Justice.

[17] En vertu de la Loi sur le SCRS, le SCRS est tenu de fournir à l'OSSNR de l'information concernant la conduite de certaines de ses activités tout au long de l'année : rapports du directeur (Loi sur le SCRS, paragraphe 4), directives ministérielles [Loi sur le SCRS, paragraphe 6(2)], ensembles de données [Loi sur le SCRS, alinéas 11.25 a), b) et c)], mesures de réduction de la menace [Loi sur le SCRS, paragraphe 12(3.5)], ententes de coopération (Loi sur le SCRS, paragraphe 17), communication d'identité [Loi sur le SCRS, paragraphe 19(3)], agissements illicites d'un employé du SCRS [Loi sur le SCRS, paragraphe 20(2)] et régime de justification [Loi sur le SCRS, alinéas 26 a), b) et c)].

[18] L'OSSNR est tenu, en vertu de l'article 32 de la Loi sur l'OSSNR, de produire un rapport annuel classifié sur les activités du SCRS à l'intention du ministre de la Sécurité publique et de la Protection civile. En vertu de la Loi sur le SCRS, l'un des prédécesseurs de l'OSSNR, le Comité de surveillance des activités de renseignement de sécurité (CSARS), était tenu de certifier le rapport annuel du directeur du SCRS destiné au ministre de la Sécurité publique et de la Protection civile. Le processus de certification s'appuyait sur diverses informations fournies au CSARS en vertu de la Loi sur le SCRS, y compris des rapports sur des actes illicites accomplis par des employés du SCRS et des ententes de coopération conclues par le SCRS avec des organisations et des gouvernements étrangers. Le processus de certification était également appuyé par l'examen et l'évaluation d'importants volumes d'informations supplémentaires demandées par le CSARS, qui portaient généralement sur les activités du SCRS présentant un risque élevé en ce qui concerne le respect de la loi.

[19] Loi sur l'OSSNR, article 33.

[20] Le Bureau du commissaire du Centre de la sécurité des télécommunications était l'organisation chargée d'examiner le respect des lois par le CST de 1996 à 2019.

[21] L'examen des communications d'IIC se trouve en ligne à l'adresse suivante : https://www.nsira-ossnr.gc.ca/wp-content/uploads/2021/06/10397868-001-FR-CII-Review-2018-19-1.pdf.

[22] L'information acquise fortuitement, dans le contexte de l'acquisition d'information par le Centre de la sécurité des télécommunications (CST), s'entend de la manière dont celle-ci est acquise dans le cas où elle n'était pas délibérément recherchée et où l'activité qui a permis l'acquisition de cette information ne visait pas un Canadien ou une personne se trouvant au Canada.

[23] Cet examen n'a pas porté sur l'efficacité du programme du CST en matière de protection de l'INC en ce qui a trait à son incidence sur la sécurité nationale.

[24] L'article 16 de la Loi sur le SCRS porte sur la collecte d'information concernant des États étrangers et des personnes étrangères.

[25] Pour obtenir de plus amples renseignements, voir la section 1.5.

[26] Dans le cas des mandats du CST en matière de renseignement étranger et de cybersécurité, le commissaire au renseignement doit approuver ces autorisations ministérielles. Le commissaire au renseignement n'est pas tenu d'approuver les autorisations ministérielles délivrées en vertu des volets du mandat du CST touchant les cyberopérations actives et les cyberopérations défensives ni d'approuver les activités réalisées en vertu du volet du mandat du CST touchant l'assistance technique et opérationnelle, qui ne sont pas nécessaires pour mener des activités aux termes d'une autorisation ministérielle.

[27] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76 (Loi sur le CST), paragraphe 21(1).

[28] Contrairement à de nombreux alliés du Canada, y compris ses quatre partenaires du Groupe des cinq, le gouvernement du Canada n'a pas exposé sa position sur la façon dont le droit international s'applique dans le cyberespace.

[29] L'examen du Dossier relatif aux incidents liés à la vie privée (DIVP), qui présente un échantillon d'incidents signalés dans le DIVP du 1er juillet 2018 au 31 juillet 2019, se trouve en ligne à l'adresse suivante : https://nsira-ossnr.gc.ca/wp-content/uploads/2021/03/PIF_Report_Sept_2020_FR.pdf.

[30] Le CST n'a pas été en mesure de fournir toutes les données que l'OSSNR espérait présenter dans le présent rapport annuel. À titre d'exemple, le CST n'était pas disposé à autoriser la publication de données liées à la valeur des rapports du CST, aux chiffres relatifs aux communications privées, ainsi qu'à l'utilisation finale des éléments de communications et de trafic recueillis. Dans les futurs rapports annuels, l'OSSNR continuera de faire pression pour obtenir l'autorisation de publier des données plus détaillées et plus diversifiées, à condition que la publication de ces données ne soit pas considérée comme portant atteinte à la sécurité nationale.

[31] Bien que l'OSSNR n'ait aucune raison de contester ces affirmations, le mandat de l'OSSNR, en général, ne vise pas à examiner l'incidence des programmes du CST sur les résultats en matière de sécurité nationale.

[32] Le CST utilise l'appellation « cyberopérations étrangères » pour désigner à la fois les cyberopérations actives (CA) et les cyberopérations défensives (CD), qui sont autorisées en vertu des articles 19 et 18 de la Loi sur le CST, respectivement. Le rapport annuel du CST 2020-2021 peut être consulté ici : https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports/rapport-annuel-du-centre-de-la-securite-des.

[33] Le Centre canadien pour la cybersécurité (CCC) est l'autorité canadienne unifiée en matière de cybersécurité. Le CCC offre une orientation, des services et une formation spécialisés, tout en travaillant en collaboration avec les

intervenants des secteurs privé et public. Le personnel du CCC, qui fait partie du CST, agit également à titre d'équipe d'intervention en cas d'incident de cybersécurité du Canada et d'équipe d'intervention en cas d'incidents informatiques du gouvernement du Canada.

[34] À titre d'exemple, l'Office of the Inspector-General of Intelligence and Security de la Nouvelle-Zélande est tenu d'évaluer et d'attester la « solidité » des systèmes de conformité des organismes dans ses rapports annuels.

[35] L'OSSNR invite les personnes qui ont des préoccupations relatives au CST et à ses fonctions à communiquer avec lui : https://nsira-ossnr.gc.ca/fr/contact-us.

[36] En vertu de l'article 43 de la Loi sur le CST, le CST peut communiquer à certaines personnes ou catégories de personnes désignées de l'information qui pourrait être utilisée pour identifier un Canadien ou une personne se trouvant au Canada et qui a été utilisée, analysée ou conservée au titre de certains types d'autorisations, s'il conclut que la communication est essentielle aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité.

[37] L'OSSNR bénéficie d'un tel accès, par exemple, aux dépôts du SCRS. Si l'OSSNR était généralement satisfait de son accès au SCRS en 2020, il estimait que l'accès au CST la même année devait être amélioré.

[38] L'information que le CST est tenu de fournir à l'OSSNR est appelée information « transmise », tandis que l'information que l'OSSNR obtient du CST est connue sous le nom d'information « tirée ».

[39] En date de juin 2021, l'équipe d'examen du CST de l'OSSNR était composée d'un gestionnaire et de six analystes, en plus de bénéficier de l'aide considérable de plusieurs experts juridiques, techniques et autres employés. La dotation de l'équipe d'examen du CST de l'OSSNR se poursuit en 2021.

[40] Loi sur l'OSSNR, alinéa. 8(1) b).

[41] Cet examen est l'un des nombreux examens de l'OSSNR qui ont porté ou porteront sur divers aspects de la protection des personnes, de l'information et des actifs du gouvernement du Canada. 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 actifs. 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 sécurité*.

[42] Examen de la mise en œuvre par les ministères de la Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères en 2019 – OSSNR (nsira-ossnr.gc.ca).

[43] *Rapport annuel de 2019 sur la communication d'information au titre de la* Loi sur la communication d'information ayant trait à la sécurité du Canada : https://nsira-ossnr.gc.ca/fr/security-of-canada-information-disclosure-act.

[44] Page Web de l'OSSNR contenant les rapports d'enquête sur les plaintes : https://nsira-ossnr.gc.ca/fr/complaints.

[45] Il convient de noter que, parfois, le travail sur les examens, y compris les demandes d'information, a commencé avant la finalisation de la mise au point du mandat. Par exemple, les travaux de fond ont commencé en juillet 2020 pour l'examen de l'INC du CST, et en janvier 2020 pour l'examen de l'utilisation et de l'échange d'information du CST.

[46] Dans le cas de certains examens, l'OSSNR n'a pas été en mesure de publier une partie ou la totalité de ces informations dans le rapport annuel de cette année. Les résumés complets de la plupart des examens dont il est question dans le présent rapport annuel sont disponibles sur demande, s'ils ne sont pas déjà publiés sur le site Web de l'OSSNR au moment de la publication du présent rapport.

[47] Examen des incidents liés à la vie privée et des erreurs de procédure autosignalés par le CST : https://nsira-ossnr.gc.ca/wp-content/uploads/2021/03/PIF_Report_Sept_2020_FR.pdf.

[48] *Rapport annuel de 2019 sur la communication d'information au titre de la* Loi sur la communication d'information ayant trait à la sécurité du Canada : https://www.nsira-ossnr.gc.ca/wp-content/uploads/2020/12/SCIDA-NSIRA-Fr-Final.pdf.

[49] *Loi de 2017 sur la sécurité nationale*, L.C. 2019, ch. 13, Préambule.

[50] Examens de l'OSSNR : https://nsira-ossnr.gc.ca/fr/reviews.

[51] Énoncé de politique concernant l'engagement de l'OSSNR à déclassifier et à dépersonnaliser le contenu de chaque rapport d'enquête sur les plaintes (Microsoft Word) : https://nsira-ossnr.gc.ca/wp-content/uploads/2021/02/Declassifed-depersonalize-policy-french.pdf .

[52] Canada (2020), « Engagement de transparence en matière de sécurité nationale ». https://www.canada.ca/fr/services/defense/securitenationale/engagement-transparence-securite-nationale.html

[53] De plus amples détails sur le cadre d'examen de l'OSSNR sont présentés à l'annexe C.

[54] Loi sur l'OSSNR, articles 13 à 15.