Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

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

National Security and Intelligence Review Agency

Examen des activités de renseignement de sources ouvertes sur Internet du ministère de la Défense nationale et des Forces armées canadiennes

OSSNR // Examen n° 24-10

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Table des matières

Sommaire ii

Sigles et abréviations iv

I. Introduction 1

Fondements législatifs 1

Portée 1

Méthodologie 1

Énoncés généraux 2

II. Contexte 2

Structure de gouvernance 2

Activités OSINT 3

Contexte juridique 5

III. Constatations, analyse et recommandations 7

Pouvoirs en matière de collecte 7

Justification de la collecte 8

Évaluation des risques 9

Échéances et gestion des risques 10

Méthodes et outils de collecte 11

Processus d'évaluation des outils 12

Assurance et options 13

Lien avec des Canadiens 14

Paramètres stratégiques 15

Autorité approbatrice 16

Responsabilisation et conformité 18

IV. Conclusion 19

Annexe A. Constatations et recommandations 21

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Sommaire

L'OSSNR veille sur les Canadiens en exerçant une surveillance des activités du gouvernement du Canada en matière de sécurité nationale et de renseignement, et c'est à ce titre qu'il a examiné les activités de renseignement de sources ouvertes (OSINT pour *Open-Source Intelligence*) menées sur Internet par le ministère de la Défense et les Forces armées canadiennes (MDN/FAC). Pendant la pandémie de COVID-19, les reportages diffusés par les médias relativement aux activités de collecte OSINT du MDN/FAC ont suscité des craintes au sein du public quant à l'ampleur et à la visée desdites activités. Par conséquent, l'OSSNR a choisi de réaliser un examen sur cet enjeu en se penchant sur les mesures prises par le MDN/FAC pour améliorer la gouvernance s'appliquant à cet aspect du renseignement de défense.

Le MDN/FAC se sert de l'OSINT dans le but de soutenir les opérations militaires et les activités de défense et de répondre à divers types de besoins en information. L'OSINT constitue un mode de collecte de renseignement souvent plus rapide, plus abordable et moins risqué que bien d'autres modes, notamment le renseignement de source humaine ou le renseignement électromagnétique. L'OSSNR a analysé l'autorisation permettant au MDN/FAC de collecter de l'OSINT, a examiné les évaluations des risques ainsi que les méthodes et les outils de collecte, puis a évalué les mécanismes de responsabilisation qui interviennent après la collecte. Les examinateurs de l'OSSNR ont porté une attention particulière aux activités OSINT du MDN/FAC ayant un rapport avec des Canadiens, dans le but d'établir si ces activités étaient légales, justes et nécessaires.

Pour être licites, les activités OSINT du MDN/FAC doivent avoir un rapport direct avec une opération militaire ou une activité de défense et ne doivent collecter que de l'information publiquement accessible. Ces activités sont assujetties à un certain nombre de lois canadiennes, notamment, la *Loi sur la défense nationale*, la *Charte canadienne des droits et libertés de la personne* (la Charte) et la *Loi sur la protection des renseignements personnels*, mais aussi à des politiques et directives établies par le gouvernement du Canada et certains ministères.

L'examen a permis de constater que le MDN/FAC disposait de l'autorisation légale de mener des activités OSINT permettant de répondre à des besoins en renseignement de défense. Toutefois, le MDN/FAC n'enregistre pas systématiquement le lien entre, d'une part, la collecte OSINT et, d'autre part, l'opération ou l'activité de défense approuvée. L'OSSNR a également constaté que les évaluations des risques du MDN/FAC, lesquelles doivent contribuer à orienter les activités OSINT, ne sont pas mises à jour en temps opportun et n'abordent pas tous les risques pertinents.

L'OSSNR constate également que le MDN/FAC dispose de critères lui permettant d'évaluer les fournisseurs de données tiers auxquels il a recours pour la collecte OSINT, mais qu'en revanche, il n'a pas systématiquement respecté ces critères dans tous les cas. Par exemple, le MDN/FAC
15(1) a) n'a effectué aucune évaluation [redacted] groupe de fournisseurs de données qui se

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

spécialisent dans la collecte d'information sur les personnes. Cette démarche pose des risques d'atteinte aux stipulations des politiques et de la Charte, notamment, un risque d'atteinte au droit à la protection contre les fouilles, les perquisitions ou les saisies abusives, dans la mesure où les personnes pourraient avoir une attente raisonnable en matière de protection des renseignements personnels relativement à certains types d'information accessible en ligne.

L'OSSNR a aussi constaté que les instruments de politique du MDN/FAC appelés à encadrer la collecte d'information sur des Canadiens ne tenaient pas suffisamment compte des risques d'atteinte à la vie privée posés par certaines activités de renseignement de sources ouvertes menées sur Internet. En outre, la démarche de surveillance des activités OSINT menées sur Internet par le MDN/FAC comporte des problèmes de gestion de l'information qui réduisent la capacité de l'OSSNR à vérifier si lesdites activités s'avèrent nécessaires lorsque la collecte touche des Canadiens. Enfin, l'examen a permis de constater que les mesures de surveillance et de conformité prises par le MDN/FAC relativement aux activités OSINT n'atténuaient pas tous les risques pertinents.

Le présent rapport contient cinq recommandations visant à aider le MDN/FAC à renforcer sa conformité aux lois applicables et à adopter un mode de gouvernance apte à encadrer ses activités OSINT.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Sigles et abréviations

CANCIT	renseignement sur des citoyens canadiens (***Can**adian **Cit**izen Information*)
Charte	*Charte canadienne des droits et libertés de la personne*
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement
FAC	Forces armées canadiennes
LDN	*Loi sur la défense nationale*
MDN	ministère de la Défense nationale
OSINT	renseignement de sources ouvertes (***O**pen-**S**ource **Int**elligence*)
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

I. Introduction

Fondements législatifs

1. Le présent examen a été réalisé en application de l'alinéa 8(1)b) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (Loi sur l'OSSNR)[1].

Portée

2. Le présent rapport d'examen se concentre sur les activités de renseignement de sources ouvertes (OSINT pour *Open-Source Intelligence*) menées sur Internet[2] par le ministère de la Défense nationale et par les Forces armées canadiennes (MDN/FAC). L'examen a été l'occasion de se pencher sur les pouvoirs en matière de collecte, puis d'analyser les évaluations des risques ainsi que les méthodes et outils de collecte en fonction de mécanismes de responsabilisation appliqués après la collecte.

3. L'examen visait deux principaux objectifs : d'abord, évaluer la gouvernance de l'OSINT assurée par le MDN/FAC en lien avec les opérations et activités de défense approuvées; ensuite, déterminer si le MDN/FAC s'est conformé aux obligations qui lui incombent lorsqu'il a été appelé à collecter et à gérer l'OSINT, toujours en lien avec les opérations et activités de défense approuvées.

Méthodologie

4. L'examen a également permis d'évaluer les activités du MDN/FAC sous divers angles, notamment, la structure organisationnelle, la gouvernance, la formation, les mécanismes de responsabilisation et la gestion de l'information. Les examinateurs ont aussi pu s'appuyer sur des réponses écrites, des séances d'information de même que sur des entrevues réalisées auprès d'analystes et de gestionnaires de l'OSINT.

5. L'analyse générale réalisée dans le cadre du présent examen a principalement porté sur les activités OSINT du MDN/FAC menées dans le contexte d'opérations approuvées

---

[1] L.C. 2019, ch. 13 [Loi sur l'OSSNR].

[2] Bien que l'OSINT englobe les activités nécessitant l'accès à de l'information autre que celle qui se trouve sur Internet, il faut savoir que, dans le contexte du présent examen, le terme OSINT renvoie exclusivement à des activités menées en ligne.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

(p. ex. exécution de missions et déploiement d'activités) ou d'activités de défense autorisées (p. ex. les fonctions de soutien qui alimentent et favorisent la prise de décisions) pendant la période s'étendant du 28 février 2022 au 28 février 2025. Il convient toutefois de noter que l'OSSNR a analysé des données produites avant et après la période visée par l'examen, de sorte à dresser un portrait analytique complet des enjeux concernés.

Énoncés généraux

6. La Loi sur l'OSSNR accorde à l'Office de surveillance le droit d'accéder en temps opportun aux informations qui relèvent de tout ministère ou qui sont en la possession de tout ministère (à l'exception des documents confidentiels du Cabinet) et de recevoir de la part desdits ministères les explications et les documents qu'il juge nécessaires. L'OSSNR exerce un suivi du degré de coopération affiché à l'égard des demandes d'accès, notamment sur le plan de la complétude et de l'exactitude des informations communiquées, dans le but de procéder à une évaluation de la réactivité d'un ministère dans le cadre de chacun des examens[3].

7. Au début de la période d'examen, le MDN/FAC n'a pas répondu aux attentes de l'OSSNR sur le plan de la réactivité, mais, par la suite, le MDN/FAC s'est amélioré à ce chapitre.

II. Contexte

Structure de gouvernance

8. Le MDN et les FAC représentent deux entités distinctes qui sont établies au titre de la *Loi sur la défense nationale* (LDN). En vertu de cette Loi, le Ministre « est responsable des Forces canadiennes; il est compétent pour toutes les questions de défense nationale ». Quant au sous-ministre de la Défense nationale, il fournit son soutien aux responsabilités ministérielles individuelles et collectives pour ce qui a trait à l'élaboration et à la mise en œuvre des politiques. La LDN confie la direction et l'administration des FAC au Chef d'état-major de la Défense, sous réserve des règles applicables et sous la direction du Ministre.

[3] Les attentes de l'OSSNR en matière de réponse aux examens sont énoncées sur le site Web de l'OSSNR (https://nsira-ossnr.gc.ca).

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

9. À moins que le gouverneur en conseil en décide autrement, c'est le Chef d'état-major de la Défense qui communique les ordres et instructions aux FAC en vue de concrétiser les décisions et d'exécuter les directives émises par le gouvernement du Canada ou par le Ministre, ce qui comprend la mise en œuvre des exigences que le gouvernement établit pour le MDN/FAC en matière de renseignement. Les titulaires de deux postes sont principalement responsables de l'exécution des activités de renseignement de défense : le Chef du renseignement de la Défense exerce un pouvoir fonctionnel pour ce qui touche à tous les programmes du renseignement de défense et constitue le principal conseiller en matière de renseignement de défense au MDN/FAC; quant au commandant du Commandement du renseignement des Forces canadiennes, il est chargé de la coordination et de l'approbation des besoins en matière de renseignement de défense, en appui aux activités de défense, ce qui comprend les opérations militaires. Ces postes sont toujours occupés par la même personne.

10. La Directive ministérielle de 2024 sur le renseignement de défense établit un lien entre la loi et les politiques. En outre, la Directive appelle le Chef du renseignement de la Défense à exercer son autorité fonctionnelle sur les programmes, l'administration et les activités de renseignement de défense dans l'ensemble du MDN/FAC. Du reste, il confie à certaines personnes la responsabilité d'élaborer des politiques en matière de renseignement de défense. À titre d'exemple, la Directive fonctionnelle du Chef du renseignement de la Défense sur la « Conduite d'activités de renseignement de sources ouvertes sur Internet » est un instrument de politique qui fait office d'ordonnance destinée aux officiers et aux militaires du rang des FAC, et de directive destinée à tous les employés du MDN. Chacun des commandants est responsable des activités de renseignement de défense exécutées dans un secteur géographique défini ou selon des responsabilités particulières, responsable également de la conformité à toutes les directives fonctionnelles.

11. La directive du Ministre stipule également que l'autorité permettant de conduire des activités de renseignement de défense est comprise dans le pouvoir de mener une opération ou d'autres activités de défense. De plus, ces fonctions du renseignement doivent avoir directement trait à une opération autorisée ou à une activité de défense autorisée.

Activités OSINT

12. Le MDN/FAC mène des activités de renseignement de défense en guise de soutien aux opérations militaires, aux programmes de défense et à la planification de scénarios au sens large. Il peut s'agir, en l'occurrence, de soutien à divers commandements permanents, notamment, l'Armée canadienne ou le Commandement – Forces d'opérations spéciales du Canada, ou à des opérations nommées déployées au Canada ou à l'étranger. Ces activités sont également menées en appui à des entités militaires

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

multinationales, comme l'Organisation du Traitde l'Atlantique Nord, mais aussi en soutien – sur demande formelle venant des ministres compétents – à des ministères et organismes du gouvernement du Canada[4].

13. Selon l'opération militaire, les commandants peuvent disposer d'un large éventail de sources et de méthodes lorsqu'il s'agit de répondre à leurs besoins en information. Par exemple, on peut penser à l'utilisation du renseignement électromagnétique, du renseignement de source humaine, du renseignement géospatial ou de l'OSINT ou encore d'une vingtaine d'autres types de renseignement. Le MDN/FAC définit l'OSINT comme étant le renseignement puisé à même l'information publiquement accessible, de même que l'information non classifiée dont la distribution est limitée ou l'accès est contrôlé. Le MDN/FAC collecte l'OSINT sur Internet pour diverses raisons, notamment pour se tenir au courant des actualités ou de l'évolution d'enjeux particuliers, mais aussi pour répondre à des besoins en matière de renseignement. Pendant que la sphère du renseignement ne cesse de s'élargir, le MDN/FAC développe continuellement ses capacités et son expertise en matière de collecte sur Internet.

14. Les analystes du MDN/FAC se servent de tout un éventail d'outils lorsqu'ils mènent des activités OSINT : les navigateurs Web, certaines applications logicielles ainsi que des bases de données en ligne pour ne nommer que ceux-là. En outre, les analystes emploient des termes de recherche avancés, inspectent du code source et utilisent d'autres méthodes visant à tirer le maximum des activités de collecte. Le MDN/FAC a également recours à des entreprises tierces qui collectent et communiquent d'importants volumes de données en ligne, et ce, moyennant des frais, la plupart du temps. Par exemple, certains fournisseurs de données permettent à leurs utilisateurs de récupérer de l'information provenant d'une multitude de sources renfermant divers types d'information. Toutefois, puisqu'on n'est pas toujours certain de la façon dont les données ont été initialement collectées par les fournisseurs de données tiers, il existe le risque juridique qu'elles aient été piratées, divulguées ou volées.

15. Outre l'autorisation de collecte, les activités OSINT sont régies par les politiques et procédures du MDN/FAC et ne peuvent être menées que par du personnel formé et autorisé. Pendant plusieurs années, le MDN/FAC ne disposait d'aucune politique générale s'appliquant à la collecte d'information concernant des Canadiens. Il y avait bien certains commandements qui disposaient de leurs propres directives concernant les Canadiens, mais sans plus.

16. Toutefois, pendant le conflit armé qui s'est déroulé entre 2011 et 2017 en Syrie et en Irak, le MDN/FAC [*] [redacted]

15(1) a)

[4] À moins d'avis contraire, le présent rapport emploie le terme « commandement » pour désigner les commandements permanents, les opérations nommées et les activités de renseignement.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

[redacted] En outre, les plus récentes capacités en matière de renseignement, notamment, le recours accru à Internet, signifie que les mesures de collecte visant à soutenir les opérations et les activités de défense sont devenues particulièrement complexes. Ces facteurs ont quelque peu forcé le MDN/FAC à prendre en compte et à résoudre les questions stratégiques qui se posent lorsque des activités de renseignement de défense impliquent des Canadiens.

17. Cette conjoncture a donné lieu à la création, en 2018, de la directive intitulée Directive sur la gestion et la protection de l'information sur les citoyens canadiens (Directive fonctionnelle CANCIT), qui a fait l'objet du Rapport spécial de 2020 du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR). Ce rapport se concentre sur le caractère adéquat de la gouvernance et des contrôles juridiques s'appliquant à la collecte du MDN/FAC relativement aux Canadiens, y compris pendant les activités en ligne.

18. Rappelons que le CPSNR s'était dit préoccupé par le fait que la gouvernance exercée par le MDN/FAC dans le cadre de ses activités de renseignement n'était abordée que dans les documents stratégiques et non, comme c'est le cas pour le Centre de la sécurité des télécommunications, dans un texte de loi. Le CPSNR avait conclu que « la clarté juridique devrait exister pour les deux ». Cette observation a été publiée tout juste avant la mise en œuvre définitive, par le MDN/FAC, de la Directive fonctionnelle CANCIT de 2018, et demeure applicable aux fins de l'analyse réalisée dans le contexte de l'examen de l'OSSNR.

19. Pendant que le CPSNR publiait son rapport de 2020, avait lieu l'opération LASER, qui faisait partie de la réponse intérieure du MDN/FAC à la pandémie de COVID-19. L'objet de cette opération était de maintenir le niveau efficacité opérationnelle des FAC, de protéger la santé des militaires et d'appuyer les autorités canadiennes. Consécutivement à ces responsabilités, il faut savoir que le MDN/FAC se tenait au courant de l'évolution de la pandémie en collectant de l'information auprès de sources en ligne, notamment les médias sociaux.

20. On a ensuite appris que la collecte en ligne effectuée par le MDN/FAC comportait des renseignements personnels sur des Canadiens, renseignements qui n'avaient aucun lien direct avec l'opération militaire. Ces activités, dont il a été largement question dans les médias, ont suscité des inquiétudes à l'égard de l'ensemble des activités menées en ligne par le MDN/FAC.

Contexte juridique

21. Les activités du MDN/FAC sont assujetties aux lois intérieures ainsi qu'à un certain nombre de lois internationales. Ainsi, le régime juridique applicable varie en fonction des

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

circonstances, selon que les activités ont lieu dans le contexte d'un conflit armé ou non, au Canada ou à l'étranger. Par ailleurs, les paramètres juridiques qui régissent le renseignement de défense, notamment les activités OSINT, évoluent en fonction des avancées technologiques et des attentes sociétales en matière de protection de la vie privée.

22. L'Internet est vaste, et l'origine de l'information peut être occultée. Ainsi, il devient parfois difficile de connaître la source ou la provenance de l'information collectée dans la sphère de l'Internet. Pour le MDN/FAC, cette situation pose certaines difficultés lorsqu'il s'agit d'évaluer l'exactitude et la fiabilité de l'information. Elle constitue également une source de préoccupation lorsqu'il est question de savoir si la collecte et l'utilisation d'information ont une incidence sur la protection des droits garantis par la loi.

23. L'article 8 de la *Charte canadienne des droits et libertés* (la Charte) garantit le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. Pour les personnes visées par la Charte, l'article 8 reconnaît l'existence d'une attente raisonnable en matière de protection de la vie privée. Or, cette attente repose sur quatre éléments : 1) établir l'objet de la fouille, de la perquisition ou de la saisie; 2) établir si la personne a des droits dans l'objet; 3) établir si la personne avait une attente subjective en matière de respect de la vie privée relativement à l'objet; 4) établir si l'attente subjective de la personne était objectivement raisonnable[5].

24. Le droit canadien accorde une grande importance à la protection de la vie privée en ce qui concerne les renseignements personnels susceptibles de révéler des détails intimes sur le mode de vie et les choix personnels d'une personne. Les Canadiens ont un droit de regard sur les entités qui ont accès à leurs renseignements personnels et sur la façon dont ceux-ci sont communiqués. Les renseignements personnels doivent également être protégés contre toute incursion abusive de la part de l'État. En effet, la Cour suprême du Canada a conclu qu'il pourrait y avoir une attente raisonnable en matière de protection de la vie privée à l'égard de certains types d'information associés aux activités sur Internet[6].

25. Bien que certains aspects des activités menées sur Internet puissent devenir publics, dans certains cas, à son insu ou sans son consentement, l'utilisateur du Web peut tout de même s'attendre à ce que ses renseignements personnels soient protégés par l'invisibilisation des liens entre ses activités en ligne et son identité. La communication de certains renseignements personnels à une tierce partie dans le but d'obtenir un service en ligne n'élimine pas l'attente raisonnable – et le droit – de cette personne à la protection desdits renseignements contre toute intrusion de l'État.

---

[5] Voir le site Web de Justice Canada, Article 8 – Fouilles, perquisitions et saisies, https://www.justice.gc.ca/fra/sjc-csj/dlc-rfc/ccdl-ccrf/check/art8.html.

[6] Voir, à titre d'exemple, *R c. Bykovets*, 2024 CSC 6.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

26. La Cour suprême a émis quelques réserves à l'égard de la collecte d'information auprès de tierces parties, dans la mesure où cette pratique s'apparenterait à l'utilisation d'un « moyen détourné », ce qui porterait atteinte aux droits de la personne[7]. Conséquemment, le MDN/FAC doit demeurer attentif au fait qu'une personne peut continuer d'avoir une attente raisonnable en matière de vie privée, lorsque des renseignements personnels sont collectés par de tierces parties, notamment, les fournisseurs de données.

III. Constatations, analyse et recommandations

Pouvoirs en matière de collecte

27. L'objet de la présente section est de faire part de l'évaluation de l'OSSNR quant à la mesure dans laquelle les activités OSINT du MDN/FAC avaient trait à une opération militaire ou à une activité de défense.

Constatation 1. L'OSSNR constate que le MDN/FAC dispose de l'autorisation légale de mener des activités de renseignement de sources ouvertes sur Internet lui permettant de répondre à des besoins en matière de renseignement de défense.

Constatation 2. L'OSSNR constate que le MDN/FAC n'enregistre pas systématiquement les liens entre, d'une part, les activités de collecte d'information provenant de sources ouvertes et, d'autre part, les opérations ou activités de défense approuvées.

28. D'après la Directive ministérielle sur le renseignement de défense, le MDN/FAC doit veiller à ce que toutes les activités de renseignement se rapportent à une opération ou une activité de défense approuvée. L'autorisation de mener des activités OSINT est implicite à la suite d'une autorisation signifiée par un commandant supérieur des FAC ou par un haut fonctionnaire du MDN dans le cas de certaines opérations militaires ou de certaines autres activités de défense. Ainsi, les opérations au Canada ou à l'étranger peuvent recevoir une autorisation de mener des activités OSINT pour la durée de l'opération. Par ailleurs, les commandements peuvent recevoir une autorisation de mener des activités OSINT en vertu d'une capacité permanente qui évolue au gré des besoins en matière de renseignement.

[7] *R c. Colarusso*, [1994] 1 RCS 20, paragr. 90, 1994 CanLII 134 (CSC).

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

29. Dans les dossiers examinés, les approbations d'opérations militaires faisaient état des autorisations légales permettant la collecte de renseignement de défense et énonçaient les exigences relatives à la gouvernance, notamment, la conformité aux instruments de politique applicables (p. ex. les directives fonctionnelles). Après avoir constaté l'autorisation venant du commandement, l'OSSNR a demandé à voir toutes les demandes de collecte OSINT que les gestionnaires ou les officiers avaient transmises à leur personnel.

Justification de la collecte

30. Compte tenu des répercussions de l'opération LASER – au cours de laquelle l'activité du renseignement de défense n'avait pas été en rapport direct avec l'opération approuvée –, l'OSSNR s'attendait, cette fois, à ce que les activités de collecte OSINT actuelles aient un lien clairement établi avec l'opération ou l'activité de défense approuvée. Or, l'examen a révélé que les gestionnaires ou les officiers pouvaient attribuer les tâches OSINT du MDN/FAC au personnel concerné de façon formelle ou informelle. Il s'avère que les demandes formelles donnent lieu à la création d'un document permanent faisant état de l'attribution des tâches, mais que ce n'est pas le cas pour les demandes informelles formulées verbalement ou par courriel. Dans les cas où aucun document permanent n'est inscrit au dossier, il faut bien comprendre que l'OSSNR n'est pas en mesure de valider la conformité du MDN/FAC aux stipulations de la directive ministérielle.

31. Dans le cas de l'attribution informelle des tâches OSINT, le MDN/FAC justifie l'absence de document en disant considérer ces activités comme étant « à faible risque et à faible impact », et que, par conséquent, il n'est pas nécessaire d'enregistrer formellement ladite attribution. Bien que l'Internet représente un environnement particulièrement dynamique et complexe, le MDN/FAC affirme avoir établi des mesures d'atténuation permettant de gérer les risques et l'impact des activités OSINT qui y sont menées. Lorsque les outils nécessaires et les mesures de protection requises ont été mis en place, le MDN/FAC estime que les commandants et les cadres civils sont en mesure d'encadrer le personnel du renseignement sans avoir recours à des mesures de supervision directe.

32. L'OSSNR reconnaît qu'il existe des circonstances où le caractère changeant des besoins en renseignement – notamment, lorsque la chaîne de commandement transmet des instructions en cours d'opération – peut ne pas être propice à l'enregistrement d'un document formel. Hormis ce raisonnement, il faut savoir qu'au moment où la décision de collecter est prise, les documents dont dispose un analyste aident celui-ci à établir si l'ensemble des activités consacrées à un enjeu ou à un sujet relatif au renseignement permet d'exécuter la tâche OSINT prévue. Or, l'absence de documents formels réduit la visibilité que les commandants – ou les personnes du MDN/FAC à qui l'on a délégué des responsabilités de surveillance – peuvent avoir sur l'attribution des tâches ou sur le

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

déroulement du processus de collecte OSINT. De plus, cette approche pose le risque que l'activité du renseignement ne soit pas en rapport direct avec l'opération militaire autorisée, ce qui est contraire aux stipulations de la Directive ministérielle.

Recommandation 1. L'OSSNR recommande que le MDN/FAC documente formellement et au moment propice l'attribution des tâches de collecte sur Internet, de sorte à formaliser le lien avec l'activité du renseignement de défense.

Évaluation des risques

33. L'objet de la présente section est de décrire les évaluations de risques effectuées au niveau du commandement du MDN/FAC, évaluations qui servent à orienter les activités OSINT et qui permettent à l'OSSNR de procéder à une analyse du caractère adéquat des processus d'évaluation en interne.

Constatation 3. L'OSSNR constate que les évaluations de risques du MDN/FAC qui servent à orienter les activités de renseignement de sources ouvertes sur Internet ne sont pas mises à jour en temps opportun et n'abordent pas tous les risques énumérés dans l'instrument de politique s'appliquant à tous les commandements.

---

34. La directive fonctionnelle du MDN/FAC « Conduite des activités de renseignement de sources ouvertes sur Internet » (Directive OSINT) reconnaît que ces activités peuvent poser, pour le MDN/FAC et le gouvernement du Canada, des risques opérationnels de même que des risques sur le plan diplomatique, juridique et réputationnel. Toute attribution de ces activités au MDN/FAC risque une divulgation des priorités en matière de renseignement et des domaines d'intérêt, mais aussi des tactiques, des techniques et des procédures employées.

35. Les commandants qui envisagent de mener des activités OSINT doivent examiner attentivement ces éléments de risque en appliquant le processus énoncé dans la politique. Pour atteindre cet objectif, la politique exige une attestation écrite de la façon dont chacun des risques reconnus sera atténué.

36. Il convient de souligner certains aspects de ce processus d'évaluation des risques. D'abord, les commandants peuvent mener une évaluation pour ensuite l'appliquer à plusieurs autres activités. Par exemple, l'évaluation des risques menée en 2022 pour le Commandement – Forces d'opérations spéciales du Canada couvrait les activités de plusieurs opérations distinctes qui étaient menées simultanément à l'échelle du globe, mais où chacune devait répondre à des besoins différents en matière de collecte.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

37. Par ailleurs, la Directive OSINT comporte une clause de droits acquis qui permet aux commandants de s'appuyer sur des évaluations de risques élaborées au titre d'anciennes versions de la politique. Une nouvelle évaluation doit être réalisée dès lors que l'on constate, en cours d'activité ou pendant un examen, que la conduite d'une activité OSINT pourrait ne plus correspondre aux paramètres fixés par l'autorisation initiale.

Échéances et gestion des risques

38. Certes, le MDN/FAC est tenu de mener un examen annuel de ses évaluations de risques, mais la majorité de celles-ci sont demeurées inchangées depuis plusieurs années. D'ailleurs, l'absence de mises à jour substantielles indique que le MDN/FAC n'a pas été en mesure de prendre en compte l'évolution des technologies ou du contexte juridique. Par exemple, en 2024, la Cour suprême du Canada a rendu une décision qui influe sur l'établissement des risques juridiques associés à certains types d'information[8]. Or, aucune des évaluations examinées par l'OSSNR n'a abordé cet enjeu.

39. L'OSSNR a également noté que les évaluations de risques n'abordaient pas tous les risques répertoriés dans la Directive OSINT en vigueur. Cette lacune tient en partie au fait que les commandants misent sur la clause de droits acquis énoncée dans cette même Directive, laquelle clause permet de se servir d'évaluations de risques préparées au titre d'une politique OSINT antérieure. Par exemple, les facteurs ayant trait à la politique ou à la réputation étaient absents des évaluations de risques employées en vertu de la clause de droits acquis. De plus, il faut savoir que la politique OSINT précédente prévoyait un processus différent pour l'organisation et l'approbation des activités OSINT, ce qui peut avoir une incidence sur la façon dont les risques sont gérés dans le cadre des opérations actuelles. Ainsi, ces facteurs ne sont pas pris en compte dans les évaluations de risques qui reposent sur le recours à la clause de droits acquis.

40. Les évaluations de risques ne suivent pas une norme à tous les commandements. Le MDN/FAC soutient que cette approche répond au principe militaire favorisant le « commandement fondé sur l'intention », un principe qui inculque aux commandants et à leurs subordonnés une compréhension de l'état final qu'un ordre vise à atteindre tout en encourageant la souplesse et la prise d'initiative permettant d'optimiser le résultat. Par conséquent, pour ce qui concerne les évaluations de risques, le MDN/FAC soutient qu'il vaut mieux préparer les documents de gouvernance en fonction d'un commandement que de tenter d'établir une norme commune à tous les commandements.

41. L'OSSNR reconnaît ce besoin qu'ont les commandants de mettre l'accent sur certains risques plutôt que sur certains autres et de disposer d'une souplesse leur permettant de

---

[8] R. c. Bykovets, 2024 CSC 6.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

préparer leurs évaluations en fonction de documents de gouvernance différents. Cela dit, les évaluations examinées différaient bel et bien les unes des autres quant aux éléments de risque visés et à la profondeur de l'analyse exercée, mais il s'avère que nombre de ces évaluations avaient passé certains risques clés sous silence.

42. Par exemple, le risque juridique a été minimalement abordé par plusieurs évaluations de risques. Ainsi, le MDN/FAC n'a pas réalisé d'évaluation de la conformité permettant de vérifier si les conseillers juridiques avaient pris en compte tous les risques juridiques posés par les activités OSINT envisagées par les divers commandements.

43. Enfin, les évaluations de risques ainsi que les mesures d'atténuation des risques posés par les activités OSINT sont deux composantes distinctes et successives du processus global d'évaluation des risques. En l'occurrence, les officiers et les gestionnaires sont chargés d'examiner régulièrement les mesures d'atténuation et, s'il y a lieu, de les adapter au niveau des opérateurs. Toutefois, le MDN/FAC ne fait pas le suivi de toutes les activités de collecte OSINT, et les mesures d'atténuation ne peuvent donc pas servir à perfectionner les évaluations de risques en temps voulu. Par conséquent, l'OSSNR n'est pas à même d'évaluer la mesure dans laquelle les correctifs auraient pu améliorer les mesures d'atténuation des risques.

Recommandation 2. L'OSSNR recommande que, dans les 12 mois, puis tous les deux ans, le MDN/FAC fasse, au niveau du commandement, une mise à jour de toutes les évaluations de risques pour ce qui concerne les activités de sources ouvertes sur Internet et veille à ce que toutes les catégories de risques concernées soient suffisamment reconnues, évaluées et gérées.

Méthodes et outils de collecte

44. L'objet de la présente section est de faire état de l'examen réalisé par l'OSSNR au sujet des critères d'évaluation sur lesquels le MDN/FAC s'appuie pour choisir les outils OSINT devant servir à collecter de l'information sur Internet.

Constatation 4. L'OSSNR constate que le MDN/FAC a établi des critères permettant d'évaluer les fournisseurs de données tiers dans le but de veiller à ce que les activités de renseignement de sources ouvertes menées sur Internet soient conformes aux lois et aux politiques applicables.

Constatation 5. L'OSSNR constate que le MDN/FAC n'applique pas systématiquement ses critères d'évaluation des fournisseurs de données tiers auxquels il a recours pour ses activités de renseignement de source ouvertes sur Internet, ce qui accroît le niveau de risque sur le plan juridique et politique.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Constatation 6. L'OSSNR constate que le MDN/FAC n'a réalisé aucune évaluation [redacted] 15 fournisseurs de données tiers qui se spécialisent dans la collecte d'information sur les personnes.

45. Pendant ses activités OSINT, le MDN/FAC a recours à divers modes d'exploitation d'Internet. En outre, la surveillance des médias sociaux, l'examen des archives publiques et l'analyse des métadonnées font partie des techniques spécialisées que le MDN/FAC emploie. Pour faciliter ce type de collecte, on peut recourir aux outils en ligne allant de la simple utilisation des moteurs de recherche au recours aux services payants offerts par les fournisseurs de données tiers.

46. Le MDN/FAC doit se conformer aux lois et aux politiques applicables du gouvernement du Canada, lesquelles exigent que les ministères et organismes exercent un contrôle sur les contenus inexacts, incomplets ou biaisés et qu'ils assurent une gestion adéquate des risques d'atteinte à la vie privée. Cette démarche nécessite une évaluation adéquate permettant de détecter les sources en ligne comportant des données qui auraient été piratées, divulguées ou volées.

Processus d'évaluation des outils

47. Le MDN/FAC a créé un groupe consultatif sur les échanges d'information pour permettre aux commandants d'aborder la question de l'évaluation des outils. Il a également créé des critères d'évaluation connexes qui visent à s'assurer que l'utilisation des outils réponde aux stipulations des protocoles de sécurité opérationnelle et des cadres juridique, stratégique et éthique. L'OSSNR a remarqué que le MDN/FAC avait effectué plusieurs évaluations d'outils en ligne et avait pris contact avec certains fournisseurs.

48. Dans ses échanges avec l'OSSNR, le MDN/FAC a soutenu qu'il n'avait acheté ou utilisé aucun service ou produit associé à de l'information piratée, divulguée ou volée. Pour sa part, l'OSSNR n'a relevé aucune occurrence où ce type d'information aurait été collectée pendant que le MDN/FAC exerçait son mandat. De plus, le MDN/FAC estime que la formation qu'il faut obligatoirement suivre avant de mener des activités OSINT conjuguée aux recherches manuelles que les analystes effectuent pour corroborer l'information et demeurer à l'affût des contenus non fiables ou problématiques sur le plan juridique permet d'atténuer les risques associés à la collecte. S'il découvre que les résultats d'une collecte contiennent de l'information douteuse, voire illégale, le MDN/FAC cesse d'utiliser l'outil en question.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Assurance et options

49. L'OSSNR a noté, dans le cas de certains outils, que l'évaluation faite par le MDN/FAC abordait certains aspects pertinents en matière de risque, entre autres, le fait d'établir si des renseignements personnels ont été collectés au moyen de l'outil en question, s'agissant particulièrement de données relatives à des Canadiens. Toutefois, dans la plupart des autres cas, les évaluations ne cherchaient pas à établir si des renseignements personnels avaient été collectés ou s'il existait des risques juridiques pouvant être liés à la collecte de renseignements relatifs à des Canadiens. Enfin, les évaluations d'outils n'ont pas pris en compte les évaluations effectuées au niveau du commandement, bien que ces deux fonctions soient directement liées l'une à l'autre.

50. L'OSSNR a également observé [redacted] 15 fournisseurs de données tiers que le MDN/FAC caractérise comme étant des outils employés pour la « recherche de personnes ». Fait crucialement important, ce type de service fournit un accès à de l'information qui pourrait avoir été obtenue en violation de l'attente raisonnable d'une personne à la protection de ses renseignements personnels (p. ex. noms et prénoms officiels, dates de naissance, adresses, numéros de téléphone, titres de propriété, antécédents personnels et professionnels, adresses IP). Or, le MDN/FAC n'a effectué aucune évaluation de ces outils.

15(1) a)

51. Avant d'utiliser les outils en ligne, particulièrement lorsqu'il s'agit de recourir aux fournisseurs de données, le MDN/FAC doit procéder à une évaluation des risques pertinents. Parmi les principaux risques qu'il convient d'évaluer, il faut compter les effets du recours à ces services particuliers. Pourtant, le MDN/FAC n'a réalisé aucune évaluation des facteurs relatifs à la vie privée pour les activités liées à l'OSINT, et ce, même si les institutions fédérales y sont tenues en vertu de la « Directive sur les pratiques relatives à la protection de la vie privée » du Secrétariat du Conseil du Trésor[9].

52. Le MDN/FAC doit aussi tenir adéquatement compte des limites pratiques de la validation de certains outils en ligne et déterminer ce qui doit être fait en pareil cas. Par exemple, les fournisseurs de données peuvent refuser de divulguer les méthodes exclusives de collecte et d'analyse ou encore les sources d'information à leurs abonnés. Lorsqu'il est impossible d'établir pleinement la provenance de l'information, les analystes ne sont pas en mesure d'établir le degré de risque. C'est particulièrement le cas lorsqu'aucune corroboration n'est possible. Dans ce cas de figure, il pourrait être nécessaire d'empêcher tout recours à l'outil/au service en question.

---

[9] Voir le site Web du Secrétariat du Conseil du Trésor et consulter la Directive sur les pratiques relatives à la protection de la vie privée, 4.1.11, https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=18309.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Recommandation 3. L'OSSNR recommande que le MDN/FAC réalise une analyse approfondie des risques de non-conformité aux dispositions de la loi et des politiques, qui sont posés par le recours à des fournisseurs de données tiers et qu'il mette en place les moyens permettant d'atténuer les risques connexes. En réaction aux évaluations juridiques et stratégiques, le MDN/FAC devrait resserrer ses critères d'évaluation et les employer chaque fois qu'il évalue un fournisseur de données tiers auquel il aura recours dans le cadre de ses activités de renseignement de sources ouvertes.

Lien avec des Canadiens

53. Comme nous l'avons indiqué à la section « Contexte » du présent rapport, le CPSNR a fait part de ses préoccupations, en 2020, quant à l'absence de « clarté législative » lorsqu'il s'agit d'encadrer la collecte du renseignement de défense. D'ailleurs, ce commentaire coïncidait avec la collecte inappropriée visant des Canadiens réalisée dans le contexte de l'opération LASER, du MDN/FAC. En fait, l'objet de la présente section est, dans un premier temps, d'établir la mesure dans laquelle la collecte OSINT actuelle du MDN/FAC vise des Canadiens et, dans un second temps, de faire part de l'évaluation de l'OSSNR concernant les garde-fous qui orientent ce type de collecte.

Constatation 7. L'OSSNR constate que l'instrument de politique qui encadre la collecte d'information sur des Canadiens ne tient pas suffisamment compte des risques d'atteinte à la vie privée posés par les activités de renseignement de sources ouvertes menées sur Internet.

Constatation 8. L'OSSNR constate que le suivi exercé par le MDN/FAC sur les activités de renseignement de sources ouvertes sur Internet comporte, sur le plan de la structure et de la gestion de l'information, des lacunes qui limitent l'aptitude de l'OSSNR à vérifier si lesdites activités sont manifestement nécessaires s'agissant d'une collecte touchant des Canadiens.

54. La Directive fonctionnelle CANCIT du MDN/FAC explique que l'abréviation CANCIT (pour *Canadian Citizen*) désigne les renseignements personnels sur un citoyen canadien ou sur un résident permanent. La Directive fonctionnelle CANCIT indique que toute collecte d'information relative à des Canadiens survenant pendant des activités de renseignement de défense doit être manifestement nécessaire au déroulement de l'opération militaire autorisée ou d'une autre activité de défense légitime. La Directive fonctionnelle CANCIT met l'accent sur la conformité aux dispositions de la *Loi sur la protection des renseignements personnels* et sur la nécessité de protéger l'information personnelle que le MDN/FAC gère grâce à une banque de renseignements personnels distincte. En outre, la collecte de renseignements personnels sur des Canadiens doit être documentée, et en cas de collecte accidentelle, les renseignements doivent être évalués.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Advenant qu'ils n'aient rien à voir avec l'opération militaire autorisée ou avec une autre activité de défense, lesdits renseignements doivent être supprimés.

55. Pendant l'examen, l'OSSNR n'a pas été en mesure de vérifier si les activités OSINT du MDN/FAC s'étaient concentrées de façon inappropriée sur des Canadiens ou sur leurs renseignements personnels. Néanmoins, parmi le nombre limité des cas examinés, l'OSSNR n'a relevé aucune activité OSINT du MDN/FAC qui puisse avoir donné lieu à une collecte excessive de renseignements personnels sur des Canadiens. Ce constat a été confirmé ultérieurement, à la suite de séances d'information, d'entrevues et de réponses écrites suivant lesquelles le MDN/FAC a clairement indiqué qu'il préférait éviter toute collecte de renseignements sur des Canadiens.

56. Tout compte fait, la collecte OSINT du MDN/FAC n'a pas pour objet de cibler des personnes. Essentiellement, elle est plutôt façonnée par les enjeux déterminants[10]. Par exemple, bien que l'examen ait permis de remarquer que le MDN/FAC évaluait les plateformes de réseaux sociaux – lesquels peuvent tout à fait contenir des commentaires formulés par des Canadiens –, il faut savoir que l'OSINT collecté est parfaitement exempt de renseignements personnels. En fait, la collecte a plutôt pour objectif de capter les sentiments généraux et les tendances ou de prendre connaissance de recherches militaires hautement spécialisées. Il ne s'agit pas ici de sous-entendre que rien ne saurait justifier le fait que le MDN/FAC cible un Canadien, quoique, même lorsque les circonstances le justifient, il s'avère que les renseignements personnels sont généralement supprimés du produit OSINT final ou que celui-ci n'est retransmis qu'à quelques intervenants choisis.

Paramètres stratégiques

57. La Directive OSINT du MDN/FAC fait valoir que toute collecte d'information sur des Canadiens doit être conforme aux stipulations de la Directive fonctionnelle CANCIT. Autrement dit, ces deux directives fonctionnelles ont pour objet de se renforcer mutuellement tout en faisant valoir qu'il convient de faire preuve d'une certaine réserve lorsqu'il s'agit de Canadiens. Toutefois, l'OSSNR a remarqué que la Directive fonctionnelle CANCIT excluait intentionnellement certaines activités OSINT, ce qui introduit une forme d'incohérence dans le cadre stratégique.

58. Pour illustrer ce propos, précisons que le MDN/FAC a établi trois catégories d'autorisation pour l'OSINT dans le but de régir et de gouverner ces activités. Ces autorisations ont une

---

[10] Les activités sur Internet menées par l'Unité nationale de contre-ingérence des Forces canadiennes, par exemple, ne sont pas couvertes par la politique OSINT. En fait, ces activités sont plutôt régies par un ensemble de politiques et de procédures à part, et tendent à se concentrer sur le personnel du MDN/FAC.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

incidence sur le choix des activités qui feront l'objet d'une vérification et d'une surveillance plus étroites. Il convient donc de noter que l'une des catégories OSINT est explicitement exclue de la Directive fonctionnelle CANCIT, et que le MDN/FAC affirme que toute collecte d'information relevant de cette catégorie « ne correspond pas à la notion de CANCIT ».

59. Le MDN/FAC affirme que cette décision est justifiée dans la mesure où la probabilité qu'il y ait une attente raisonnable en matière de protection des renseignements personnels à l'égard d'information provenant de sources publiquement accessibles « est extrêmement faible ». De plus, le MDN/FAC déclare que les analystes OSINT sont formés pour savoir à partir de quand leur activité n'est plus visée par la politique ou les directives et quand il convient de demander de nouvelles consignes. Toutefois, cette explication ne dit rien sur la portée des outils ou sur l'information qui peut être accessible et utilisée dans une catégorie d'activités OSINT qui pourrait comprendre l'information venant des fournisseurs de données. Certains de ces fournisseurs de données vont certainement fournir un accès à des renseignements sur des Canadiens, même si une part de cette information pourrait susciter de vives préoccupations en matière de protection de la vie privée.

60. Comme il est énoncé dans la Directive OSINT, toute collecte doit puiser son information dans des sources publiquement accessibles, et cette information ne doit susciter aucune attente raisonnable juridiquement défendable en matière de protection des renseignements personnels, quelle que soit la catégorie d'OSINT employée. Bien que le MDN/FAC puisse collecter de l'information publiquement accessible sur des Canadiens, il ne faut pas nécessairement conclure que cette information ne comporte aucun risque d'atteinte à la protection des renseignements personnels.

61. Le principal point de mire du MDN/FAC en matière de renseignement (p. ex. principalement les adversaires étrangers) et les considérations d'ordre pratique qui orientent un commandant dans ses intentions de collecte (p. ex. les tendances par opposition aux renseignements sur des personnes) incitent à éviter la collecte directe d'information sur des Canadiens. Toutefois, le cadre stratégique sur l'OSINT tient compte des changements de priorités en matière de renseignement et de collecte, ce qui n'empêcherait pas le MDN/FAC de redéfinir ses visées en matière de renseignement et de collecter de l'information sur des Canadiens. Ainsi, les préoccupations exprimées par le CPSNR en 2020 concernant le fait de miser sur une simple politique pour encadrer les activités de renseignement de défense sont toujours d'actualité.

Autorité approbatrice

62. Lorsque la Directive fonctionnelle CANCIT est entrée en vigueur, certaines catégories d'OSINT axées sur l'information relative à des Canadiens devaient recevoir, préalablement à la collecte, une approbation distincte de la part du Chef d'état-major de la Défense ou

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

du sous-ministre. Cette mesure correspondait aux pratiques normales en vigueur dans l'ensemble du gouvernement, où les activités perçues comme étant particulièrement intrusives ou délicates nécessitent l'approbation d'un échelon supérieur. Cependant, le MDN/FAC a ensuite précisé qu'il n'était pas nécessaire d'obtenir une approbation distincte pour la collecte planifiée d'information CANCIT, lorsque celle-ci est menée à l'occasion d'activités de renseignement de défense menées dans le contexte d'opérations et de mesures autorisées. Lorsque l'OSSNR a demandé comment cette décision pouvait se justifier, le MDN/FAC a répondu qu'une « double autorisation » n'était pas nécessaire. Autrement dit, l'approbation initiale d'une opération militaire ou d'une autre activité de défense est suffisante pour justifier la collecte CANCIT.

63. Le fait de changer la pratique voulant que le Chef d'état-major de la Défense accorde, à la collecte CANCIT, une autorisation distincte de celle, plus générale, accordée à une opération militaire ou à une activité de défense se voulait pragmatique : l'intention était de simplifier le processus d'autorisation. Toutefois, le MDN/FAC a maintes fois répété à l'OSSNR que la collecte CANCIT constituait une activité exceptionnelle. Pourtant, ce processus d'approbation semble contredire cette position, dans la mesure où l'on considère la collecte d'information sur des Canadiens comme une simple fonction des opérations militaires ou d'autres activités de défense.

64. L'absence d'une approbation explicite de la collecte CANCIT n'est pas sans conséquences. Dans le présent rapport, on a déjà établi que le MDN/FAC n'enregistrait pas régulièrement le lien entre les activités OSINT et l'opération ou l'activité de défense connexe. Même si la Directive fonctionnelle CANCIT exige que toute collecte sur des Canadiens soit manifestement nécessaire, cette exigence ne peut pas être pleinement vérifiée en raison de l'absence de documents formels permettant d'assurer un suivi des activités OSINT en général et, par le fait même, des activités OSINT concernant plus particulièrement des Canadiens.

65. Une autre question difficile tient aux produits de renseignement qui sont associés à l'OSINT et dans lesquels il pourrait y avoir de l'information CANCIT. Or d'après la Directive fonctionnelle CANCIT, le MDN/FAC est tenu de documenter [traduction] « la collecte, l'utilisation et la conservation » de l'information sur des Canadiens. Malgré cette exigence, le MDN/FAC ne dispose d'aucune liste complète des produits du renseignement de défense. Ainsi, l'OSSNR n'a pas été en mesure d'établir pleinement quels étaient les produits de renseignement qui contenaient de l'information CANCIT.

66. Ces contraintes qui pèsent sur les mesures de vérification découlent d'une structure axée sur le commandement qui prévaut depuis longtemps au sein des FAC. Elles découlent également de pratiques de gestion de l'information en vigueur dans l'ensemble du MDN/FAC, lesquelles pratiques ont accentué le cloisonnement des fonctions du renseignement. Nonobstant les facteurs organisationnels ou les pratiques de gestion de

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

l'information, cette réalité n'exonère pas le MDN/FAC de l'obligation de fournir des justifications précises et formellement énoncées quant aux activités du renseignement de défense touchant des Canadiens. C'est précisément parce que la collecte du MDN/FAC touchant des Canadiens est régie par un document de politique plutôt que par un texte de loi, qu'il convient d'accorder une importance particulière à la nécessité de suivre un processus d'approbation et des règles de responsabilisation qui soient rigoureux. Ainsi, il importe de faire le nécessaire pour empêcher tout glissement vers une régularisation de la collecte touchant des Canadiens.

Recommandation 4. L'OSSNR recommande que le MDN/FAC modifie ses politiques de sorte à résoudre la question relative à la collecte d'information sur des Canadiens menée dans le cadre des activités de renseignement de sources ouvertes sur Internet et qu'il s'assure de disposer des documents qu'il convient de produire pour montrer que les activités sont nécessaires.

Responsabilisation et conformité

67. L'objet de la présente section est de faire part de ce que l'OSSNR a déterminé concernant le caractère adéquat des mesures de surveillance et de conformité que le MDN/FAC applique aux activités OSINT.

Constatation 9. L'OSSNR constate que les mesures de surveillance et de conformité que le MDN/FAC applique aux activités de renseignement de sources ouvertes menées sur Internet ne sont pas parvenues à atténuer tous les risques pertinents.

---

68. Les directives OSINT du MDN/FAC indiquent que, pour atténuer les risques, les activités doivent faire l'objet de mesures de surveillance et de conformité. Or, l'une des principales mesures de surveillance consiste à tenir à jour des journaux de vérification mensuelle des activités. Il conviendrait également d'effectuer un examen limité des activités enregistrées par certains comptes d'analystes.

69. Comme il a été dit précédemment, le MDN/FAC a établi des catégories d'autorisation pour l'OSINT. L'une de ces catégories, laquelle comprend une part importante des activités OSINT du MDN/FAC, permet aux analystes d'accéder à Internet directement, sans qu'aucune politique n'exige quelque forme de suivi ou de vérification. Toutes les autres catégories nécessitent le recours à un système de gestion de l'attribution, à savoir un outil employé pour brouiller les traces d'activité du MDN/FAC sur Internet. Seules les catégories d'autorisation nécessitant le recours au système de gestion de l'attribution produisent une journalisation des activités grâce à une fonction intégrée.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

70. Concernant les activités faisant l'objet d'une vérification, le système de gestion des attributions du MDN/FAC procure une visibilité complète des activités menées par les analystes. En l'occurrence, ce système produit divers journaux de vérification dans lesquels sont enregistrés les accès aux sites Web, les téléchargements et les données envoyées à une imprimante.

71. En dépit de cette capacité technique, le MDN/FAC a plutôt réduit la portée de sa fonction de vérification en la limitant à la sécurité opérationnelle [redacted]

15(1) a)

[redacted] Concrètement, [redacted]

72. Le système de gestion de l'attribution offre également au MDN/FAC la chance de tirer de l'information des journaux de vérification et d'investir cette information dans les évaluations des risques que posent les activités OSINT sur le plan diplomatique et politique, juridique ou réputationnel. Autrement dit, le système du MDN/FAC est assez polyvalent pour effectuer des vérifications liées à des risques autres que la sécurité opérationnelle. Bien que cette fonction fût disponible, l'OSSNR a constaté que le MDN/FAC n'avait pas exploité les journaux de vérification à cette fin, même si la Directive OSINT avait reconnu que d'autres catégories de risques méritaient qu'on s'y attarde.

Recommandation 5. L'OSSNR recommande que le MDN/FAC documente régulièrement et uniformément les activités de renseignement de sources ouvertes menées sur Internet de sorte à favoriser l'application des mesures de conformité.

IV. Conclusion

73. Le présent rapport propose une analyse des activités OSINT du MDN/FAC, plus particulièrement de celles ayant un lien avec des Canadiens. Pour être licites, les activités OSINT doivent être directement liées à une opération militaire ou à une autre activité de défense autorisées, et la collecte d'information doit se limiter à ce qui est publiquement accessible.

74. Puisque la sphère des activités en ligne évolue rapidement au gré des avancées technologiques et des attentes sociétales en matière de protection de la vie privée, le MDN/FAC doit disposer d'un cadre de gouvernance adéquat pour les activités OSINT. Certains problèmes ont été soulevés dans le présent rapport dans le but d'aider le MDN/FAC à améliorer sa posture et à résoudre de nouvelles difficultés tout en favorisant le principe de responsabilisation et en tenant compte du caractère évolutif des activités

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

de renseignement en ligne. Du reste, l'information obtenue dans le cadre de la présente analyse essentielle des activités OSINT permettra à l'OSSNR de planifier de nouveaux examens et d'en établir le degré de priorité.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Annexe A. Constatations et recommandations

Dans le cadre du présent examen, l'OSSNR a formulé les constatations et recommandations suivantes.

Pouvoirs en matière de collecte

Constatation 1. L'OSSNR constate que le MDN/FAC dispose de l'autorisation légale de mener des activités de renseignement de sources ouvertes sur Internet lui permettant de répondre à des besoins en matière de renseignement de défense.

Constatation 2. L'OSSNR constate que le MDN/FAC n'enregistre pas systématiquement les liens entre, d'une part, les activités de collecte d'information provenant de sources ouvertes et, d'autre part, les opérations ou activités de défense approuvées.

Recommandation 1. L'OSSNR recommande que le MDN/FAC documente formellement et au moment propice l'attribution des tâches de collecte sur Internet, de sorte à formaliser le lien avec l'activité du renseignement de défense.

Évaluation des risques

Constatation 3. L'OSSNR constate que les évaluations de risques du MDN/FAC qui servent à orienter les activités de renseignement de sources ouvertes sur Internet ne sont pas mises à jour en temps opportun et n'abordent pas tous les risques énumérés dans l'instrument de politique s'appliquant à tous les commandements.

Recommandation 2. L'OSSNR recommande que, dans les 12 mois, puis tous les deux ans, le MDN/FAC fasse, au niveau du commandement, une mise à jour de toutes les évaluations de risques pour ce qui concerne les activités de sources ouvertes sur Internet et veille à ce que toutes les catégories de risques concernées soient suffisamment reconnues, évaluées et gérées.

Méthodes et outils de collecte

Constatation 4. L'OSSNR constate que le MDN/FAC a établi des critères permettant d'évaluer les fournisseurs de données tiers dans le but de veiller à ce que les activités de renseignement de sources ouvertes menées sur Internet soient conformes aux lois et aux politiques applicables.

Constatation 5. L'OSSNR constate que le MDN/FAC n'applique pas systématiquement ses critères d'évaluation des fournisseurs de données tiers auxquels il a recours pour ses activités de renseignement de source ouvertes sur Internet, ce qui accroît le niveau de risque sur le plan juridique et politique.

15(1) a)

Constatation 6. L'OSSNR constate que le MDN/FAC n'a réalisé aucune évaluation [redacted] 15 fournisseurs de données tiers qui se spécialisent dans la collecte d'information sur les personnes.

Document released under the *Access to Information Act* /
Document divulgé en vertu de la *Loi sur l'accès à l'information*

Recommandation 3. L'OSSNR recommande que le MDN/FAC réalise une analyse approfondie des risques de non-conformité aux dispositions de la loi et des politiques, qui sont posés par le recours à des fournisseurs de données tiers et qu'il mette en place les moyens permettant d'atténuer les risques connexes. En réaction aux évaluations juridiques et stratégiques, le MDN/FAC devrait resserrer ses critères d'évaluation et les employer chaque fois qu'il évalue un fournisseur de données tiers auquel il aura recours dans le cadre de ses activités de renseignement de sources ouvertes.

Lien avec des Canadiens

Constatation 7. L'OSSNR constate que l'instrument de politique qui encadre la collecte d'information sur des Canadiens ne tient pas suffisamment compte des risques d'atteinte à la vie privée posés par les activités de renseignement de sources ouvertes menées sur Internet.

Constatation 8. L'OSSNR constate que le suivi exercé par le MDN/FAC sur les activités de renseignement de sources ouvertes sur Internet comporte, sur le plan de la structure et de la gestion de l'information, des lacunes qui limitent l'aptitude de l'OSSNR à vérifier si lesdites activités sont manifestement nécessaires s'agissant d'une collecte touchant des Canadiens.

Recommandation 4. L'OSSNR recommande que le MDN/FAC modifie ses politiques de sorte à résoudre la question relative à la collecte d'information sur des Canadiens menée dans le cadre des activités de renseignement de sources ouvertes sur Internet et qu'il s'assure de disposer des documents qu'il convient de produire pour montrer que les activités sont nécessaires.

Responsabilisation et conformité

Constatation 9. L'OSSNR constate que les mesures de surveillance et de conformité que le MDN/FAC applique aux activités de renseignement de sources ouvertes menées sur Internet ne sont pas parvenues à atténuer tous les risques pertinents.

Recommandation 5. L'OSSNR recommande que le MDN/FAC documente régulièrement et uniformément les activités de renseignement de sources ouvertes menées sur Internet de sorte à favoriser l'application des mesures de conformité.