



Le Comité des parlementaires sur la sécurité nationale et le renseignement

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

Présenté au premier ministre le 30 août 2019 en vertu du paragraphe 21(2)
de la *Loi sur le comité des parlementaires sur la sécurité nationale et le renseignement*
(Version révisée selon le paragraphe 21(5) de la *Loi sur le CPSNR*)

© Sa Majesté la Reine du chef du Canada (2020)

Tous droits réservés.

Ottawa, ON.

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport spécial sur la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens dans le contexte des activités du renseignement de défense du ministère de la Défense nationale et des Forces armées canadiennes (Version révisée selon le paragraphe 21(5) de la *Loi sur le CPSNR*)

CP104-2/2020F (Imprimé)

ISBN 978-0-660-33059-4 (Imprimé)

CP104-2/2020F-PDF (En ligne)

ISBN 978-0-660-33058-7 (En ligne)

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

**Le Comité des parlementaires
sur la sécurité nationale et le renseignement**

**L'honorable David McGuinty, C.P., député
Président**

**Présenté au premier ministre le 30 août 2019
Version révisée déposée au Parlement en mars 2020**

Révisions

En application du paragraphe 21(2) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* (Loi sur le CPSNR), le Comité peut présenter au premier ministre et au ministre concerné un rapport spécial sur toute question liée à son mandat. Conformément au paragraphe 21(5) de la Loi sur le CPSNR, le premier ministre peut, après consultation du président du Comité, ordonner au Comité de lui présenter un rapport révisé du rapport annuel ou spécial qui ne contient pas de renseignements dont la communication porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales, ou qui sont protégés par le secret professionnel de l'avocat, selon le premier ministre.

Le présent document constitue une version révisée du Rapport spécial fourni au premier ministre le 30 août 2019. Les révisions ont été apportées de façon à retirer l'information dont la communication, selon le premier ministre, porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales, ou qui est protégée par le secret professionnel de l'avocat. Lorsque la suppression n'affecte pas la lisibilité du texte, le Comité a signalé la suppression par trois astérisques (***) dans le texte du présent document. À l'inverse, le Comité a révisé le document pour résumer l'information retirée. Ces passages sont signalés par trois astérisques au début et à la fin du résumé et sont placés entre crochets (voir l'exemple ci-dessous).

EXEMPLE: [*** Les passages révisés sont signalés par trois astérisques en début et en fin de phrase, et le résumé est placé entre crochets. ***]

Le Rapport spécial inclut la lettre du 30 août 2019 du président du Comité au ministre de la Défense nationale. Cette lettre était à l'origine classifiée SECRET//Réservé aux Canadiens puisque le rapport ci-joint l'était à l'époque.

**LE COMITÉ DES PARLEMENTAIRES
SUR LA SÉCURITÉ NATIONALE ET LE RENSEIGNEMENT**

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

L'honorable Percy Downe, sénateur

L'honorable Rob Nicholson, C.P., Q.C.,
député

Monsieur Emmanuel Dubourg, député

Monsieur Murray Rankin, député
(a démissionné le 1^{er} août 2019)

L'honorable Diane Finley, C.P., députée

L'honorable Hedy Fry, C.P. députée

Madame Brenda Shanahan, députée

Madame Gudie Hutchings, députée

L'honorable Vernon White, sénateur

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

National Security and Intelligence
Committee of Parliamentarians



Comité des parlementaires sur la
sécurité nationale et le renseignement

Chair

Président

Le 9 mars 2020

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 du Comité des parlementaires sur la sécurité nationale et le renseignement, j'ai le plaisir de vous présenter notre rapport spécial sur la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les citoyens canadiens par le ministère de la Défense nationale et les Forces armées canadiennes lors de la conduite d'activités de renseignement de défense. Ce rapport unanime contient quatre conclusions, dont une a été entièrement caviardée, et trois recommandations visant à clarifier et améliorer la gouvernance de cette importante et délicate activité.

Conformément au paragraphe 21(5) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*, le rapport a été révisé pour en exclure des renseignements dont la communication porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales ou des renseignements protégés par le secret professionnel de l'avocat.

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

A handwritten signature in blue ink, appearing to read 'D. McGuinty', with a small dot at the end.

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



Chair

Président

SECRET // CCS (avec la pièce jointe)

Le 30 août 2019

L'honorable Harjit S. Sajjan, C.P., député
Ministre de la Défense nationale
101, promenade du Colonel By
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 21(2) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement (Loi sur le CPSNR)*, je suis heureux de vous présenter le Rapport spécial du Comité sur la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens dans le contexte des activités de renseignement du ministère de la Défense nationale et des Forces armées canadiennes. Le Rapport spécial comprend quatre conclusions et trois recommandations. Une copie du Rapport spécial a aussi été présentée au très honorable Justin Trudeau, C.P., député, le Premier ministre du Canada.

Il convient de noter que, comme le stipule le paragraphe 31(1) de la *Loi sur le CPSNR*, j'ai également présenté une copie du Rapport spécial au procureur général pour l'informer de la conclusion du Comité selon laquelle le ministère de la Défense nationale ne se conforme pas entièrement à la *Loi sur la protection des renseignements personnels*.

Veuillez agréer mes salutations distinguées.

A handwritten signature in blue ink, appearing to read 'D. McGuinty', with a large flourish at the end.

L'honorable David McGuinty, C.P., député
Président

P.j.

Table des matières

Introduction	1
Chapitre 1 : Le contexte opérationnel	5
Les citoyens canadiens qui combattent à l'étranger	5
Le ciblage des Canadiens par les forces alliées	6
Les délibérations des représentants gouvernementaux.....	7
Opération à l'étranger ***	8
Chapitre 2 : Le cadre juridique	11
Les fondements juridiques pertinents au renseignement de défense	11
La prérogative de la Couronne	11
Le cadre juridique des activités du renseignement de défense qui sont menées au Canada	12
Le cadre juridique des activités du renseignement de défense qui sont menées dans les opérations internationales	13
L'application extraterritoriale du droit canadien.....	14
Le <i>Code criminel</i>	14
La <i>Loi sur la protection des renseignements personnels</i>	15
La <i>Charte canadienne des droits et libertés</i>	16
Chapitre 3 : Le traitement de l'information sur des Canadiens avant la directive fonctionnelle CANCIT	19
Les activités de renseignement à l'aide d'Internet	19
Le renseignement d'origine électromagnétique.....	21
Le renseignement d'origine humaine	22
L'exploitation des sources et les interrogatoires dans le cadre du renseignement	22
Le débriefing stratégique	22
Les données biométriques	23
La contre-ingérence	24
Le matériel et l'équipement capturés / l'équipement et les documents saisis	26
L'échange du MEC *** avec le MDN/FAC et la directive fonctionnelle CANCIT.....	27
Les questions soulevées par l'échange du MEC avec le MDN/FAC.....	28

Chapitre 4 : La directive fonctionnelle CANCELIT	31
Les objectifs et l'application de la directive fonctionnelle CANCELIT.....	31
Le fondement juridique.....	32
L'orientation stratégique.....	33
Chapitre 5 : L'évaluation du Comité	35
Le cadre stratégique du MDN/FAC relatif aux Canadiens.....	36
L'application extraterritoriale de la <i>Loi sur la protection des renseignements personnels</i>	39
La collecte de renseignements sur les Canadiens.....	42
Les interdictions dans les politiques du MDN/FAC relatives à la collecte intentionnelle de renseignements sur les Canadiens	42
La prérogative de la Couronne	44
Conclusion.....	47
Conclusions du Comité	49
Recommandations	50
Annexe A – La directive fonctionnelle CANCELIT	51
Annexe B – Liste des témoins	61

Introduction

1. En 2018, le Comité des parlementaires sur la sécurité nationale et le renseignement (le Comité) a procédé à un examen des activités du renseignement de défense du ministère de la Défense nationale et des Forces armées canadiennes (MDN/FAC). Cet examen avait pour objectif, tout d'abord, d'augmenter la sensibilisation et les connaissances des Canadiens et des parlementaires à l'égard du mandat et des activités du MDN et des FAC en matière de renseignement de défense. Cet examen a porté sur le cadre juridique et la structure organisationnelle générale du programme de renseignement de défense du MDN et des FAC¹. Dans la dernière partie de cet examen, le MDN/FAC a fourni au Comité la directive fonctionnelle du Chef du renseignement de la défense à l'égard de la collecte de renseignements sur les citoyens canadiens (titre officiel en anglais *Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information*) ci-après désigné par directive fonctionnelle CANCELIT. Le Comité a déterminé qu'il n'avait pas suffisamment de temps pour analyser cette nouvelle directive et l'intégrer à son Rapport annuel 2018, mais qu'elle soulevait d'importantes questions qui méritaient une attention supplémentaire.

2. Le Comité a invoqué trois raisons justifiant cet examen. Premièrement, le Comité voulait réconcilier la contradiction apparente entre les déclarations faites par le MDN/FAC en 2018 et le but de la directive fonctionnelle CANCELIT. En effet, le MDN/FAC avait déclaré dans des présentations devant le Comité qu'il ne cible pas les Canadiens dans ses activités du renseignement de défense². Ces déclarations semblent contredire le titre et la substance de la directive fonctionnelle CANCELIT. En bref, à première vue, la directive fonctionnelle CANCELIT semble autoriser le MDN/FAC à viser les Canadiens dans le cadre de ses activités du renseignement de défense.

3. Deuxièmement, le Comité voulait comprendre le cadre juridique qui gouverne la collecte, l'utilisation, la conservation et la communication d'information sur des Canadiens par le MDN/FAC. Tel que mentionné dans le Rapport annuel 2018 du Comité, les autorisations pour utiliser ce que le MDN/FAC décrit comme le spectre complet des activités du renseignement de défense découlent de la *Loi sur la défense nationale* (assistance à une organisation gouvernementale) ou à l'exercice de la prérogative de la Couronne. Les activités menées en vertu de la prérogative de la Couronne ne sont pas autorisées par une loi du Parlement. En comparaison, tous les autres organismes du renseignement canadiens fonctionnent en vertu d'un régime juridique précis, qui est adapté à leur mandat, particulièrement lorsqu'il est question de renseignements sur les Canadiens³. Le Comité voulait revisiter son évaluation précédente des autorisations du MDN/FAC afin de déterminer si des modifications

¹ Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), *Rapport annuel 2018*.

² Ministère de la Défense nationale et Forces armées canadiennes (MDN/FAC), déclarations au Secrétariat du CPSNR, 1^{er} novembre 2018; MDN/FAC, observations au Comité, 4 décembre 2018.

³ Voir par exemple les articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, et partie V.1 de la *Loi sur la défense nationale* (Centre de la sécurité des télécommunications). Au moment de la présentation du rapport, la partie V.1 de la *Loi sur la défense nationale* avait été abrogée et remplacée par la *Loi sur le Centre de la sécurité des télécommunications*, qui est entrée en vigueur le 1^{er} août 2019. Pour plus de clarté, le présent rapport renvoie à la structure de pouvoir prévue à la partie V.1 de la *Loi sur la défense nationale*, qui était en vigueur pendant la période faisant l'objet de l'examen.

étaient nécessaires aux conclusions et aux recommandations qui figurent au Chapitre 4 du Rapport annuel 2018 du Comité.

4. Finalement, le Comité voulait évaluer si les cadres juridiques et stratégiques sur lesquels reposent la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens par le MDN/FAC soulèvent des risques juridiques ou opérationnels particuliers.

5. Le cadre de référence de l'examen énonçait quatre objectifs précis :

- Décrire l'autorité et le cadre stratégique du MDN/FAC pour la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens;
- Décrire les circonstances dans lesquelles la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens sont autorisées, et dans quels buts, comparativement aux circonstances où ces activités sont interdites;
- Décrire de quelle manière le MDN/FAC fait le suivi de la collecte, de l'utilisation, de la conservation et de la diffusion des renseignements sur les citoyens canadiens et consigne cette information;
- Évaluer les cadres juridique, stratégique et administratif grâce auxquels la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens sont permises ou interdites.

6. Le 6 décembre 2018, le Comité a informé le ministre de la Défense nationale de sa décision de préparer un Rapport spécial, en vertu du paragraphe 21(2) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement (Loi sur le CPSNR)*, sur la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens dans le contexte des activités du renseignement de défense du MDN/FAC. Le même jour, le Comité a fourni au ministre de la Défense nationale le cadre de référence du Rapport spécial.

7. Entre le 6 décembre 2018 et le 23 août 2019, le Comité a examiné les documents qui avaient été reçus du MDN/FAC (classifiés et non classifiés) dans le cadre de l'examen de 2018, ainsi que plus de 950 pages de nouveaux documents destinés au présent rapport, qui comprenaient des avis juridiques, des lettres ministérielles, des directives ministérielles, des directives et des ordonnances fonctionnelles et opérationnelles, des notes d'information, des présentations et des autorisations opérationnelles. Le Comité a ajouté à ces documents des résultats de recherches universitaires et juridiques. Des représentants du MDN/FAC ont témoigné devant le Comité à une occasion, ont rencontré le personnel du Secrétariat à sept reprises, et ont fourni des réponses écrites aux questions du Comité. Le Comité a tenu une audience avec les représentants du MDN/FAC. Le Comité a aussi reçu de l'information de la part d'autres ministères et organismes fédéraux, tels que le Centre de la sécurité des télécommunications (CST), concernant ses politiques visant à protéger les renseignements personnels des Canadiens; le ministère de la Justice, concernant *** et le Service canadien du renseignement de la sécurité (SCRS) concernant *** Le Comité a aussi demandé l'avis du Bureau du commissaire à la protection de la vie privée sur une des recommandations du Comité.

8. Le présent rapport comporte quatre sections. La première section présente une description du contexte dans lequel le MDN/FAC entre en contact avec de l'information sur des Canadiens dans la conduite de ses opérations. La deuxième section sert à expliquer le cadre juridique de ces opérations, et est largement tirée du Rapport annuel 2018 du Comité. La troisième section décrit les parties les plus pertinentes de la directive fonctionnelle CANCIT. Le Comité formule ensuite son évaluation, ses conclusions et ses recommandations. Pendant le déroulement de l'examen, le Comité a connu quelques difficultés dans ses interactions avec le MDN/FAC, notamment :

- Le MDN/FAC a déclaré qu'il n'y avait pas eu d'échange de courriels entre les fonctionnaires responsables de l'élaboration de la directive, laquelle a duré un an. L'absence de ces courriels a empêché le Comité de déterminer le motif de cette directive.
- Dans certains cas, le MDN/FAC a fourni des résumés de l'information importante, au lieu des documents d'origine, ce qui aurait permis au Comité de juger par lui-même des faits en cause.
- Le MDN/FAC n'a pas fourni de son propre chef des documents pertinents à l'examen, et qui, comme l'a découvert par la suite le Comité, avaient été divulgués en vertu de demandes d'accès à l'information.

9. Le Comité a fondé son évaluation, ses conclusions et ses recommandations sur les faits qui lui ont été présentés.

Chapitre 1 : Le contexte opérationnel

10. La directive fonctionnelle du Chef du renseignement de la défense à l'égard de la collecte de renseignements sur les citoyens canadiens a été créée pour tenir compte des problèmes qui découlent d'un environnement d'une complexité croissante dans lequel le MDN/FAC aurait à composer avec des combattants ennemis qui sont également des Canadiens⁴. Étant donné l'ampleur du soutien que le renseignement apporte aux opérations, la probabilité que le MDN/FAC entre en contact avec de l'information sur des Canadiens dans le cadre de ses activités de renseignement n'est pas que possible; cette situation est quasi inévitable.

Les citoyens canadiens qui combattent à l'étranger

11. Des citoyens canadiens se rendent à l'étranger afin de se joindre à divers groupes qui cherchent à atteindre leurs buts par des moyens violents. Ces Canadiens s'associent à ces groupes de diverses façons, notamment par les plateformes en ligne qui sont utilisées par les terroristes et les extrémistes violents pour mener des activités de recrutement ou d'endoctrinement ciblées, et pour encourager leurs partisans à la violence⁵. Les données les plus récentes indiquent qu'approximativement 190 voyageurs extrémistes (aussi connu sous le nom de combattants étrangers) qui ont des liens avec le Canada se trouvent à l'étranger, y compris à des endroits comme l'Irak, la Syrie, la Turquie, l'Afghanistan, le Pakistan, l'Afrique du Nord et le Moyen Orient⁶. Les médias ont rapporté en avril 2019 que depuis 2012, des terroristes canadiens pourraient avoir tué ou blessé plus de 300 personnes à l'extérieur du Canada, et que des citoyens de 19 pays avaient été tués dans des attaques auxquelles des Canadiens auraient participé⁷. Voici des exemples de ces attaques :

- En juillet 2012, Hassan El Hajj Hassan, un membre allégué du Hezbollah, de Vancouver, en Colombie-Britannique, aurait, semble-t-il, joué un rôle important dans un complot pour faire exploser une bombe dans un autobus en Bulgarie, tuant cinq passagers et le chauffeur⁸.
- En janvier 2013, Ali Medlej et Xristos Xatsiroubas, deux Canadiens de London, en Ontario, ont pris part à l'attaque contre l'usine de gaz Amenas en Algérie, qui a fait plus de 60 morts⁹.
- En avril 2013, Mahad Ali Dhore, un membre canadien d'Al Chabaab, a participé à l'attaque contre la Cour suprême de Somalie, causant 34 morts¹⁰.

⁴ La directive fonctionnelle CANCIT définit « citoyen canadien » au sens de l'article 3 de la *Loi sur la citoyenneté*, L.R.C. 1985, ch. C-29; ou un résident permanent au sens de l'article 2 de la *Loi sur l'immigration et la protection des réfugiés*, L.C. 2001, ch. 27. Le terme « Canadien » est utilisé dans l'ensemble du présent rapport.

⁵ Sécurité publique Canada, *Rapport public de 2018 sur la menace terroriste pour le Canada*, sans date.

⁶ Sécurité publique Canada, *Rapport public de 2018 sur la menace terroriste pour le Canada*, sans date.

⁷ Stewart Bell, « Deadly Export: Canadians responsible for hundreds of terrorism death and injuries overseas », *Global News*, 11 avril 2019, https://globalnews.ca/news/5117211/deadly-export-canadian-terrorists/?utm_source=%40globalnews&utm_medium=Twitter.

⁸ Sécurité publique Canada, *Rapport public de 2014 sur la menace terroriste pour le Canada*.

www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2014-pblc-rpr-trrrst-thrt/2014-pblc-rpr-trrrst-thrt-eng.pdf.

⁹ Gendarmerie royale du Canada (GRC), *Guide de sensibilisation au terrorisme et à l'extrémisme violent*, juin 2016. www.rcmp-grc.gc.ca/fr/guide-sensibilisation-au-terrorisme-et-a-lextremisme-violent.

12. Dans le cadre de sa contribution à la sécurité internationale, le Canada a déployé le MDN/FAC à des endroits qui sont connus pour avoir attiré des voyageurs extrémistes. Dans un cas, le MDN/FAC a obtenu de l'information sur des Canadiens dans l'exécution de missions déployées, causant des problèmes juridiques et opérationnels pour les forces déployées¹¹. Dans un autre cas, le MDN/FAC a travaillé avec ***¹² Ces cas sont expliqués plus en détail ci-dessous.

Le ciblage des Canadiens par les forces alliées

13. Dans une note d'information du 16 septembre 2015 à l'intention du Chef d'état-major de la Défense figurent des détails sur les problèmes stratégiques associés au ciblage de combattants ennemis qui sont également des citoyens canadiens. Cette note stipule :

[traduction] Compte tenu que le Canada est engagé dans un conflit armé contre l'EIL [Daech] et des groupes armés associés, les opérations du MDN/FAC dans le cadre de l'opération IMPACT [la contribution du Canada à la Coalition mondiale contre Daech] comprennent à la fois du soutien direct aux frappes, de même que la participation à celles-ci, contre des ensembles d'objectifs qui incluent des combattants ennemis¹³. À l'occasion, ces ensembles d'objectifs consistent d'individus identifiés précis, dont la nationalité est parfois connue avant l'engagement. Le processus de ciblage de la Coalition veille à que tous les individus ciblés dans l'opération IMPACT soient réellement des combattants ennemis¹⁴. *** Par l'emploi du processus de la Coalition, et sa participation active avec les autres pays aux opérations *** le Canada **accroît la capacité de communiquer des informations**, et offre des options aux partenaires [du gouvernement du Canada] *** Bien que la nationalité des individus ciblés dans le contexte du droit des conflits

¹⁰ Sécurité publique du Canada, *Rapport public de 2014 sur la menace terroriste pour le Canada*, www.securitepublique.gc.ca/cnt/rsrscs/pblctns/2014-pblc-rpt-trrrst-thrt/index-fra.aspx.

¹¹ Pour une description détaillée des problèmes juridiques et opérationnels associés à cette affaire, voir les paragraphes 75 à 79 du chapitre 3 du présent rapport.

¹² Voir la section du présent Rapport spécial sur ***

¹³ L'opération IMPACT a été mise sur pied en septembre 2014. En plus de mener une campagne militaire, la Coalition mondiale est résolue à découvrir l'infrastructure économique et financière de Daech, à empêcher le transit de combattants terroristes étrangers d'un pays à l'autre, à appuyer la stabilisation et le redressement des services publics essentiels aux régions libérées de Daech, et à lutter contre la propagande de ce groupe (<https://theglobalcoalition.org/en>). Le MDN/FAC utilise un Centre du renseignement de toutes sources dans le cadre de cette opération. Il recueille de l'information de diverses sources, et est responsable de recueillir, de synthétiser et d'analyser cette information. Le renseignement qui en résulte sert ensuite à la planification opérationnelle afin de protéger les forces de la coalition et à déterminer comment mener les opérations de la coalition. www.canada.ca/fr/ministere-defense-nationale/services/operations/operations-militaires/operations-en-cours/operation-impact.html.

¹⁴ Pour le MDN/FAC, le « ciblage » est le processus de sélectionner et d'ordonner la priorité des objectifs et de faire correspondre l'intervention appropriée, en tenant compte des exigences et des capacités opérationnelles.

armés ne soit pas en cause, des **préoccupations sur le plan stratégique, politique et juridique pour le Canada peuvent apparaître**¹⁵. (gras ajouté)

14. [***Le paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée et en assurer la lisibilité. Il énonce que le MDN/FAC est au fait de tels incidents, y compris des endroits où le MDN/FAC a mené des opérations, et qu'un allié lui a demandé de fournir d'autre information. ***]¹⁶
***¹⁷

15. [***Le paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée et en assurer la lisibilité. Il décrit le contenu d'une note d'information au Chef d'état-major de la Défense, qui présentait trois recommandations. ***]

- ***
- ***
- ***¹⁸

Les délibérations des représentants gouvernementaux

16. La question de la participation de Canadiens aux conflits armés contre le MDN/FAC a été discutée au sein du gouvernement du Canada, notamment par le MDN/FAC. En 2015, le conseiller à la sécurité nationale et au renseignement auprès du premier ministre a tenu des discussions avec des cadres supérieurs du gouvernement sur l'utilisation possible d'une force létale contre des Canadiens dans le contexte de la campagne contre Daech. Bien que le MDN/FAC a déclaré que les activités du renseignement de défense [traduction] « n'entraînent généralement pas de risques aux droits et libertés des Canadiens¹⁹ », les notes préparées à l'avance de ces discussions pour le sous-ministre délégué de la Défense nationale et le sous-ministre délégué principal de la Défense nationale indiquent que la question de la communication de renseignement à des pays alliés avait été soulevée dans le contexte du phénomène des voyageurs extrémistes²⁰.

¹⁵ MDN/FAC, *OP IMPACT – Canadian Citizens and Targeting of ISIS Combatants*, note d'information pour le Chef d'état-major de la Défense (CEMD), 16 septembre 2015. Dans le contexte de l'examen du Comité des activités du renseignement de défense de 2018, les documents fournis par le MDN/FAC décrivent plus en détail le rôle du MDN/FAC dans le ciblage de la coalition, et définissent *** MDN, *** 23 décembre 2016.

¹⁶ ***

¹⁷ MDN/FAC, *OP IMPACT – Canadian Citizens and Targeting of ISIS Combatants*, note d'information pour le CEMD, 16 septembre 2015.

¹⁸ MDN/FAC, *OP IMPACT – Canadian Citizens and Targeting of ISIS Combatants*, note d'information pour le CEMD, 16 septembre 2015.

¹⁹ Murray Brewster, « A Parliamentary Committee is set to shine a light on the shadowy business of military intelligence », *CBC*, 8 avril 2019; MDN/FAC, *Accountability Measures taken and considered with respect to the Defence Intelligence Function*, note d'information pour le conseiller à la sécurité nationale auprès du premier ministre, 8 octobre 2015.

²⁰ MDN/FAC, note de scénario pour le sous-ministre associé principal – réunion du 29 septembre sur les citoyens canadiens et le ciblage des combattants de l'EIIL; note de scénario pour le sous-ministre associé principal – réunion du 9 octobre sur les citoyens canadiens et le ciblage des combattants de l'EIIL. Même si les notes de scénario ne sont pas datées, le MDN/FAC a confirmé qu'elles avaient été préparées en 2015.

17. *** a exprimé des préoccupations sur la communication au MDN/FAC de renseignement sur les Canadiens associés à Daech. Le MDN/FAC a déclaré dans une note d'information interne que pour *** [traduction] « ces préoccupations étaient probablement attribuable à des inquiétudes sur la manière dont le MDN/FAC, ou les alliés à qui le MDN/FAC peut transmettre le renseignement, peuvent utiliser ce renseignement à des fins de ciblage²¹. » Le MDN/FAC a mentionné les principales questions suivantes, en insistant sur le besoin d'en arriver à un accord par rapport au ciblage des Canadiens qui participent aux hostilités contre le Canada ou contre des pays alliés :

- Quel est le droit applicable?
- Dans le cas où des Canadiens sont identifiés comme des combattants [de Daech], quelles conditions devons-nous satisfaire pour *** des individus en cause?
- Lorsque des renseignements sur des Canadiens *** sachant qu'ils serviront au ciblage?
- Si une décision est prise concernant ces questions, quel mécanisme devrait être en place pour guider le processus décisionnel²²?

Opération à l'étranger ***

18. [***Le paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée. Il décrit une opération à l'étranger dans le cadre de laquelle la collecte de renseignements sur des Canadiens est devenue un enjeu pour les autorités canadiennes. ***]²³ ***²⁴ ***²⁵

19. [***Le paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée et en assurer la lisibilité. Il décrit les objectifs de la participation du MDN/FAC à une opération multinationale, jugée comme représentant une occasion unique pour le Canada de mieux comprendre la portée de la menace que posent les voyageurs extrémistes canadiens et les organisations extrémistes violentes envers les intérêts du Canada, au pays et à l'étranger. ***] ***²⁶ ***²⁷

20. [***Le paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée et en assurer la lisibilité. Il indique que le Comité a reçu de l'information contradictoire concernant les autorisations du MDN/FAC à participer à cette opération multinationale. En effet, le MDN/FAC affirme

²¹ MDN/FAC, note de scénario pour le sous-ministre associé principal – réunion du 9 octobre sur les citoyens canadiens et le ciblage des combattants de l'EIL. Tel qu'indiqué à la note au bas de page 14, pour le MDN/FAC, le « ciblage » est le processus de sélectionner et d'ordonner la priorité des objectifs et de faire correspondre l'intervention appropriée, en tenant compte des exigences et des capacités opérationnelles. Cette intervention peut comprendre une gamme d'options, jusqu'à l'usage de la force létale.

²² MDN/FAC, note de scénario pour le sous-ministre associé principal – réunion du 9 octobre sur les citoyens canadiens et le ciblage des combattants de l'EIL.

²³ MDN/FAC, Ordre de mission du CEMD pour ***

²⁴ MDN/FAC, Ordre de mission du CEMD pour ***

²⁵ Lettre ***

²⁶ ***

²⁷ MDN/FAC, *Action Briefing Note for the MND* ***

que la prérogative de la Couronne autorisait sa participation, alors que d'autres documents indiquaient que le MDN/FAC ne pouvait pas y participer au titre de ses propres autorisations. ***] ***²⁸ ***²⁹

21. [***Le paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée et en assurer la lisibilité. Il indique que le Canada a décidé que le MDN/FAC pouvait participer en application d'une autre autorisation. ***]***³⁰ ***³¹

²⁸ MDN/FAC, Réponses fournies aux questions du CPSNR liées *** dans le cadre de l'examen 2018 du CPSNR sur les activités du renseignement de défense du MDN/FAC.

²⁹ ***

³⁰ Lettre ***

³¹ Lettre ***

Chapitre 2 : Le cadre juridique

Les fondements juridiques pertinents au renseignement de défense

22. Le déploiement des membres des FAC et des employés du MDN, pour l'exécution entre autres d'activités du renseignement de défense, est régi par les lois canadiennes et internationales. Dans le cadre de l'examen de 2018 du Comité sur les activités du renseignement de défense du MDN/FAC, la juge-avocat général a donné les explications suivantes :

- Toutes les opérations des FAC sont autorisées par la loi.
- Toutes les opérations des FAC sont menées conformément à la loi.
- Alors que la source de l'autorisation légale peut varier :
 - Toutes les opérations nationales doivent avoir trouvé un fondement juridique dans les lois du Canada, et être menées conformément aux lois du Canada;
 - Toutes les opérations à l'étranger doivent trouver un fondement juridique dans les lois du Canada et le droit international, et doivent être menées conformément aux lois du Canada et au droit international applicable³².

23. Le MDN/FAC mène des activités du renseignement de défense à l'intérieur d'un cadre juridique unique et complexe. L'autorisation pour le MDN/FAC de mener la majorité de ces activités découle de la prérogative de la Couronne, alors que d'autres autorisations se trouvent dans les lois fédérales. Le MDN/FAC est également assujéti à d'autres instruments légaux internationaux et au droit international coutumier ayant force exécutoire, qui ont parfois une incidence sur la conduite des activités du renseignement de défense. Ces activités sont également assujéties à de nombreux instruments politiques, notamment des politiques gouvernementales générales, des directives et des autorisations ministérielles, des procédures et des politiques internes, des directives fonctionnelles et des ordres émis par la chaîne de commandement militaire. Le Rapport de 2018 du Comité décrit en vertu de quelles autorisations légales le MDN/FAC mène ses activités du renseignement de défense, et de quelle manière ces autorisations appuient la responsabilité du ministère et du ministre pour leur emploi. Les parties pertinentes du rapport sont résumées ici par soucis de commodité.

La prérogative de la Couronne

24. En plus des autorisations légales qui sont prévues par la *Loi constitutionnelle, 1867* et la *Loi sur la défense nationale*, la prérogative de la Couronne constitue le principal fondement juridique pour le déploiement des FAC. Elle représente aussi la source d'où le MDN/FAC prend son autorité pour mener les activités du renseignement de défense qui y sont associées. La prérogative de la Couronne est une source de pouvoir et de privilège exécutif qui est accordée par la *common law* à la Couronne, dans des

³² MDN/FAC, observations de la juge-avocat général au CPSNR, 19 juin 2018.

circonstances où l'autorité de la Couronne n'est pas autrement limitée³³. Le théoricien constitutionnel britannique A. V. Dicey décrit que la prérogative de la Couronne en tant que [traduction] « résidu du pouvoir discrétionnaire ou arbitraire, qui reste toujours aux mains de la Couronne³⁴. » Plus simplement, la prérogative de la Couronne est l'autorité exercée par le gouvernement pour prendre des décisions dans des domaines où les « mains de la Couronne » ne sont pas liées par la Constitution, une loi du Parlement ou une décision de la cour qui interprète la portée des pouvoirs du gouvernement.

25. Dans des termes plus généraux, l'autorisation de mener des activités du renseignement de défense est accessoire à l'autorisation de déployer des forces militaires. Comme l'a mentionné le MDN/FAC, [traduction] « l'autorisation de mener des activités du renseignement de défense est implicite lorsque le MDN/FAC est mandaté, en vertu des lois ou de l'exercice de la prérogative de la Couronne, de mener des opérations militaires et d'autres activités de défense³⁵. » Ni la *Loi sur la défense nationale* ni aucune autre loi ne contient de disposition qui régit spécifiquement la conduite d'activités du renseignement de défense par le MDN/FAC dans le contexte de l'exécution de son mandat de base.

26. Le MDN/FAC a déclaré que la conduite d'activités du renseignement de défense en vertu de la prérogative est conditionnelle à l'exigence d'un « lien raisonnable » entre les activités du renseignement de défense et la mission de défense, qui est censé servir de [traduction] « contraintes aux activités du renseignement de défense³⁶. » En 2013, le MDN/FAC a officialisé l'exigence de ce lien dans la Directive ministérielle sur le renseignement de défense.

Le cadre juridique des activités du renseignement de défense qui sont menées au Canada

27. Les activités du renseignement de défense peuvent appuyer les opérations nationales du MDN/FAC. Ces opérations sont autorisées en vertu des lois ou par l'exercice de la prérogative de la Couronne.

28. Lorsque des activités de renseignement servent à appuyer des opérations nationales, leur portée est circonscrite par la loi, par les responsabilités individuelles des divers ministères et organismes, et par l'équilibre des pouvoirs entre les compétences fédérales et provinciales. En ce qui concerne les lois nationales, le MDN a précisé plusieurs sources de droit³⁷ :

- **La Loi sur la défense nationale** : l'article 273.6 de la *Loi* permet au MDN/FAC d'accomplir des tâches de service public et de prêter assistance dans des questions d'application de la loi. La partie VI de la *Loi* détermine les circonstances dans lesquelles les FAC peuvent venir en aide au

³³ Peter W. Hogg, « *Constitutional Law of Canada* », Looseleaf ed. (Thomson Carswell, 1997).

³⁴ « *Reference as to the Effect of the Exercise of the Royal Prerogative of Mercy Upon Deportation Proceedings* », [1933] R.C.S. 269, à la page 272, selon C. J. Duff, citant A. V. Dicey, « *Introduction to the Study of the Law of the Constitution* », 8^e édition, Macmillan and Co, 1915.

³⁵ MDN, *** 27 avril 2018.

³⁶ MDN, observations écrites au CPSNR, 19 novembre 2018.

³⁷ MDN, *** 27 avril 2018; Cabinet du juge-avocat général, « *The Law of Interrogations. The Issue of Torture and Ill-treatment* », *Strategic Legal Paper Series*, Numéro 1, 2008; et MDN, *** 18 juillet 2003.

pouvoir civil (à savoir, intervenir en cas d'émeutes ou de troubles à la paix qui ne peuvent être réglés sans l'aide du MDN/FAC).

- **La Charte canadienne des droits et libertés** : Les activités de renseignement du MDN/FAC ne doivent pas enfreindre les dispositions de la *Charte*, particulièrement l'article 7 (le droit à la vie, à la liberté et à la sécurité de sa personne) et l'article 8 (le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives).
- **Le Code criminel** : Les activités de renseignement du MDN/FAC ne doivent pas enfreindre le *Code criminel*, notamment les articles sur l'interception des communications privées.
- **La Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels** : Les activités et les pratiques de conservation liées au renseignement du MDN/FAC doivent être conformes aux dispositions de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*.

29. Dans la plupart des cas, le MDN/FAC mène ses opérations au Canada à l'appui d'autres ministères ou organismes du gouvernement, à la demande officielle de leur ministre. Dans de tels cas, ces opérations, y compris les activités du renseignement de défense, sont menées en vertu des pouvoirs légaux de l'entité appuyée par le MDN/FAC. Comme l'a indiqué le juge-avocat général, [traduction] « lorsque les FAC soutiennent une autre organisation, leurs pouvoirs ne sont pas supérieurs à ceux de l'organisation appuyée³⁸. » En bref, le MDN/FAC peut mener une activité de renseignement (par exemple, intercepter des communications) en appui à une autre organisation fédérale (par exemple, la Gendarmerie royale canadienne), uniquement si cette organisation dispose elle-même de l'autorisation de le faire (par exemple, un mandat de la cour).

Le cadre juridique des activités du renseignement de défense qui sont menées dans les opérations internationales

30. Les activités du renseignement de défense en appui aux opérations internationales du MDN/FAC sont surtout menées sous l'autorité de la prérogative de la Couronne. Le MDN/FAC est également soumis aux instruments du droit international qui abordent les activités du renseignement de défense, tels que la *Charte des Nations Unies*, les *Conventions de Genève* et d'autres conventions et règles coutumières prévues dans le droit des conflits armés.

31. Le MDN/FAC a noté que la source précise de droit national ou international qui peut avoir une incidence sur une activité du renseignement de défense varie selon les circonstances de chaque cas, notamment :

- Le lieu de l'opération;
- Si l'opération est menée à l'invitation d'un pays étranger ou sous les auspices d'une résolution des Nations Unies;

³⁸ MDN, observations de la juge-avocat général au CPSNR, 19 juin 2018.

- Si l'opération est menée dans le cadre d'un conflit armé international reconnu, auxquels s'appliquent des instruments précis de droit international et de droit humanitaire international;
- Si une activité particulière est réputée contrevenir au droit international ou au droit humanitaire international.

L'application extraterritoriale du droit canadien

32. Le droit canadien suit le MDN/FAC. Cependant, il n'est pas toujours clair de savoir si une loi canadienne s'applique à l'extérieur du Canada. Cette section comporte des exemples sur la manière dont les lois canadiennes peuvent s'appliquer à l'extérieur du territoire. Elle fournit aussi un exemple

Le *Code criminel*

33. Que ce soit au Canada ou dans un déploiement à l'étranger, les membres des FAC sont assujettis au *Code de discipline militaire*, qui figure à la partie III de la *Loi sur la défense nationale*³⁹. Ce *Code* s'applique aussi au personnel du MDN qui accompagne les FAC dans les missions internationales. Il étend l'application du droit criminel canadien aux emplacements à l'étranger. Ainsi, si un membre des FAC (ou dans certains cas, un employé du MDN) commet une infraction criminelle, il peut être accusé d'une infraction militaire dans le système de justice militaire du Canada⁴⁰. Le terme « infraction militaire » comprend une infraction au terme de la *Loi sur la défense nationale*, du *Code criminel* ou d'autres lois du Parlement, commise par une personne alors qu'elle est soumise au *Code de discipline militaire*⁴¹.

34. Certaines parties du *Code criminel* ont trait directement aux activités du renseignement de défense. Par exemple, les activités du renseignement de source électromagnétique (SIGINT) entraînent un risque élevé d'interception de communications privées, ce qui constitue un acte criminel si l'activité qui a mené à l'interception a été réalisée sans autorisation judiciaire (un mandat, par exemple). Puisque le *Code de discipline militaire* étend l'application du *Code criminel* aux territoires étrangers, les membres du MDN/FAC qui interceptent des communications en provenance ou à destination du Canada pourraient s'exposer à des poursuites. Bien que certaines infractions ne s'appliquent pas aux membres du MDN/FAC⁴², le *Code criminel* ne comporte pas d'exception pour les interceptions qui ont lieu dans le cadre d'une mission militaire autorisée par la loi.

35. En vertu de la partie V.1 de la *Loi sur la défense nationale*, le ministre de la Défense nationale pouvait autoriser le CST à intercepter des communications privées si certaines conditions prévues dans

³⁹ MDN, observations écrites au CPSNR, 19 novembre 2018.

⁴⁰ *Loi sur la défense nationale*, art. 67.

⁴¹ *Loi sur la défense nationale*, art 2.

⁴² Voir par exemple l'article 117.08 du *Code criminel*, L.R.C., 1985, chap. C-46.

la loi étaient réunies⁴³. Lorsqu'une telle autorisation était en place, la partie VI du *Code criminel* ne s'appliquait pas à l'interception de communications privées⁴⁴. L'interception de communications privées en vertu de la partie V.1 de la *Loi sur la défense nationale*, lorsque le ministre l'avait autorisée, ne constituait pas alors une infraction criminelle. Lorsque le MDN/FAC menait des activités SIGINT sous l'autorité du CST, le personnel du MDN/FAC était soumis aux autorisations du ministre, et était également exempté de l'application de la partie VI du *Code criminel* à cet effet⁴⁵. Cela dit, le MDN/FAC devait également respecter les obligations, les politiques et les procédures légales en place pour le CST afin de protéger les renseignements personnels des Canadiens, notamment l'interdiction absolue de viser des Canadiens ou toute personne au Canada dans le cadre de ses activités de renseignement étranger SIGINT⁴⁶.

La Loi sur la protection des renseignements personnels

36. La *Loi sur la protection des renseignements personnels* est la loi qui régit les pratiques liées aux renseignements personnels des institutions du gouvernement fédéral, y compris le MDN/FAC⁴⁷. Cette loi s'applique à la façon dont les renseignements personnels sont recueillis, utilisés et communiqués par les institutions fédérales. Elle donne aussi le droit aux Canadiens d'accéder aux renseignements personnels les concernant qui sont gardées par ces institutions⁴⁸. Dans la plupart des cas, l'information qui est recueillie à la suite d'activités de renseignement, y compris dans le cadre des activités du renseignement de défense, constituent des renseignements personnel au sens de la *Loi sur la protection des renseignements personnels*⁴⁹.

37. Aucune jurisprudence n'existe concernant l'application ou non de la *Loi sur la protection des renseignements personnels* à l'extérieur du territoire du Canada. [*** Les paragraphes 37-40 ont été revus pour retirer de l'information préjudiciable ou privilégiée. Ils décrivent des consultations qui ont eu lieu entre ministères.***] ***⁵⁰

38. ***⁵¹ ***⁵²

39. ***

⁴³ *Loi sur la défense nationale*, para. 273.65(2).

⁴⁴ *Loi sur la défense nationale*, art. 273.69.

⁴⁵ MDN/FAC, *Ministerial Directive on the Integrated SIGINT Operations Model*.

⁴⁶ *Loi sur la défense nationale*, art. 273.64(2). Au moment de la présentation du rapport, la partie V.1 de la *Loi sur la défense nationale* avait été abrogée et remplacée par la *Loi sur le Centre de la sécurité des télécommunications*, qui est entrée en vigueur le 1^{er} août 2019.

⁴⁷ *Loi sur la protection des renseignements personnels*, L.R.C., 1985, chap. P-21.

⁴⁸ www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels/r_o_a/

⁴⁹ Voir la définition de « renseignements personnels » à l'article 3 de la *Loi sur la protection des renseignements personnels*.

⁵⁰ ***

⁵¹ *Règlement sur la protection des renseignements personnels*, DORS/83-508.

⁵² ***

40. *** **53

La Charte canadienne des droits et libertés

41. La *Charte* s'applique clairement aux activités de renseignement du MDN/FAC sur le territoire canadien⁵⁴. Son application aux activités du renseignement de défense à l'extérieur du territoire est moins claire. [***Le reste du paragraphe a été supprimé pour retirer de l'information préjudiciable ou privilégiée. Il traite de l'application extraterritoriale de la *Charte*.***]⁵⁵

42. Le droit canadien offre des protections constitutionnelles solides contre l'intrusion du gouvernement dans la vie des Canadiens. Si la *Charte* s'appliquait aux activités du renseignement de défense extraterritoriales du MDN/FAC, ces activités devraient se conformer, par exemple, à l'article 8 de la *Charte*, qui prévoit que « Chacun a droit à la protection contre les fouilles, les perquisitions et les saisies abusives. » Généralement, une fouille ou une saisie sera jugée raisonnable si elle est autorisée par la loi (le plus souvent dans un statut) que cette loi est raisonnable, et la manière dont la fouille et la saisie sont menées est raisonnable⁵⁶. Dans la plupart des cas, l'État ne peut pas intervenir lorsqu'il y a des attentes raisonnables à l'égard du respect de la vie privée, à moins que l'activité en question de l'État ait été autorisée par un juge.

43. Dans le contexte de la sécurité nationale et du renseignement, deux lois se rapportent à cet examen (en plus du *Code criminel*, expliqué aux paragraphes 33-35)⁵⁷. La première régit les activités du Service canadien du renseignement de sécurité (SCRS) au Canada et à l'extérieur, à savoir la Loi sur le SCRS : « Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. » Le directeur du SCRS peut, au besoin selon le contexte d'une enquête du genre, faire une demande auprès d'un juge désigné de la Cour fédérale pour un mandat l'autorisant à utiliser certaines mesures intrusives dans le cadre de la collecte de renseignement. L'activité autorisée peut comprendre l'interception de communications privées de Canadiens, ou la saisie de dispositifs qui contiennent des renseignements personnels. Le juge désigné peut imposer des conditions qu'il juge appropriées. L'autorisation accordée au SCRS par la Cour fédérale peut s'appliquer au renseignement sur des Canadiens au pays ou à

⁵³ Observations au CPSNR par le conseiller juridique et avocat général adjoint, Conseiller juridique de la défense nationale et des Forces canadiennes (ministère de la Justice), 30 mai 2019.

⁵⁴ « La présente charte s'applique au Parlement et au gouvernement du Canada, pour tous les domaines relevant du Parlement, y compris ceux qui concernent le territoire du Yukon et les territoires du Nord-Ouest » *Charte canadienne des droits et liberté*, partie 1 de la *Loi constitutionnelle*, annexe B de la *Loi de 1982 sur le Canada*, 1982. c. 11, alinéa 32(1)(a).

⁵⁵ MDN/FAC, ***

⁵⁶ *R. c. Collins*, [1987] 1 R.C.S. 265; *Hunter c. Southam*, [1984] 2 R.C.S. 145; *R. c. Nolet*, [2010] 1 R.C.S. 851; *R. c. Shepherd*, [2009] 2 R.C.S. 527.

⁵⁷ L'application de la partie VI du *Code criminel* (interceptions de communications privées) ne prévoit aucune exception pour le MDN/FAC peu importe le contexte. Selon le *Code de discipline militaire*, la partie VI s'applique au MDN/FAC.

l'étranger. La partie VI du *Code criminel* (interception de communications privées) ne s'applique pas aux cas où l'interception est autorisée par un mandat⁵⁸.

44. La deuxième loi qui se rapporte est la partie V.1 de la *Loi sur la défense nationale (Centre de la sécurité des télécommunications)*, qui autorisait un certain niveau d'intrusion dans la vie privée des personnes. Entre autre choses, la partie V.1 de la *Loi* conférait au Centre de la sécurité des télécommunications (CST) le mandat d'acquérir et d'utiliser de l'information de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers en conformité avec les priorités du gouvernement du Canada en matière de renseignement⁵⁹. Elle interdisait aussi au CST de viser les Canadiens à l'étranger ou toute personne au Canada dans ses activités. Celles-ci devaient aussi être soumises à des mesures pour protéger la vie privée des Canadiens dans l'utilisation et la conservation de l'information interceptée. En vertu de cette *Loi*, le ministre de la Défense nationale pouvait autoriser le CST à intercepter des communications privées dans l'exécution de son mandat, pourvu que les conditions établies dans la *Loi* fussent réunies.

45. Toutefois, les sources d'autorisations légales pour interférer avec les droits qui sont protégés par la *Charte* ne se limitent pas aux lois. Les tribunaux canadiens ont reconnu que dans certains cas restreints, le *Common Law* peut accorder suffisamment d'autorité pour mener une fouille ou une saisie⁶⁰. Ces cas se sont limités pour l'instant aux actions des forces de l'ordre. Aucune jurisprudence n'existe à l'heure actuelle laissant croire que le droit commun fournit une justification suffisante pour l'utilisation de méthodes ou de techniques intrusives dans le contexte des activités de sécurité nationale et de renseignement, y compris les activités du renseignement de défense.

⁵⁸ Loi sur le SCRS, L.R.C., 1985, chap. C-23, ss. 2, 12, 21, 21.1 et 26.

⁵⁹ En 2019, le projet de loi C-59, *Loi concernant des questions de sécurité nationale*, L.C. 2019, ch. 13, partie 3, établit la Loi sur le CST, qui confère au CST le mandat suivant : 15(1) Le Centre est l'organisme national du renseignement électromagnétique en matière de renseignement étranger et l'expert technique de la cybersécurité et de l'assurance de l'information. Le projet de loi a reçu la sanction royale le 21 juin 2019, et est entré en vigueur le 1^{er} août 2019.

⁶⁰ Voir par exemple *R. c. Caslake*, [1998] 1 R.C.S. 51.

Chapitre 3 : Le traitement de l'information sur des Canadiens avant la directive fonctionnelle CANSIT

46. Le MDN/FAC a déclaré qu'avant la publication de la directive fonctionnelle CANSIT, [traduction] « l'orientation pour la manipulation [de l'information sur des Canadiens] était fournie dans des politiques et des directives distinctes liées à des disciplines ou à des activités précises du renseignement de défense dans lesquelles de l'information sur des citoyens canadiens peut être recueillie dans le cadre d'activités ou d'opérations autorisées du MDN/FAC⁶¹. » Parmi toutes les activités du renseignement de défense qui sont réalisées par le MDN/FAC, cinq ont retenu l'attention en raison de leur pertinence, dans le contexte de cet examen spécial, en ce qui a trait à la collecte, l'utilisation, la conservation et la communication d'information sur les Canadiens. Ces activités, expliquées plus en détail ci-dessous, sont :

- le renseignement à l'aide d'Internet;
- le renseignement de source électromagnétique (SIGINT);
- le renseignement d'origine humaine (HUMINT);
- la contre-ingérence;
- l'équipement et le matériel capturés (désigné depuis le 1^{er} avril 2019 par équipement et de documents saisis).

Les activités de renseignement à l'aide d'Internet

47. Le MDN/FAC définit les activités de renseignement à l'aide d'Internet par [traduction] « l'utilisation de ressources et de plateformes de source ouvertes sur Internet pour découvrir, recueillir et utiliser de l'information dans le but de générer des produits du renseignement ou d'y contribuer⁶². » Le Chef du renseignement de défense a publié la directive fonctionnelle du Chef du renseignement de la défense à l'égard du cadre pour la conduite d'activités de renseignement à l'aide d'Internet (*Chief of Defence Intelligence Functional Directive: Framework for the Conduct of Intelligence Activities Using the Internet*) en février 2017. Cette directive énonce qu'elle a pour but de [traduction] « permettre la conduite d'activités du renseignement de défense à l'aide d'Internet, en faisant en sorte que ces activités sont conformes au mandat du Ministère, et qu'elles tiennent compte du risque *** [et stipule] un processus d'analyse du risque standard et uniforme pour voir à ce que les autorisations, la technologie et les procédures appropriées sont employées⁶³. »

48. La directive décrit que les fondements juridiques sur lesquelles reposent les activités de renseignement à l'aide d'Internet sont cohérents aux fondements juridiques des autres activités du

⁶¹ MDN/FAC, réponse à la demande d'information du CPSNR, 25 mars 2019.

⁶² MDN/FAC, *Chief of Defence Intelligence Functional Directive: Framework for the Conduct of Intelligence Activities Using the Internet*.

⁶³ DND/CAF, *Chief of Defence Intelligence Functional Directive: Framework for the Conduct of Intelligence Activities Using the Internet*.

renseignement de défense. En d'autres mots, l'autorisation légale de mener des activités de renseignement à l'aide d'Internet se trouvent dans des éléments de la *common law*, et plus particulièrement dans la prérogative de la Couronne, dans les lois du Canada (par exemple, la *Loi sur la défense nationale*) et dans le droit international. Cette autorisation découle de l'autorisation du MDN/FAC de mener des activités et des opérations de défense autorisées, tel qu'approuvé par le gouvernement du Canada⁶⁴.

49. La directive comporte des contrôles clés pour la conduite d'activités de renseignement à l'aide d'Internet par le MDN/FAC, notamment :

- L'information ne peut pas être recueillie uniquement sur le motif qu'elle est publiquement disponible sur Internet – le personnel du MDN/FAC [traduction] « qui agit à titre d'agent de l'État doit voir à ce que la collecte soit légale et cohérente selon son mandat »;
- Le personnel du MDN/FAC ne doit pas recueillir intentionnellement de l'information sur des Canadiens, sauf lorsqu'il est autorisé à le faire par une autorité compétente disposant d'un mandat légal.

50. La directive n'interdit pas explicitement la collecte intentionnelle d'information sur les Canadiens. Elle reconnaît plutôt dans sa description des types d'activités et des méthodes à l'aide d'Internet qui sont utilisés pour acquérir de l'information sur Internet la possibilité que de l'information sur des citoyens canadiens soit recueillie intentionnellement ou accidentellement. Cette directive exige du personnel du MDN/FAC qu'il réalise une évaluation formelle du risque avant d'amorcer une opération de renseignement à l'aide d'Internet, qui doit comprendre, entre autres, une évaluation pour savoir si le personnel du MDN/FAC prévoit une collecte intentionnelle ou non de renseignements personnels sur des Canadiens. Lorsqu'il prévoit une collecte intentionnelle, le personnel du MDN/FAC est tenu de démontrer de quelle manière cette collecte est permise dans le mandat de la mission en question⁶⁵.

51. La directive mentionne également l'autorisation du MDN/FAC de fournir du soutien en matière de renseignement sur Internet à d'autres ministères ou organismes fédéraux, en vertu de l'article 273.6 de la *Loi sur la défense nationale*. [*** Le reste du paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée. Il donne un exemple du soutien en question offert par le MDN/FAC à un autre ministère. ***]⁶⁶

⁶⁴ MDN/FAC, *Chief of Defence Intelligence Functional Directive: Framework for the Conduct of Intelligence Activities Using the Internet*.

⁶⁵ MDN/FAC, *Chief of Defence Intelligence Functional Directive: Framework for the Conduct of Intelligence Activities Using the Internet*.

⁶⁶ MDN/FAC, réponse à la demande d'information du CPSNR, 25 mars 2019.

Le renseignement d'origine électromagnétique

52. Le renseignement d'origine électromagnétique (SIGINT) est dérivé de l'interception, de la collecte, du traitement et de l'analyse des communications et des liens de données, notamment les communications par courriel, par téléphone cellulaire et par téléphone. Le renseignement SIGINT comprend également le renseignement dérivé des émissions électromagnétiques et des signaux d'instruments provenant de dispositifs comme des radars et des systèmes de commande et de guidage de missiles⁶⁷.

53. Avant le 1^{er} août 2019, le MDN/FAC tirait son autorisation de mener des activités SIGINT de la prérogative de la Couronne, ou au moyen de l'autorisation légale du Centre de la sécurité des télécommunications (CST), qui figurait alors à la partie V.1 de la *Loi sur la défense nationale*⁶⁸. En ce qui a trait aux opérations déployées, le ministre de la Défense nationale avait délégué l'autorisation de mener des activités SIGINT du CST aux FAC, en conformité avec la directive ministérielle sur l'*Integrated SIGINT Operations Model*. Ainsi, les activités SIGINT du MDN/FAC, menées en vertu des autorisations du CST, étaient soumises aux mêmes restrictions de la partie V.1 de la *Loi sur la défense nationale*, notamment l'interdiction de viser des Canadiens⁶⁹. Ces activités sont également assujetties aux autorisations ministérielles pertinentes, et leur fondement juridique faisait l'objet d'un examen par le commissaire du CST⁷⁰. L'interdiction de viser des Canadiens était sujette à une exception : lorsque le CST fournissait une aide technique et opérationnelle aux forces de l'ordre fédérales en vertu de l'alinéa 273.64(1)(c) de la *Loi sur la défense nationale*. Les demandes d'assistance du CST au MDN/FAC auraient été soumises aux limites qu'impose la loi à l'organisme ou au ministère qui reçoit l'assistance (comme la GRC ou le SCRS⁷¹).

⁶⁷ La collecte d'information d'origine électromagnétique (SIGINT) par l'appareil canadien du renseignement est menée à la fois par le CST en vertu de la partie A de son mandat (renseignement étranger) et par le MDN/FAC dans le cadre de ses opérations déployées en vertu des autorisations qui lui sont déléguées par le CST. MDN/FAC, présentation au Secrétariat du CPSNR sur le « *Integrated SIGINT Operations Model* », 23 juillet 2018.

⁶⁸ Au moment de la présentation du présent rapport, la partie V.1 de la *Loi sur la défense nationale* avait été abrogée et remplacée par la *Loi sur le Centre de la sécurité des télécommunications*. Pour plus de clarté, le présent rapport renvoie à la structure de pouvoir en vertu de la partie V.1 de la *Loi sur la défense nationale*, qui était en vigueur pendant la période visée par l'examen.

⁶⁹ La collecte d'information d'origine électromagnétique (SIGINT) par l'appareil canadien du renseignement est menée à la fois par le CST en vertu de la partie A de son mandat (renseignement étranger) et par le MDN/FAC dans le cadre de ses opérations déployées en vertu des autorisations qui lui sont déléguées par le CST. MDN/FAC, présentation au Secrétariat du CPSNR sur le « *Integrated SIGINT Operations Model* », 23 juillet 2018. Le CST a noté que les FAC mènent aussi des activités SIGINT en vertu des autorisations du CST, qui ne sont pas réalisées en appui direct aux opérations déployées (par exemple, ***).

⁷⁰ Les rapports annuels du Bureau du commissaire du CST n'abordent pas tous les activités du Groupe des opérations d'information des Forces canadiennes. En règle générale, les activités SIGINT des FAC ne sont pas examinées systématiquement par le commissaire du CST, mais peuvent cependant faire l'objet d'un examen par celui-ci. CST, observations écrites au CPSNR, 1^{er} octobre 2018. De plus, si le MDN/FAC mène des activités SIGINT en vertu de la prérogative de la Couronne, le MDN/FAC ne serait pas soumis aux limites prescrites à la partie V.1 de la *Loi sur la défense nationale* et ne ferait pas l'objet d'un examen. Rétroactions du CST relativement au rapport CANCIT préliminaire, 21 juillet 2019.

⁷¹ MDN/FAC, déclaration en réponse aux demandes d'information du CPSNR, 25 mars 2019. Pour sa part, le CST n'a pu nommer un cas dans lequel le MDN/FAC a prêté assistance au CST à la suite d'une demande d'assistance en vertu de l'alinéa 273.64(1)(c) de la *Loi sur la défense nationale*. Rétroactions du CST relativement au rapport CANCIT préliminaire, 9 août 2019.

Le renseignement d'origine humaine

54. Le renseignement d'origine humaine (HUMINT) est le renseignement dérivé de la collecte et de l'analyse de renseignement de sources humaines. Les activités HUMINT sont menées par du personnel spécialisé du MDN/FAC. Le cadre stratégique relatif aux activités HUMINT du MDN/FAC renvoie à plusieurs spécialités dans la conduite des activités HUMINT, notamment : l'exploitation de sources, la conduite d'interrogatoires du renseignement et de débriefings stratégiques.

L'exploitation des sources et les interrogatoires dans le cadre du renseignement

55. Les opérations d'exploitation des sources sont des activités contrôlées HUMINT qui sont menées par des unités spécialisées et comprennent *** afin de recueillir et de fournir de l'information. La directive fonctionnelle du Chef du renseignement de la Défense à l'égard du cadre stratégique pour la conduite des activités HUMINT (*Chief of Defence Intelligence Functional Directive: CF Policy Framework for the Conduct of HUMINT Activities*) gouverne les opérations d'exploitation des sources.

56. Un interrogatoire du renseignement est défini comme le processus contrôlé, systématique et conforme sur le plan juridique d'utiliser des méthodes, des stratégies et des stratagèmes approuvés du MDN/FAC pour interroger des personnes placées en détention pendant des opérations internationales afin de recueillir de l'information dans le but de satisfaire à des exigences de renseignement. Les interrogatoires du renseignement sont gouvernés par la directive fonctionnelle du renseignement de défense 2014 à l'égard des opérations d'interrogatoires du renseignement HUMINT dans le cadre des opérations internationales (*Defence Intelligence Functional Directive: CF HUMINT Intelligence Interrogation Operations in International Operations 2014*).

57. Ni les opérations d'exploitation des sources ni les interrogatoires du renseignement ne peuvent viser ou autrement impliquer les Canadiens. Si un Canadien fait l'objet d'une opération de direction de source ou si de l'information sur un Canadien est recueillie accidentellement, l'opération doit être suspendue et l'incident doit être signalé au commandant de l'opération. Pareillement, si l'on détermine que le sujet de l'interrogatoire est un Canadien, l'interrogatoire doit être suspendu et l'incident doit être porté à l'attention de la chaîne de commandement dès que possible.

Le débriefing stratégique

58. Le MDN/FAC définit le débriefing comme l'interrogatoire volontaire de personnes qui peuvent avoir des connaissances d'intérêt pour le renseignement de défense, afin d'obtenir de l'information utile ou pour confirmer de l'information recueillie précédemment, en réponse à des exigences de renseignement de défense ou militaire. Par débriefing stratégique, on entend l'interrogatoire délibéré et systématique d'individus qui peuvent posséder de l'information pertinente aux besoins du renseignement stratégique et opérationnel. Ces activités sont régies par la directive fonctionnelle du

renseignement de défense 2015 sur le débriefing stratégique (*Defence Intelligence Functional Directive: Strategic Debriefing*).

59. La directive fonctionnelle sur le débriefing stratégique énonce que les débriefings stratégiques peuvent avoir lieu au Canada ou à l'étranger. Elle énumère aussi trois groupes de personnes qui peuvent avoir de l'information ayant valeur de renseignement qui justifierait la conduite de débriefings stratégiques :

- *** ces débriefings doivent être autorisés par le commandant du Commandement du renseignement des Forces canadiennes;
- *** ces débriefings doivent être autorisés au cas par cas par le ministre de la Défense nationale ou le Chef d'état-major de la Défense;
- *** ces débriefings doivent être autorisés au cas par cas par le ministre de la Défense nationale ou le Chef d'état-major de la Défense.

60. La directive fonctionnelle sur le débriefing stratégique stipule que le fondement juridique de mener ce type d'activité découle, comme pour toutes les activités du renseignement de défense, du droit canadien (par exemple, la *Loi sur la défense nationale*), du droit international et des éléments du *common law*, plus particulièrement de la prérogative de la Couronne. Conséquemment, toutes les méthodes employées dans la conduite de débriefing stratégique sont soumises au droit canadien et international et aux politiques et directives gouvernementales et ministérielles applicables. Ce type d'activité requiert aussi l'existence d'un lien entre la nature et la portée de l'activité et l'opération ou l'activité de défense autorisée par la loi.

Les données biométriques

61. Un ordre du MDN/FAC pour l'opération IMPACT interdit la collecte de données biométriques sur les Canadiens et l'autorise uniquement sur les ressortissants étrangers qui cherchent à entrer dans les zones contrôlées par le MDN/FAC⁷². Cet ordre stipule que si des données biométriques sur un Canadien sont recueillies accidentellement, et que le Canadien en question est jugé comme pouvant constituer une menace, les données doivent être séparées du reste des données. Le personnel du MDN/FAC est alors tenu de consulter la chaîne de commandement pour déterminer si les données peuvent être communiquées à une autre organisation du gouvernement du Canada. Si le Canadien dont les données ont été recueillies accidentellement ne constitue pas une menace, les données doivent être immédiatement supprimées de tous les systèmes.

⁷² MDN/FAC, *Biometrics – [Operation] IMPACT, Concept of Operations*, 22 juillet 2015.

La contre-ingérence

62. Le MDN/FAC définit la contre-ingérence comme les activités visant à déceler et à neutraliser les menaces contre la sécurité des employés du MDN, des militaires et des biens du MDN/FAC, résultant des activités de services ou d'organisations du renseignement de pays hostiles ou d'organisations ou d'agents se livrant ou susceptibles de se livrer à l'espionnage, au sabotage, à la subversion, au terrorisme, ou à des activités en rapport avec le crime organisé ou autres activités criminelles⁷³. Le MDN/FAC a déclaré que les opérations de contre-ingérence sont l'un des deux domaines qui ont été autorisés pour la collecte intentionnelle de données sur les Canadiens (l'autre étant une autre activité de renseignement) ***⁷⁴

63. Le MDN/FAC utilise différentes autorisations pour mener ses activités de contre-ingérence. Selon les explications du MDN/FAC, dans les opérations de déploiement, l'Unité nationale de contre-ingérence des Forces canadiennes mène des activités de contre-ingérence en vertu de l'exercice de la prérogative de la Couronne⁷⁵.

64. Pour les opérations au Canada, le MDN/FAC a déclaré que l'autorisation de mener des activités de contre-ingérence se trouve dans la Politique sur la sécurité du gouvernement, qui est publiée par le Secrétariat du Conseil du Trésor sous l'autorité de l'article 7 de la *Loi sur la gestion des finances publiques*. En application de l'autorité que confère cette politique aux administrateurs généraux, le Vice-chef d'état-major de la Défense a publié des directives et ordonnances administratives de la Défense (la série 8002) pour satisfaire à l'obligation du Chef d'état-major de la Défense et du sous-ministre, en leur qualité d'administrateurs généraux, de gérer les activités de sécurité au MDN/FAC⁷⁶. Le Chef du renseignement de la défense a aussi publié deux directives fonctionnelles sur les enquêtes relatives à la contre-ingérence. Ensembles, les directives fonctionnelles et la série 8002 établissaient le cadre du Programme national de contre-ingérence et le Comité de surveillance de la contre-ingérence. Ces instruments accordent aussi l'autorisation à l'Unité nationale de contre-ingérence des Forces canadiennes de recueillir, de rassembler et d'évaluer l'information de contre-ingérence sur les menaces à la sécurité afin de fournir du renseignement de sécurité, de l'information relative à la menace à la sécurité et des alertes précoces aux cadres supérieurs et aux commandants du MDN/FAC.

65. Le MDN/FAC a expliqué que l'Unité nationale de contre-ingérence des Forces canadiennes acquière de l'information sur des Canadiens dans les circonstances suivantes :

- Au moment de l'identification et de la surveillance des menaces à la sécurité du MDN/FAC;

⁷³ MDN/FAC, Directive et ordonnance administrative (DOAD 8002-0), Contre-ingérence, www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes/directives-ordonnances-administratives-defense/serie-8000/8002/8002.html.

⁷⁴ MDN/FAC, réponse à la demande d'information du CPSNR, 25 mars 2019.

⁷⁵ MDN/FAC, observations au CPSNR, 30 mai 2019

⁷⁶ MDN/FAC, Directive et ordonnance administrative (DOAD 8002), Table des matières, www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes/directives-ordonnances-administratives/serie-8000/8002.html.

- Dans la conduite des activités du Programme de liaison du renseignement de sécurité au titre de l'organisme responsable de la collecte de renseignement de sécurité;
- Au moyen de demandes d'accès à l'information approuvées par l'Unité nationale de contre-ingérence des Forces canadiennes (désignée en tant qu'organisme d'enquête dans la *Loi sur la protection des renseignements personnels*);
- Quand les autres ministères ou organismes fédéraux lui communiquent de l'information en conformité avec la *Loi sur la communication d'information ayant trait à la sécurité du Canada*⁷⁷;
- Dans les échanges avec le Centre d'analyse des opérations et des déclarations financières du Canada sur l'information financière liée aux personnes qui font l'objet d'une enquête active de l'Unité nationale de contre-ingérence des Forces canadiennes, en conformité au paragraphe 55.1(1) de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*⁷⁸.

66. Le MDN/FAC a déclaré que son système de tenue de dossiers n'était pas conçu pour produire des statistiques sur l'ampleur de la collecte, de la conservation, de l'utilisation et de la diffusion de renseignements sur les Canadiens par l'Unité nationale de contre-ingérence des Forces canadiennes⁷⁹. Cependant, le MDN/FAC a indiqué qu'entre le 1^{er} janvier et le 14 mars 2019, l'Unité avait rédigé *** rapports de contre-ingérence, parmi lesquels *** (80 %) contenaient de l'information sur des Canadiens, et *** dont le contenu avait été communiqué vive-voix par le MDN/FAC à des partenaires de la sécurité du Canada.

67. Le MDN/FAC a décrit cet échantillon de données comme représentatif de la quantité de renseignements sur les Canadiens que l'Unité peut obtenir de ses partenaires de sécurité canadiens ou leur communiquer dans une période donnée de dix semaines. Le MDN/FAC a déclaré qu'il communique ce renseignement à ses partenaires de la sécurité pour deux raisons : la première, pour déterminer si les partenaires possèdent de l'information défavorable sur une personne d'intérêt pour l'Unité nationale de contre-ingérence des Forces canadiennes; et la deuxième, pour déterminer si les partenaires de la sécurité possèdent de l'information qui laisse croire que la personne constitue une menace ou fait l'objet de menace. L'information de contre-ingérence, notamment l'information sur des Canadiens, peut être communiquée conformément à la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et à l'alinéa 8(2)(a) de la *Loi sur la protection des renseignements personnels*. Conformément à cette dernière, l'Unité nationale de contre-ingérence des Forces canadiennes maintient une banque de

⁷⁷ Pendant la période visée par l'examen, le titre de la version anglaise de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (*Security of Canada Information Sharing Act* (SCISA)) a été remplacé par *Security of Canada Information Disclosure Act* (SCIDA), au moment où la *Loi concernant des questions de sécurité nationale* (Projet de loi C-59) a reçu la sanction royale le 21 juin 2019.

⁷⁸ MDN/FAC, réponse à la demande d'information du CPSNR, 25 mars 2019.

⁷⁹ Le MDN/FAC a indiqué qu'il utilise à l'heure actuelle une base de données Microsoft Access pour consigner ses activités, et que les statistiques doivent en être manuellement extraites. L'Unité nationale de contre-ingérence des Forces canadiennes a formellement déterminé la nécessité d'un nouveau système et de nouveaux logiciels sophistiqués pour gérer l'information qu'elle conserve. MDN/FAC, réponse à la demande d'information du CPSNR, 25 mars 2019

renseignements personnels pour la collecte, la conservation et l'utilisation de l'information sur des Canadiens en appui à ses activités⁸⁰.

68. Bien que le MDN/FAC ait déclaré qu'il ne communique pas de renseignement réel ou potentiel à ses partenaires internationaux, le ministère a noté qu'il peut le diffuser en toute légalité, [traduction] « si la divulgation est autorisée en vertu de la *Loi sur la protection des renseignements personnels*, conformément à la *Charte* selon le cas, et conformément à l'instruction du ministre pour éviter la complicité dans les cas de mauvais traitement par des entités étrangères. » Toute communication proposée de renseignement ferait l'objet de consultations avec des conseillers juridiques et des conseillers politiques⁸¹.

Le matériel et l'équipement capturés / l'équipement et les documents saisis

69. Jusqu'à récemment, le matériel et l'équipement capturés (MEC) étaient régis au Canada par la directive fonctionnelle du Chef du renseignement de la Défense de 2012: *** (directive fonctionnelle sur le MEC de 2012). En juillet *** le MDN/FAC a ordonné que cette directive fonctionnelle soit révisée en raison de [traduction] « l'écart dans la politique du renseignement de défense, par rapport à la communication de renseignement dérivé de l'analyse du MEC⁸². » À ce moment, le Chef du renseignement de la Défense a publié une orientation stratégique intérimaire *** (*Interim Defence Intelligence Policy Guidance in Support of* *** Entre autres choses, l'orientation stratégique intérimaire stipulait que *** communiquera des renseignements *** uniquement si le ministère ou l'organisme canadien d'où proviennent les renseignements juge qu'il est possible de les communiquer⁸³. Le 1^{er} avril 2019, la directive fonctionnelle sur le MEC a été remplacée par la directive fonctionnelle du Chef du renseignement de la Défense : Exploitation de l'équipement et des documents saisis (la directive fonctionnelle sur l'EDS de 2019)⁸⁴.

70. Les termes matériel et équipement capturés (MEC) et équipement et documents saisis (EDS) englobent l'un et l'autre les documents, les supports d'information et l'équipement récupérés d'une personne capturée, pendant la fouille d'un emplacement, ou généralement, pendant la conduite d'une opération. L'exploitation du MEC constitue une activité courante du renseignement parmi les armées modernes, et fournit aux décideurs du renseignement concernant les capacités et les intentions des forces ennemies. Elle peut aussi fournir des renseignements pour la planification et la conduite d'opérations subséquentes, le ciblage et l'amorce d'autres activités de collecte de renseignement⁸⁵.

⁸⁰ Système de gestion de l'information 085 du MDN, fichiers de renseignements personnels.

⁸¹ MDN/FAC, réponse à la demande d'information du CPSNR, 25 mars 2019.

⁸² Lettre du Chef du renseignement de la Défense ***

⁸³ MDN/FAC, *Interim Defence Intelligence Policy Guidance in Support of* ***

⁸⁴ La Directive fonctionnelle du Chef du renseignement de la Défense : exploitation de l'équipement et des documents saisis a été approuvée le 10 janvier 2019 et est entrée en vigueur le 1^{er} avril 2019, et n'a pas été communiquée au Comité avant le 19 juillet 2019. Cette nouvelle directive fonctionnelle ne change en rien l'analyse des faits par le Comité.

⁸⁵ MDN/FAC, Directive fonctionnelle du Chef du renseignement de la Défense : *** 21 novembre 2012; et Directive fonctionnelle du Chef du renseignement de la Défense : exploitation de l'équipement et des documents saisis, 1^{er} avril 2019.

71. La directive fonctionnelle sur le MEC de 2012 et la directive fonctionnelle sur l'EDS de 2019 définissent l'exploitation comme la récupération et l'analyse systématique de l'équipement, des documents et des supports d'information. L'exploitation peut comprendre l'extraction et le traitement de l'information de nature technique, tactique ou procédurale au moyen de capacités particulières. Même si la directive fonctionnelle sur l'EDS de 2019 n'énumèrent pas ces capacités, la directive fonctionnelle sur le MEC de 2012 précise que ces capacités peuvent comprendre ***⁸⁶

72. La directive fonctionnelle sur le MEC de 2012 était muette sur la manière de gérer l'information sur des Canadiens. En contrepartie, la directive fonctionnelle sur l'EDS de 2019 prévoit que « si la collecte, la manipulation, la divulgation ou la communication de renseignements sur les citoyens canadiens a lieu, [la directive fonctionnelle CANCEL] s'appliquera. »

L'échange du MEC * avec le MDN/FAC et la directive fonctionnelle CANCEL**

73. L'absence d'une orientation claire sur la gestion de l'information sur des Canadiens *** a constitué un incitatif important pour l'élaboration de la directive fonctionnelle CANCEL. En général, le MDN/FAC attribuait la nécessité de cette directive aux changements dans l'environnement opérationnel, en expliquant que le risque de recueillir de l'information sur des Canadiens par accident avait augmenté dans les dernières années. Le MDN/FAC a cité trois nouveautés qui ont amplifié ce risque :

- L'arrivée de nouvelles capacités du renseignement, notamment la conduite accrue d'activités de renseignement à l'aide d'Internet par le MDN/FAC;
- L'augmentation de MEC récupérés sur le champ de bataille par les forces canadiennes et les forces de coalition;
- La difficulté liée au nombre croissant de Canadiens dans les zones d'opérations du MDN/FAC (par exemple, les voyageurs extrémistes⁸⁷).

74. Le MDN/FAC a toutefois cité un incident particulier *** qui a précipité la mise au point de la directive fonctionnelle CANCEL. À un certain moment donné en [*** Les deux phrases suivantes ont été revues pour supprimer l'information préjudiciable ou privilégiée et en assurer la lisibilité. Elles décrivent l'incident. ***]***⁸⁸ En fait, le MDN/FAC a indiqué qu'il avait découvert, dans les travaux pour préciser la portée de la directive, que certains membres du MDN/FAC pensaient que le MDN/FAC n'avait pas le droit de recueillir de l'information sur des Canadiens, peu importe les circonstances. Le MDN/FAC a expliqué que cette perception a mené le personnel du renseignement à demander une orientation *** sur la manière de gérer les informations sur des Canadiens qui étaient [***liées à l'incident***]⁸⁹. Le

⁸⁶ MDN/FAC, Directive fonctionnelle du Chef du renseignement de la Défense : *** 21 novembre 2012; et Directive fonctionnelle du Chef du renseignement de la Défense : exploitation de l'équipement et des documents saisis, 1^{er} avril 2019.

⁸⁷ MDN/FAC, réponse à la demande d'information du CPSNR, 25 mars 2019.

⁸⁸ MDN/FAC, *** *Intelligence Sharing Update*, note d'information pour le Chef d'état-major de la Défense, et le sous-ministre, 22 décembre

⁸⁹ MDN/FAC, réponse à la demande d'information du CPSNR, 25 mars 2019.

MDN/FAC a déclaré que le Ministère a élaboré la directive fonctionnelle CANCIT à titre d'orientation proactive afin de fournir au personnel du MDN/FAC des directives claires sur les circonstances où il est permis de recueillir de l'information sur des Canadiens. Le MDN/FAC voulait aussi décrire les procédures relatives à la déclaration, à la consignation et à la destruction d'information sur les Canadiens quand ces informations sont décelées ou recueillies par accident⁹⁰.

Les questions soulevées par l'échange du MEC avec le MDN/FAC

75. La communication du MEC *** au Canada a soulevé des problèmes immédiats au MDN/FAC concernant le bien-fondé juridique de communiquer ce renseignement aux autres organisations du gouvernement du Canada, et le caractère adéquat des cadres juridiques et stratégiques sur lequel repose *** Le MDN/FAC a déclaré que les activités du renseignement de défense mettent en cause des renseignements opérationnels très éphémères, dont la valeur diminue avec le temps⁹¹. Dans une note d'information à l'intention du Chef d'état-major de la Défense et du sous-ministre de la Défense nationale, les fonctionnaires du MDN/FAC ont déclaré que l'information trouvée *** aurait dû être communiquée dès que possible aux forces de l'ordre et aux organismes de sécurité du Canada, mais que cette communication avait été retardée par la complexité des différentes lois et politiques canadiennes sur la communication d'information. Ils ont décrit cette situation comme un exemple des problèmes plus généraux qui sont associés à la collecte, à la manipulation, à l'échange et à l'exploitation du MEC⁹².

76. La note d'information énumère trois questions générales liées à la communication et à l'exploitation de ces informations au Canada :

- Les mandats différents des organismes partenaires : le SCRS, la GRC et le CST ont chacun des mandats de sécurité nationale différents. Chacun possède des politiques et des exigences distinctes en matière de réception de renseignement de la part d'une entité externe.
- La communication de grands volumes d'information : les instruments actuels de communication de renseignement, tels que la *Loi sur la communication d'information ayant trait à la sécurité du Canada*, n'ont pas été créés en vue de tenir compte de grandes quantités d'information, ou d'information qui n'a pas été examinée pour en déterminer la nature.
- Les exigences de la *Loi sur la protection des renseignements personnels* concernant l'exploitation d'information par le MDN/FAC au Canada : si l'exploitation de cette information *** a lieu au Canada, les exigences cette loi doivent être satisfaites⁹³.

77. La question des exigences de la *Loi sur la protection des renseignements personnels* est particulièrement importante. [***Le paragraphe a été revu pour supprimer de l'information

⁹⁰ MDN/FAC, observations au CPSNR, 30 mai 2019.

⁹¹ MDN/FAC, *Accountability Measures Taken and Considered with Respect to the Defence Intelligence Function*, note d'information pour le conseiller à la sécurité nationale auprès du premier ministre, 8 octobre 2015.

⁹² MDN/FAC, *** *Intelligence Sharing Update*, note d'information pour le Chef d'état-major de la Défense, et le sous-ministre, 22 décembre ***

⁹³ MDN/FAC, *** *Intelligence Sharing Update*, note d'information pour le Chef d'état-major de la Défense, et le sous-ministre, 22 décembre ***

préjudiciable ou privilégiée et en assurer la lisibilité. Il indique que le MDN/FAC savait qu'une fois que les renseignements se trouvaient au Canada, les obligations au titre de la *Loi sur la protection des renseignements personnels* s'appliqueraient et il devrait se soumettre à certaines obligations et mettre en place une infrastructure requise. Ces obligations comprennent de déterminer la portée et la nature des renseignements personnels sur les Canadiens que possède le MDN/FAC, de faire en sorte que ces renseignements personnels ne sont utilisés qu'aux fins pour lesquelles ils ont été obtenus, et de déterminer les mesures en place pour protéger ces renseignements de tout accès non autorisés. La *Loi sur la protection des renseignements personnels* prévoit aussi une exigence relative à la création de fichiers de renseignements personnels afin de conserver des renseignements personnels⁹⁴. ***]⁹⁵

78. [*** Les paragraphes 78 et 79 ont été revus pour supprimer de l'information préjudiciable ou privilégiée et en assurer la lisibilité. Ils décrivent comment s'est concrétisée l'entente de coopération entre le MDN/FAC et un autre ministère. ***]⁹⁶

79. ***⁹⁷

⁹⁴ Voir le paragraphe 10(1) de la *Loi sur la protection des renseignements personnels*.

⁹⁵ MDN/FAC, ***

⁹⁶ Lettre du Chef d'état-major de la Défense et le sous-ministre ***

⁹⁷ Mémorandum au Chef d'état-major de la Défense et au sous-ministre, ***

Chapitre 4 : La directive fonctionnelle CANCEIT

Les objectifs et l'application de la directive fonctionnelle CANCEIT

80. La directive fonctionnelle du Chef du renseignement de la Défense relative à la collecte de renseignements personnels sur les Canadiens (*Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Personal Information*) (désignée par directive fonctionnelle CANCEIT) est une ordonnance pour tous les officiers et les militaires du rang des FAC et une directive pour tous les employés du MDN. Le but énoncé de cette directive est [traduction] :

- d'assurer la clarté des contraintes légales et stratégiques pour la collecte de renseignement sur les Canadiens dans la conduite des activités du renseignement de défense;
- de fournir une orientation pour les circonstances où de l'information sur des Canadiens est recueilli accidentellement par le MDN/FAC dans la conduite d'activités du renseignement de défense;
- d'établir des paramètres généraux pour la collecte de renseignement sur les Canadiens aux fins du renseignement de défense dans les environnements d'opérations et d'instruction⁹⁸.

81. Le MDN/FAC a déclaré que la directive fonctionnelle CANCEIT est censée s'appliquer à la collecte intentionnelle ou accidentelle de renseignement sur les Canadiens, qui a lieu dans le contexte de toute opération et activité de renseignement du MDN/FAC (au Canada et à l'étranger), à l'exception des activités qui sont déjà régies par des directives existantes concernant la collecte de renseignement sur les Canadiens⁹⁹. Avant la publication de la directive fonctionnelle CANCEIT, les directives relatives au traitement de renseignement sur les Canadiens étaient énoncées dans des politiques et des directives individuelles liées à des activités précises de renseignement, notamment le renseignement d'origine électromagnétique, d'origine humaine et la contre-ingérence, et qui sont toujours en vigueur (voir le chapitre 3). Conséquemment, le MDN/FAC a déclaré que la directive fonctionnelle CANCEIT ne s'applique pas à ces activités. Il a aussi déclaré que « La directive est très claire. Le personnel du MDN/FAC peut recueillir de manière délibérée des renseignements sur les Canadiens à des fins de renseignement uniquement dans deux types de circonstances : la première, en appui à une opération ou à une activité de défense autorisée – et actuellement, cette autorisation pour la collecte délibérée s'applique uniquement aux opérations de contre-ingérence; la deuxième, en appui à un autre ministère ou organisme du gouvernement, à la suite d'une demande d'assistance autorisée en vertu de l'article 273.6 de la *Loi sur la défense nationale*¹⁰⁰. Sans égard à ces déclarations, la directive fonctionnelle CANCEIT ne définit pas ou ne limite pas son application par rapport à d'autres directives concernant d'autres activités de renseignement, et ne précise pas qu'elle s'applique uniquement aux activités du

⁹⁸ MDN/FAC, *Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information*, 31 août 2018.

⁹⁹ MDN/FAC, observations au CPSNR, 30 mai 2019.

¹⁰⁰ MDN/FAC, observations au CPSNR, 30 mai 2019. À l'heure actuelle, *** s'inscrit dans le deuxième type.

renseignement de défense pour lesquelles il n'existe pas déjà une orientation concernant la collecte de renseignement sur les Canadiens.

Le fondement juridique

82. La directive fonctionnelle CANCIT énonce que le fondement juridique pour mener les activités du renseignement de défense est implicite lorsque le MDN/FAC est légalement autorisé de mener des opérations militaires ou d'autres activités de défense, en vertu des lois ou de l'exercice de la prérogative de la Couronne, et lorsqu'un lien clair existe entre la nature et la portée de l'activité du renseignement de défense, et la mission autorisée. Tous les moyens utilisés pour mener des activités du renseignement de défense demeurent cependant assujettis au droit canadien et international, aux politiques gouvernementales et aux directives ministérielles.

83. La directive fonctionnelle CANCIT précise que les opérations et les activités du MDN/FAC ne doivent pas comporter de collecte de renseignement sur les Canadiens à des fins de renseignement de défense. Cette interdiction est accompagnée de deux exceptions :

- La collecte a lieu en appui aux opérations ou aux activités de défense autorisées¹⁰¹;
- La collecte a lieu à l'appui d'un autre ministère ou organisme, et est subordonnée à l'autorité, au mandat et aux exigences, tels que prescrit par la loi, de cet autre ministère ou organisme.

84. Le MDN/FAC a expliqué que la directive fonctionnelle CANCIT n'accorde pas de nouvelle autorité pour recueillir de l'information sur des Canadiens à l'appui de ses opérations et de ses activités autorisées. Cette autorité provient de la mission ou du mandat légal qui a été approuvé à l'échelon du ministre, du Cabinet ou du premier ministre, et qui est normalement le résultat de l'exercice de la prérogative de la Couronne. Le MDN/FAC a rajouté qu'en même temps, la directive fonctionnelle CANCIT ne restreint pas ou ne limite pas la capacité du MDN/FAC à mener des activités du renseignement de défense. Le MDN/FAC a cité l'article 273.6 de la *Loi sur la défense nationale* comme étant le fondement juridique pour fournir de l'assistance aux autres ministères et organismes¹⁰².

85. [*** Les paragraphes 85, 86 et 87 ont été revus pour supprimer de l'information préjudiciable ou privilégiée. Ils décrivent de l'information fourni au MDN/FAC. ***]***¹⁰³

- ***¹⁰⁴
- ***
- ***

¹⁰¹ Le terme « opérations » est défini à la section 3.8 de la directive fonctionnelle : « L'exécution de service, d'entraînement ou d'une mission administrative militaire; le processus d'exécuter des opérations de combat (ou des opérations pacifiques). » Cette définition est tirée de la Banque de terminologie de la Défense.

¹⁰² MDN/FAC, observations au CPSNR, 30 mai 2019

¹⁰³ MDN/FAC, *** 24 août 2018

¹⁰⁴ ***

- ***

86. ***

- ***
- ***
- ***

87. ***¹⁰⁵

L'orientation stratégique

88. La section sur l'orientation stratégique de la directive fonctionnelle CANCEIT fournit une orientation sur les diverses conditions générales et particulières relativement au renseignement sur les Canadiens qu'il faut satisfaire pendant la conduite des activités du renseignement de défense. À titre général, les commandants opérationnels qui autorisent les activités du renseignement de défense doivent coordonner ces activités avec le Chef du renseignement de la Défense afin d'évaluer le risque d'être en contact avec des Canadiens ou de l'information sur des Canadiens, dans le cadre de l'activité ou de la mission appuyée. Dans tous les cas, l'information sur les Canadiens doit avoir un lien direct et immédiat avec l'opération ou l'activité autorisée, et le caractère nécessaire de ce renseignement peut être démontré.

89. Bien que censée s'appliquer à la collecte intentionnelle ou accidentelle de renseignement sur les Canadiens¹⁰⁶, la directive fonctionnelle CANCEIT ne contient pas de disposition qui traite précisément de la collecte intentionnelle. Elle est cependant très claire sur ce qui est attendu dans le cas de renseignement recueilli accidentellement :

- La chaîne de commandement et le Bureau de la coordination de la diffusion et de la divulgation du Commandement du renseignement des Forces canadiennes doivent être avisés de la collecte, à moins de l'application d'un protocole de signalement particulier à l'activité de collecte;
- L'information doit être supprimée des bases de données du MDN/FAC dès la confirmation qu'elle ne peut pas être conservée à des fins de renseignement de défense pour appuyer les opérations ou les activités de défense autorisées, ou transmise légalement à un autre ministère ou organismes canadiens;
- Toutes les instances de collecte doivent être consignées;
- Les exercices d'instruction qui comportent des éléments du renseignement de défense doivent prévoir des plans d'atténuation pour la collecte accidentelle d'information sur des Canadiens.

¹⁰⁵ Conseiller juridique et avocat général adjoint du MDN/FAC (ministère de la Justice), observations au CPSNR, 30 mai 2019.

¹⁰⁶ MDN/FAC, observations au CPSNR, 30 mai 2019.

90. Finalement, la directive fonctionnelle CANCEIT stipule que l'information sur des Canadiens peut être communiquée à d'autres ministères ou organismes canadiens si la divulgation est autorisée par la loi, notamment la *Loi sur la communication d'information ayant trait à la sécurité du Canada*, selon le cas, et la *Charte canadienne des droits et libertés*. Même si la directive ne permet pas explicitement la communication aux entités étrangères, elle requiert la tenue de registres de la communication d'information sur des Canadiens à des entités nationales ou étrangères, et la suppression d'information communiquée des bases de données du MDN/FAC.

91. Le MDN/FAC a expliqué qu'avant la publication de la directive fonctionnelle CANCEIT en août 2018, il n'y avait pas d'exigence de consignation ou de tenue de registres pour les instances de communication de renseignement sur les Canadiens à d'autres ministères ou organismes canadiens ou étrangers. Selon la directive actuelle, toute communication proposée doit faire l'objet de consultation auprès de conseillers juridiques et stratégiques. Tous les agents du MDN/FAC responsables de la diffusion et de la divulgation de renseignement doivent se soumettre à une formation formelle et recevoir une accréditation en matière de politiques et de procédures de communication de renseignement. Seul le personnel du MDN/FAC qui a suivi cette formation et qui a été accrédité dans la base de données de formation du MDN/FAC est autorisé à communiquer des renseignements et de l'information aux ministères canadiens et aux entités étrangères. La manipulation de l'information sur les Canadiens est couverte par cette formation. En général, toute l'information sur le renseignement de défense porte une classification de sécurité claire et pertinente, des marques de contrôle et d'usage spécial, de même que des mises en garde sur la manipulation. Toutes les restrictions et les contrôles de communications sont clairement indiqués sur les documents¹⁰⁷.

¹⁰⁷ MDN/FAC, réponse à une demande d'information du CPSNR, 25 mars 2019.

Chapitre 5 : L'évaluation du Comité

92. Ce Rapport spécial sur la collecte, l'utilisation, la conservation et la communication d'information sur des Canadiens dans le contexte des activités du renseignement de défense du MDN/FAC a été déclenché par la publication de la directive fonctionnelle CANCIT le 31 août 2018, qui a été fourni au Comité le 26 octobre. Tel que stipulé dans le cadre de référence du Comité, ce Rapport spécial avait les objectifs suivants :

- Décrire les fondements juridiques et le cadre stratégique du MDN/FAC pour la collecte, l'utilisation, la conservation et la communication d'information sur les Canadiens;
- Décrire les circonstances dans lesquelles la collecte, l'utilisation, la conservation et la communication d'information sur des Canadiens sont autorisées, et dans quels buts, comparativement aux circonstances où ces activités sont interdites;
- Décrire de quelle manière le MDN/FAC fait le suivi de la collecte, de l'utilisation, de la conservation et de la communication d'information sur des citoyens canadiens et consigne cette information;
- Évaluer les cadres juridique, stratégique et administratif suivant lesquels la collecte, l'utilisation, la conservation et la communication d'information sur des Canadiens sont permises ou interdites.

93. Le rapport spécial a atteint les trois premiers objectifs ci-dessus :

- **Les fondements juridiques et le cadre stratégique du MDN/FAC** : en l'absence de dispositions claires sur le renseignement de défense dans les lois, le MDN/FAC mène ses activités du renseignement de défense largement en vertu de l'autorité juridique que lui confère la prérogative de la Couronne. Dans la pratique, quand le MDN/FAC doit composer avec la possibilité d'être en contact avec du renseignement sur des Canadiens, il dépend du fondement juridique prévu dans le *Integrated SIGINT Signals Intelligence Operations Model* pour ses activités SIGINT (voir les paragraphes 35 et 53) et de ses partenariats avec d'autres ministères ou organismes du gouvernement pour ses autres activités (telles que *** voir les paragraphes 18-21 et 69-79 respectivement) au moyen d'une demande d'assistance en vertu de l'article 273.6 de la *Loi sur la défense nationale*. Les activités du renseignement de défense du MDN/FAC sont également assujetties à plusieurs instruments stratégiques, surtout sous la forme de directives fonctionnelles, dont plusieurs comportent des directives sur la manipulation de l'information sur les Canadiens. La directive fonctionnelle CANCIT, censée s'appliquer à toutes les activités du renseignement de défense, est la dernière à voir le jour dans l'ensemble des politiques. (Chapitres 1–4)
- **Les circonstances dans lesquelles la manipulation de l'information sur des Canadiens est autorisée ou interdite** : La collecte intentionnelle d'information sur des Canadiens est actuellement uniquement autorisée dans le contexte du programme de contre-ingérence du MDN/FAC, et lorsque le MDN/FAC prête assistance à un autre ministère ou organisme en vertu de l'article 273.6 de la *Loi sur la défense nationale*. Dans tous les autres cas, le MDN/FAC adopte

une approche prudente. Le plus souvent, il choisit *** dans laquelle il a été en contact avec de l'information sur des Canadiens par accident. (Chapitres 3–4)

- **La consignation et le suivi de l'utilisation de l'information CANCIT** : Avant la publication de la directive fonctionnelle CANCIT, il n'y avait aucune exigence concernant le suivi de la manipulation de l'information sur des Canadiens. Étant donné le peu de données disponible, le Comité ne peut pas commenter cet aspect du Rapport spécial. (paragraphe 89-91)

94. Le Comité s'est ensuite penché sur les cadres juridique, stratégique et administratif selon lesquels la collecte, l'utilisation, la conservation et la communication d'information sur des Canadiens sont permises ou interdites. Le Comité a évalué trois aspects. Le premier a constitué l'élément déclencheur de ce Rapport spécial : le cadre stratégique actuel du MDN/FAC pour la manipulation de l'information sur des Canadiens. Le deuxième touchait la question de l'application extraterritoriale de la *Loi sur la protection des renseignements personnels*. Le troisième aspect portait sur la dépendance du MDN/FAC à la prérogative de la Couronne pour mener ses activités du renseignement de défense, particulièrement quand ces activités comportent la collecte de renseignement sur des Canadiens.

Le cadre stratégique du MDN/FAC relatif aux Canadiens

95. La directive fonctionnelle CANCIT a pour but premier [traduction] « d'assurer la clarté des contraintes juridiques et stratégiques entourant la collecte de renseignement sur les Canadiens dans la conduite des activités du renseignement de défense¹⁰⁸. » Pour les raisons qui suivent, le Comité estime que la directive fonctionnelle CANCIT n'atteint pas ce but, et qu'elle n'est pas suffisamment claire à l'égard de sa portée et des fondements juridiques sur lesquels le MDN/FAC s'appuie pour la collecte de renseignement sur les Canadiens dans la conduite d'activités du renseignement de défense.

96. En ce qui a trait à la portée, la directive fonctionnelle CANCIT a été rédigée au titre d'une directive générale à l'intention du MDN/FAC. Cette caractéristique est évidente dans tout le document :

- La directive s'applique à tous les officiers et aux militaires du rang des FAC et à tous les employés du MDN, et non seulement aux unités responsables des activités spécifiques du renseignement de défense;
- Le but de la directive fait référence aux activités du renseignement de défense de manière générale;
- Les définitions qui figurent dans la directive sont génériques et sont tirées de la nomenclature officielle du MDN/FAC (par exemple, renseignement de défense, information, renseignement, opérations)

97. Malgré les énoncés de la directive relative à sa portée et à son application, le MDN/FAC a cherché à limiter son application générale pendant le déroulement de l'examen. Le MDN/FAC a expliqué qu'en

¹⁰⁸ MDN/FAC, *Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information*, 31 août 2018.

pratique, les directives et les ordonnances qui régissent les autres domaines d'activités du renseignement de défense – tel que le renseignement d'origine électromagnétique (SIGINT) et le renseignement d'origine humaine (HUMINT) – continuent d'être en vigueur et doivent être lues en parallèle à la directive fonctionnelle CANCIT¹⁰⁹. Le MDN/FAC a aussi déclaré que l'exigence de mettre en place la directive fonctionnelle CANCIT découlait de questions liées à la manipulation de matériel et d'équipement capturés *** Or, la directive fonctionnelle CANCIT ne mentionne pas les domaines d'activités du renseignement SIGINT, HUMINT, CEM ou d'autres domaines, ni ne requiert pas de lire la directive en parallèle à d'autres directives fonctionnelles pertinentes. En bref, la directive fonctionnelle CANCIT ne définit pas les activités du renseignement de défense qu'elle vise, et ne précise pas les directives qui ont préséance dans la manipulation de l'information sur des Canadiens. Comme présenté au paragraphe 8, le Comité n'a pu vérifier les raisons pour lesquelles la directive fonctionnelle CANCIT était requise, étant donné l'orientation qui est fournie dans les autres directives fonctionnelles, ni établir les problèmes que cette directive était censée régler.

98. Le manque de clarté dans le cadre stratégique se manifeste aussi dans la caractérisation des autorisations juridiques du MDN/FAC. La directive fonctionnelle CANCIT stipule ce qui suit [traduction] :

Les opérations et les activités du MDN/FAC ne doivent pas comporter la collecte de renseignement sur les Canadiens aux fins du renseignement de défense, sauf lorsque :

- la collecte a lieu en appui à des opérations ou à des activités de défense autorisées;
- la collecte en appui à un autre ministère ou organisme est subordonnée aux autorités, au mandat et aux exigences, telles que prescrites par la loi, du ministère ou de l'organisme canadien qui reçoit l'appui pour recueillir l'information¹¹⁰.

99. Même si en apparence, la directive fonctionnelle CANCIT interdit la collecte d'information sur des Canadiens, le Comité est préoccupé par la première exception à cette interdiction, qui semble l'annuler dans sa totalité. À première vue, le langage utilisé dans la directive laisse fortement croire que le personnel du MDN/FAC est autorisé à recueillir de l'information sur les Canadiens dans tous les cas où des activités du renseignement de défense ont lieu en appui à des opérations autorisées. Tout comme d'autres parties de la directive fonctionnelle CANCIT, le propos renvoie à toutes les activités du renseignement de défense. La directive ne mentionne aucune activité du renseignement de défense, dont certaines, notamment les activités SIGINT, sont assorties d'interdictions juridiques explicites en matière de collecte intentionnelle de communications de Canadiens, y compris dans le contexte d'opérations autorisées. Plus encore, la définition que donne la directive fonctionnelle CANCIT du terme

¹⁰⁹ MDN/FAC, observations au CPSNR, 30 mai 2019.

¹¹⁰ MDN/FAC, *Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information*, 31 août 2018.

« opérations » comprend une grande gamme d'activités militaires, et laisse croire, de nouveau, que la collecte d'information sur des Canadiens est permise dans toutes les missions militaires.

100. Dans les dossiers qui ont été fournis au Comité dans le cadre de son examen de 2018 des activités du renseignement de défense et de ce Rapport spécial, en fait, il est clair que le MDN/FAC n'emploie pas la prérogative de la Couronne pour recueillir de l'information sur des Canadiens dans ses activités du renseignement de défense dans le contexte de ses opérations autorisées¹¹¹. Le Comité est préoccupé cependant par l'ambiguïté dans les directives et les politiques du MDN/FAC sur ses autorisations à mener ces activités. En résumé, il faudrait clairement énoncer l'orientation sur les autorisations légales de mener des activités du renseignement de défense, particulièrement lorsqu'elles peuvent mettre en cause de l'information sur des Canadiens.

101. Le Comité estime que les fondements juridiques pour le deuxième type de collecte, en appui à un autre ministère et subordonné à ses autorisations, ont une plus grande clarté. Le MDN/FAC a mentionné qu'un tel appui est fourni en vertu de l'article 273.6 de la *Loi sur la défense nationale*. Puisque qu'il avait pris connaissance de la demande [***d'une autre organisation gouvernementale au MDN/FAC ***], le Comité est satisfait que des mécanismes appropriés sont en place pour obtenir les autorisations nécessaires.

102. Toutefois, le Comité revient sur un thème qu'il a soulevé dans son Rapport annuel 2018 : les limites importantes qui sont établies pour les activités de renseignement, mais qui figurent dans les documents stratégiques plutôt que dans des lois¹¹². L'exigence dans la directive fonctionnelle CANSIT (et similairement, dans la directive ministérielle sur le renseignement de défense) que l'appui en matière de renseignement de défense à un autre ministère soit assujéti aux autorisations légales du ministère qui en fait la demande est une restriction auto-imposée par le MDN/FAC. L'article 273.6 de la *Loi sur la défense nationale* prévoit que « Le gouverneur en conseil ou le ministre [de la Défense nationale] peut autoriser les Forces canadiennes [sur demande du ministre de la Sécurité publique et de la Protection civile ou d'un autre ministre] à accomplir des tâches de service public. » Le terme « service public » n'est pas défini, et il n'existe pas de restrictions sur les activités que peut mener le MDN/FAC. À l'opposé, l'autorité du Centre de la sécurité des télécommunications (CST) de fournir de l'assistance est limitée, au moyen d'un énoncé clair dans la loi, aux pouvoirs du ministère ou de l'organisme qui reçoit l'aide¹¹³. Le Comité ne comprend pas pourquoi des limites pour ce genre d'aide se trouvent dans les politiques pour une organisation et dans les lois pour une autre; la clarté juridique devrait exister pour les deux.

¹¹¹ L'examen de 2018 a démontré que plusieurs activités du renseignement de défense comportent des restrictions ou des interdictions claires à l'égard de telles activités, surtout concernant les activités de renseignement d'origine électromagnétique (SIGINT) ou d'origine humaine (HUMINT). Voir CPSNR, *Rapport annuel 2018*, paragraphes 180 et 181, www.nsicop-cpsnr.ca/reports/rp-2019-04-09/2019-04-09_annual_report_2018_public_fr.pdf.

¹¹² CPSNR, *Rapport annuel 2018*, paragraphe 251.

¹¹³ *Loi sur la défense nationale*, 1985 L.R.C., chap. N-5, para. 273.64(3).

L'application extraterritoriale de la *Loi sur la protection des renseignements personnels*

103. Tout au long de cet examen, le Comité a pris conscience de deux problèmes particulièrement préoccupants relativement à la *Loi sur la protection des renseignements personnels*. Le premier problème concerne l'application inconstante de la *Loi sur la protection des renseignements personnels* par le MDN/FAC. Dans le domaine de la collecte du renseignement de défense au Canada, et plus précisément dans ses activités de contre-ingérence, le MDN/FAC applique cette loi à la communication de renseignement à d'autres ministères en ce qui a trait aux questions de sécurité du personnel, et à la tenue d'un fichier de renseignements personnels (voir le paragraphe 67). Dans l'ensemble, le MDN/FAC semble appliquer cette loi dans le contexte de la communication de renseignement à d'autres ministères. La directive fonctionnelle elle-même cite la *Loi sur la protection des renseignements personnels* comme document de référence, et précise que [traduction] « L'information CANSIT peut être communiquée à d'autres ministères et organismes du gouvernement du Canada si la divulgation est autorisée par la loi, y compris la *Loi sur la protection des renseignements personnels*. »

104. [*** Le paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée. Toutefois, dans le cadre de son examen, le Comité a conclu que le MDN/FAC est d'avis que la *Loi sur la protection des renseignements personnels* ne s'applique pas à ses opérations à l'étranger. Le Comité s'est penché sur une étude de cas qui faisait ressortir, selon le Comité, que le MDN/FAC mettait cette position en pratique. La *Loi sur la protection des renseignements personnels* est en vigueur depuis 1983 et ne comporte aucune exception quant à son application aux activités du MDN/FAC à l'extérieur du Canada. Le Comité croit que le ministre de la Défense devrait préciser la position du ministère et formule des recommandations à cet effet à la fin du présent rapport. ***]¹¹⁴ ***¹¹⁵

105. [***Le paragraphe a été revu pour supprimer de l'information préjudiciable ou privilégiée. Il décrit le deuxième problème connexe qu'il a soulevé.***]

106. Vu son mandat unique, le MDN/FAC dispose de deux conseillers juridiques : le juge-avocat général et le ministre de la Justice. Selon la *Loi sur la défense nationale*, le juge-avocat général est le conseiller juridique auprès du gouverneur général, du ministre de la Défense nationale, du ministre de la Défense nationale et des Forces armées canadiennes pour les questions relatives au droit et à la justice militaire, deux domaines d'expertise très spécialisée¹¹⁶. Le Parlement a enchâssé le mandat du juge-avocat général dans la *Loi sur la défense nationale* en 1998.

¹¹⁴ MDN/FAC, ***

¹¹⁵ Voir les exceptions et l'annexe de la *Loi sur la protection des renseignements personnels* : <https://laws-lois.justice.gc.ca/fra/Lois/P-21/TexteCompleet.html>.

¹¹⁶ *Loi sur la défense nationale*, 1985 L.R.C., chap. N-5, art. 9.1. Voir aussi la *Loi sur la défense nationale*, 1985 L.R.C., chap. N-5, art. 10.1, qui prévoit que pour une plus grande certitude, l'article 9.1 ne modifie en rien les attributions du ministre de la Justice et procureur général du Canada que lui confère la *Loi sur le ministère de la Justice*.

107. Pour sa part, le ministre de la Justice et procureur général est mandaté de fournir des conseils aux « chefs des divers ministères sur toutes les questions de droit qui concernent ceux-ci¹¹⁷. » La mission du ministère de la Justice est de :

- Seconder le ministre de la Justice dans la tâche d'assurer, au Canada, l'existence d'une société juste et respectueuse des lois, pourvue d'un système judiciaire efficace, équitable et accessible;
- Fournir des conseils et autres services juridiques de grande qualité au gouvernement ainsi qu'aux ministères ou organismes clients;
- Promouvoir le respect des droits et libertés, de la loi et de la Constitution¹¹⁸.

108. Le rôle du ministère de la Justice comprend d'aider « le gouvernement fédéral à élaborer des politiques, à rédiger des lois et à les réformer au besoin. » Ses responsabilités reflètent « le double rôle du ministre de la Justice, qui est également, de par la loi, le procureur général du Canada. En termes généraux, le Ministère s'occupe de l'administration de la justice, y compris des questions de politiques dans des domaines tels que la justice pénale, le droit de la famille, le droit de la personne et la justice applicable aux Autochtones; en sa qualité de procureur général, il est le premier conseiller juridique de la Couronne chargé de diriger tous les procès au nom du gouvernement fédéral¹¹⁹. » En bref, le ministère de la Justice constitue le « cabinet juridique » du gouvernement sur les grandes questions de droit et la Constitution.

109. En parallèle à la décision d'accorder au juge-avocat général un fondement statutaire en 1998, le ministère de la Justice a créé la fonction de conseiller juridique du MDN/FAC, chargé de fournir des avis juridiques sur des questions qui relevaient précédemment de la compétence du juge-avocat général. En principe, le juge-avocat général fournit des avis au ministère de la Défense nationale, aux Forces armées canadiennes et au ministre de la Défense nationale sur des domaines spécialisés du droit et des opérations militaires, et le ministère de la Justice fournit des avis sur les questions plus larges de droit et la Constitution. Dans les domaines qui se chevauchent, les deux organisations travaillèrent ensemble pour dégager des principes communs et fournir un avis cohérent. Or, bien que cette méthode puisse générer des conflits en pratique¹²⁰, il est à l'avantage du MDN/FAC de recevoir des avis juridiques de la part d'organisations qui ont une expertise dans le domaine de droit pertinent. Il est raisonnable, semble-t-il, par exemple, que l'avis juridique du juge-avocat général ait préséance dans les questions liées au droit des conflits armés, aussi connu sous le titre du droit humanitaire international. Toutefois, lorsque les activités du MDN/FAC entraînent des questions de droit public plus générales susceptibles d'être également soulevées par d'autres organismes dans des contextes différents (par exemple, les

¹¹⁷ *Loi sur le ministère de la Justice*, 1985 L.R.C., chap. J-2, para. 5(b)

¹¹⁸ Ministère de la Justice, « Notre mission », www.justice.gc.ca/fra/pr-rp/pm-cp/aprop-about/index.html.

¹¹⁹ Ministère de la Justice « Notre rôle », www.justice.gc.ca/fra/pr-rp/pm-cp/aprop-about/index.html.

¹²⁰ Dès 1999, un schisme « est devenu apparent entre le MDN et le juge-avocat général concernant la prestation de services juridiques. » En effet « À quelques reprises [...] les deux cabinets ont offert des avis juridiques divergents à propos d'une même affaire, la plupart du temps, à leur insu. » Le juge-avocat d'alors a noté que « pareilles conclusions malencontreuses sont difficiles à éviter quand les conseils prodigués aux responsables d'une institution gouvernementales proviennent de deux sources différentes, une source interne, mais indépendante, et une source extérieure. » Cabinet du JAG, *Rapport du JAG (1998-99)*, 4 août 1999, www.Lareau-law.ca/Pitzul88-89.pdf.

activités consulaires d’Affaires mondiales Canada, des demandes de visas faites par des agents de l’immigration à l’extérieur du Canada), la nécessité pour les avocats du gouvernement de parler d’une même voix s’accroît.

110. [***Le paragraphe a été revu pour supprimer de l’information préjudiciable ou privilégiée. Il aborde l’évaluation par le Comité du rôle du ministère de la Justice.***]

La collecte de renseignements sur les Canadiens

111. Dans de récentes missions, le MDN/FAC a obtenu de l'information sur des Canadiens qui pouvaient être membres de groupes extrémistes armés, tels que Daech. Tout comme des citoyens de nos alliés les plus proches, des Canadiens se rendent dans des zones de conflits pour faire la promotion de leurs objectifs par des moyens violents. [*** Les deux phrases suivantes ont été revues pour supprimer l'information préjudiciable ou privilégiée et en assurer la lisibilité. Elles indiquent que le MDN/FAC est au fait de tels incidents, y compris dans les endroits où le MDN/FAC a mené des opérations, et qu'un allié lui a demandé de fournir d'autres informations. Le MDN/FAC a obtenu des renseignements sur des Canadiens qui participent peut-être à des activités terroristes contre le Canada, sous l'autorité d'un autre ministère. ***] En soi, ces incidents sont isolés et peuvent renforcer l'argument du MDN/FAC selon lequel ses activités de renseignement de défense mettent rarement en cause des Canadiens. Néanmoins, ces cas soulèvent une importante question : le MDN/FAC devrait-il avoir une autorisation explicite pour recueillir, utiliser, conserver et diffuser des renseignements sur des Canadiens lorsqu'il est approprié de le faire, y compris dans des circonstances où l'utilisation d'une force létale contre la personne visée est envisagée?

Les interdictions dans les politiques du MDN/FAC relatives à la collecte intentionnelle de renseignements sur les Canadiens

112. Au-delà de la disposition dans la directive fonctionnelle CANCEIT selon laquelle la collecte de renseignements sur des Canadiens peut avoir lieu à l'appui des activités et des opérations autorisées en vertu de la prérogative de la Couronne, le MDN/FAC démontre un biais clair dans ses politiques contre la collecte de renseignements sur les Canadiens dans le contexte de ses activités de renseignement de défense.

- Le MDN/FAC réalise ses activités SIGINT en vertu des autorisations du CST, dont les activités sont assujetties à une interdiction légale générale de viser des Canadiens dans ses activités de renseignement¹²¹.
- Les activités du MDN/FAC en cours pour recueillir de l'information *** sur des Canadiens qui pourraient constituer une menace envers le Canada sont menées en vertu ***¹²²
- Le MDN/FAC a officialisé un processus selon lequel [***un autre ministère***] communique l'information qui pourrait intéresser le MDN/FAC ***.
- Le MDN/FAC a mis en place des politiques et des directives opérationnelles qui lui interdisent de mener des activités HUMINT au Canada, ou de viser des Canadiens dans ses activités HUMINT partout au monde¹²³.

¹²¹ La collecte de renseignement d'origine électromagnétique (SIGINT) par l'appareil canadien du renseignement est menée à la fois par le CST en vertu de la partie A de son mandat (renseignement étranger) et par le MDN/FAC dans le cadre de ses opérations déployées en vertu des autorisations qui lui sont déléguées par le CST ou de la prérogative de la Couronne. MDN/FAC, présentation au Secrétariat du CPSNR sur le « *Integrated SIGINT Operations Model* », 23 juillet 2018.

¹²² MDN/FAC, Ordre de mission du CEMD pour ***

- Le MDN/FAC a déclaré sans équivoque qu'il ne communique pas d'information sur des Canadiens aux alliés du Canada¹²⁴.

Selon ces règles, les voyageurs extrémistes canadiens qui peuvent être présents dans la zone d'opération du MDN/FAC ***

113. Ces restrictions stratégiques sont difficiles à réconcilier avec la réalité opérationnelle décrite au chapitre 1 de ce Rapport spécial. Le Comité reconnaît les aspects sensibles associés aux conséquences possibles d'une action militaire contre des Canadiens, même lorsque l'usage de la force n'est pas envisagé. Cependant, la menace que posent les voyageurs extrémistes canadiens requiert une réponse proportionnelle. Le Comité n'est pas convaincu que l'approche actuelle du MDN/FAC *** pour les activités du renseignement de défense qui mettent en cause des Canadiens, ou de l'information à leur sujet, constitue une réponse appropriée à la menace qu'ils représentent.

114. Le gouvernement envoie fréquemment des membres des FAC et des employés du MDN à l'étranger pour participer à des opérations internationales, le plus souvent dans le cadre d'une coalition de pays. Lorsque des Canadiens physiquement présents dans la zone d'opération posent une menace envers les forces de la coalition, il revient au Canada d'utiliser ses ressources du renseignement pour aider les forces de la coalition à comprendre la menace, [*** Le reste de cette phrase et les deux suivantes ont été revues pour supprimer l'information préjudiciable ou privilégiée. Les phrases décrivent les préoccupations du Comité quant à l'approche du MDN/FAC. ***]

115. [*** Le paragraphe a été revu pour supprimer l'information préjudiciable ou privilégiée et en assurer la lisibilité. En l'absence de fondement juridique clair, le MDN/FAC se tourne vers d'autres partenaires canadiens pour obtenir l'autorisation de mener des activités de renseignement. Dans certains cas, ce recours est parfaitement légitime : le Parlement a fourni des mécanismes légaux aux organisations de la sécurité et du renseignement afin d'appuyer les activités des autres ministères quand elles ont des capacités ou des pouvoirs uniques. Dans d'autres cas, ce recours n'est pas idéal. Le présent Rapport spécial a traité d'une situation lors de laquelle le MDN/FAC a obtenu de l'information contenant de l'information sur des Canadiens et n'était pas certain s'il pouvait posséder ou analyser les informations. La collaboration avec un autre ministère dans ces situations n'est pas toujours efficace, puisque ceux-ci pourraient ne pas comprendre les exigences relatives au renseignement ou aux opérations du MDN/FAC. Rien ne garantit que le ministère puisse détecter dans cette information des détails en rapport direct à une opération militaire ou communiquer cette information dans un format utile au contexte militaire. Finalement, le fait que le MDN/FAC dépende des autorisations juridiques des autres organisations peut entraîner des difficultés. Cette façon de fonctionner est incompatible avec la fluidité des opérations militaires, dans lesquelles la valeur des renseignements opérationnels diminue

¹²³ MDN/FAC, *Defence Intelligence Functional Directive: CF HUMINT Intelligence Interrogation Operations in International Operations*, 2014; *Defence Intelligence Functional Directive: Strategic Debriefing*, 2015; et *Concept of Operations titled Biometrics – [Operation] IMPACT*, 22 juillet 2015.

¹²⁴ MDN/FAC, réponse à une demande d'information du CPSNR, 25 mars 2019.

avec le temps (par exemple, l'emplacement physique d'une personne ou l'intervalle dans lequel un événement va se produire). ***] ***¹²⁵

116. Quand il est en contact avec des renseignements sur des Canadiens qui peuvent prendre part aux hostilités, le MDN/FAC ne devrait avoir aucun doute sur son autorité à obtenir ces renseignements, à déterminer leur pertinence, et à les communiquer aux autres organisations gouvernementales ou, s'il y a lieu, aux pays alliés.

La prérogative de la Couronne

117. Comme noté, la directive fonctionnelle CANCIT comprend la mention que la collecte de l'information sur des Canadiens peut avoir lieu à l'appui des opérations et des activités autorisées par la prérogative de la Couronne. En effet, le MDN/FAC dépend de la prérogative de la Couronne pour toutes ses activités du renseignement de défense, sauf quand il agit en vertu des autorisations juridiques d'un autre ministère ou organisme. Pour le Comité, la question était de savoir, dans la pratique, quand la prérogative de la Couronne fournit une autorisation implicite au MDN/FAC pour qu'il mène ses activités du renseignement de défense dans le contexte d'une opération déployée, pourquoi n'a-t-elle pas aussi constitué un fondement juridique suffisant pour que le MDN/FAC puisse recueillir, utiliser, conserver et communiquer de l'information sur des Canadiens dans le même contexte? En d'autres mots, pourquoi le MDN/FAC ne vise-t-il pas des Canadiens dans ses activités de renseignement?

118. Il semble que la prérogative de la Couronne n'est pas suffisante à ces fins. Bien qu'elle fournisse certaines autorisations implicites pour les activités du renseignement de défense qui sont menées à l'appui de missions spécifiques du MDN/FAC, ces autorisations sont incertaines pour savoir si elles permettent la collecte, l'utilisation, la conservation et la communication d'information sur des Canadiens par le MDN/FAC. Par conséquent, le MDN/FAC recueille de l'information sur des Canadiens uniquement dans le cadre de son programme de contre-ingérence, en vertu des autorisations de la *Loi sur la gestion des finances publiques*, ou quand elle mène des activités selon les autorisations juridiques d'un autre ministère, en vertu de l'article 273.6 de la *Loi sur la défense nationale*¹²⁶. Pour les autres activités du renseignement de défense, le MDN/FAC dépend des autorisations juridiques des autres ministères ou organisme concernant la manipulation de l'information sur des Canadiens quand il est en contact avec cette information. Ces autorisations sont bien établies dans les lois et la jurisprudence, mais n'ont pas été conçues pour les besoins spécifiques des forces militaires.

¹²⁵ MDN/FAC. Lettre du CEMD et du sous-ministre de la Défense nationale ***

¹²⁶ Le Comité note que le terme « contre-ingérence » dans ce contexte devrait être compris pour inclure les activités du MDN/FAC ayant trait à sa position de sécurité interne dans le cadre de la Politique sur la sécurité du gouvernement, qui sont comparables aux activités des autres ministères et organismes du gouvernement du Canada. Le MDN/FAC n'a pas les pouvoirs, par exemple, d'intercepter les communications, et au lieu, dépend du SCRS, de la GRC et d'autres activités des forces de l'ordre pour mener des enquêtes à la suite d'une demande officielle d'assistance afin d'obtenir un mandat pour intercepter les communications.

119. L'application de la Charte aux activités du renseignement de défense est une autre source d'incertitude. Dans l'état actuel du droit, la Charte ne s'applique pas ordinairement à l'extérieur du territoire, et *** Cependant, à l'heure actuelle, la Cour suprême a comme position que la Charte peut s'appliquer dans certaines circonstances, surtout quand des acteurs étatiques canadiens enfreignent leurs obligations selon le droit international. À l'avenir, cette situation pourrait inclure les actions du MDN/FAC dans un pays étranger.

120. Si l'on venait à trouver que la Charte s'applique aux activités du renseignement de défense du MDN/FAC à l'extérieur du Canada, le Comité croit que l'argument selon lequel la prérogative de la Couronne offre un fondement juridique suffisant pour recueillir de l'information sur des Canadiens ne suffirait pas à convaincre. D'un point de vue légal, selon les faits, le Parlement et les gouvernements successifs croient, en ce qui a trait aux activités de renseignement du Canada, que des protections doivent être en place lorsque l'État recueille de l'information sur des Canadiens, même lorsque l'application de la Charte est incertaine. Cet état de fait est évident dans les deux principales organisations du renseignement du Canada : le CST et le SCRS.

121. Le régime juridique sous lequel le CST mène ses activités l'interdit de viser des Canadiens, même à l'extérieur du Canada¹²⁷. En reconnaissance du fait que les activités du CST comportent le risque de recueillir accidentellement de l'information sur des Canadiens, le régime demande à l'organisme de mettre en place des mesures pour protéger la vie privée des Canadiens dans l'utilisation et la conservation des communications interceptées¹²⁸. Ce régime a été récemment modifié par le Parlement pour lui ajouter un nouveau mécanisme de surveillance du CST, le commissaire sur le renseignement, dont le mandat sera d'examiner les conclusions à partir desquelles le ministre de la Défense nationale a autorisé le CST à mener une activité autorisée, et d'approuver l'autorisation si les conclusions du ministre sont raisonnables, y compris celles concernant les mesures pour protéger la vie privée des Canadiens¹²⁹. Des restrictions similaires sont en place pour les situations où il y a un risque d'interception de communications privées de Canadiens¹³⁰. Dans la même veine, le Parlement a récemment modifié la Loi sur le SCRS pour étendre la compétence d'un juge désigné de la Cour fédérale afin d'émettre un mandat autorisant le SCRS à prendre des mesures d'enquête à l'extérieur du Canada¹³¹. Même si cette modification avait pour but de régler des problèmes de compétences entourant certaines activités du SCRS, elle atténue également les risques dans certaines circonstances où un droit protégé par la Charte peut être enfreint, et dans lesquels il faut se munir d'un mandat.

122. En d'autres mots, dépendre de la prérogative de la Couronne comme source de fondement juridique pour recueillir, utiliser, conserver et communiquer de l'information sur des Canadiens n'est pas une option viable. Plutôt, le Comité réitère le raisonnement qu'il a donné dans son Rapport annuel

¹²⁷ *Loi sur la défense nationale*, L.R.C., 1985, chap. N-5, alinéa 273.64(2)(a).

¹²⁸ *Loi sur la défense nationale*, L.R.C., 1985, chap. N-5, alinéa. 273.64(2)(b).

¹²⁹ Le projet de loi C-59, *Loi concernant des questions de sécurité*, L.C. 2019, chap. 13, partie 2, sanctionnée le 21 juin 2019, et entrée en vigueur le 1^{er} août 2019.

¹³⁰ *Loi sur la défense nationale*, L.R.C., 1985, chap. N-5, art. 273.65.

¹³¹ *Loi protégeant Canada contre les terroristes*, L.C., 2015, chap. 9, art. 8.

2018, selon lequel le gouvernement devrait fournir des autorisations légales explicites pour la conduite des activités du renseignement de défense (voir le chapitre 4, Rapport annuel 2018, et plus particulièrement « Renseignement de défense : la question de législation », paragraphes 241-252). D'après cet examen, le Comité offre deux autres raisons pour accorder un fondement juridique au MDN/FAC pour mener ses activités du renseignement de défense.

123. Premièrement, l'approche actuelle à l'égard des activités du renseignement de défense, qui sont menées sous l'autorité de la prérogative de la Couronne et d'un ensemble de directives et d'autres instruments, suscite de l'incertitude. Dans les pires cas, le MDN/FAC ne sait pas s'il a l'autorité légale de faire des choses qui, du point de vue stratégique ou opérationnel, il devrait avoir le droit de faire. [*** Cette phrase a été revue pour supprimer l'information préjudiciable ou privilégiée. Cette phrase note que le Comité a félicité le MDN/FAC. ***] beaucoup d'énergie est dépensée pour les éclaircir. Les consultations internes et externes entreprises dans le feu de l'action pour éclaircir les incertitudes liées aux fondements juridiques peuvent contribuer à des retards dans les opérations, une situation qui peut porter atteinte à la sécurité des membres des FAC et aux intérêts nationaux du Canada. De plus, les solutions que peut employer le MDN/FAC peuvent être imparfaites ou tarabiscotées, dans lesquelles le MDN/FAC a recours aux autorisations d'autres ministères ou organismes. Bien que ces autorisations puissent fournir au MDN/FAC un refuge légal, elles viennent avec ***

124. Deuxièmement, les fondements juridiques flous suscitent des doutes dans un système démocratique régi par la primauté du droit. Le Parlement n'a jamais envisagé le travail du MDN/FAC dans le domaine du renseignement de défense, ni étudié les enjeux du renseignement de défense par rapport aux droits protégés par la Charte. Par conséquent, le renseignement de défense constitue une anomalie parmi les autres formes du renseignement du Canada. Bien qu'il soit vrai que la prérogative de la Couronne est la source d'une partie du fondement juridique, elle n'est pas une source transparente et démocratique. Les lois établies par le Parlement apportent crédibilité et acceptation sociale. Les pouvoirs étatiques qui n'ont jamais été précisés par une loi sont rares; plus ils sont invasifs, plus ils sont susceptibles, avec raison, d'attirer la controverse. Si l'on procède correctement pour inscrire le mandat du renseignement de défense du MDN/FAC dans une loi, nous pourrions régler les préoccupations et préserver la souplesse dont le MDN/FAC a besoin pour exécuter ses missions.

Conclusion

125. Le Comité a préparé ce Rapport spécial pour trois raisons. La première cherchait à réconcilier l'affirmation du MDN/FAC, selon laquelle il ne vise pas de Canadiens dans ses activités du renseignement de défense, avec la directive fonctionnelle CANCIT, qui, à la première lecture, laisse croire que le MDN/FAC fait le contraire. La deuxième raison consistait à comprendre le cadre juridique du MDN/FAC qui régit l'information sur des Canadiens, pour déterminer si les recommandations de 2018 du Comité devaient être modifiées. La troisième raison était de fournir une analyse de la question de savoir si le cadre juridique du MDN/FAC soulevait des risques opérationnels ou juridiques.

126. Sur les faits qui ont été présentés au Comité, il est clair qu'à l'heure actuelle, le MDN/FAC ne vise pas de Canadiens dans ses activités du renseignement de défense, à l'exception de circonstances bien précises, quand il détient l'autorisation claire de le faire (contre-ingérence) ou quand il prête assistance à d'autres organisations du gouvernement, en vertu de leurs autorisations (un cas étudié dans le présent examen). Cette clarté n'est pas traduite dans la directive fonctionnelle CANCIT. Elle reflète plutôt ce qu'affirme le MDN/FAC, qu'une décision du gouvernement en vertu de la prérogative de la Couronne peut lui fournir le fondement juridique nécessaire pour viser des Canadiens dans ses activités du renseignement de défense.

127. Le Comité ne croit pas que cette affirmation soit raisonnable. Le droit canadien comporte des protections substantielles contre les fouilles et saisies abusives, et des dispositions visant à protéger le droit à la vie privée de Canadiens. Ces protections reposent sur les lois qui s'appliquent à toutes les principales organisations de sécurité et de renseignement. Si le gouvernement du Canada décide d'autoriser le MDN/FAC à viser des Canadiens dans ses activités du renseignement de défense, le recours à la prérogative de la Couronne pourrait se révéler insuffisante comme source de fondement juridique. Dans son Rapport annuel 2018, le Comité a recommandé au gouvernement d'étudier sérieusement la question de fournir un fondement juridique explicite pour la conduite des activités du renseignement de défense du MDN/FAC. Pour les raisons expliquées dans le présent Rapport spécial, le Comité croit maintenant qu'il ne suffit plus simplement d'examiner cette question; plutôt, le gouvernement devrait fournir au MDN/FAC un fondement juridique clair pour mener ses activités du renseignement de défense dans le contexte de ses opérations déployées, notamment pour recueillir de l'information sur des Canadiens.

128. Le présent Rapport spécial a aussi cerné des risques juridiques et opérationnels qui, selon le Comité, devraient être éliminés. Le premier risque concerne la conclusion du Comité selon laquelle le MDN/FAC est d'avis que la *Loi sur la protection des renseignements personnels* ne s'applique pas à ses opérations à l'étranger, même si le ministère allègue qu'il applique l'esprit de la *Loi* *** Dans ce cas aussi, le Comité est d'opinion que la position du MDN/FAC est injustifiable, ***

129. Le deuxième risque est que le droit canadien pourrait ne pas être assez clair *** lorsque des Canadiens sont présents dans le théâtre des opérations. De tels cas sont peut-être rares, mais ils ont eu

lieu. Ils soulèvent alors d'importantes questions stratégiques, juridiques et opérationnelles. Le Comité croit que les Canadiens qui se rendent à l'étranger pour poursuivre leur objectif avec des moyens violents ne devraient pas être épargnés par les activités légitimes de renseignement des organisations de sécurité et de renseignement du Canada. Le Comité croit également que le gouvernement a la responsabilité d'aider à identifier ces personnes et à prendre les mesures nécessaires pour les neutraliser. Dans ce contexte, le personnel du renseignement du MDN/FAC doit connaître clairement son autorité d'acquérir, de recueillir, d'analyser et de communiquer de l'information sur des Canadiens, selon des limites juridiques claires et raisonnables, et dans le respect de la Charte, peu importe si elle s'applique à l'extérieur du Canada ou non.

Conclusions du Comité

130. Le Comité formule les conclusions suivantes :

- C1. Le cadre stratégique que le ministère de la Défense nationale/les Forces armées canadiennes (MDN/FAC) emploie pour la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens a besoin d'éclaircissements. (paragraphe 95-102)
- C2. Le MDN/FAC n'est pas entièrement conforme à la *Loi sur la protection des renseignements personnels* en ce qui concerne ses activités de renseignement qui ont lieu à l'extérieur du Canada, des activités auxquelles le Comité estime que cette loi s'applique. (paragraphe 103-104).
- C3. ***
- C4. La prérogative de la Couronne pourrait ne pas constituer un fondement juridique adéquat pour la conduite des activités de renseignement du MDN/FAC, en particulier lorsque du renseignement sur les Canadiens peut être en cause. (paragraphe 117-124)

Recommandations

131. Le Comité formule les recommandations suivantes :

- R1. Le ministère de la Défense nationale / les Forces armées canadiennes (MDN/FAC) abroge la *Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information* et, en consultation avec le commissaire à la protection de la vie privée, revoit toutes ses directives fonctionnelles et autres instruments stratégiques qui ont trait à la collecte, à l'utilisation, à la conservation et à la diffusion de renseignements sur les Canadiens pour assurer une gouvernance cohérente de ces activités.
- R2. Afin de régler la question de l'application extraterritoriale de la *Loi sur la protection des renseignements personnels*, le ministre de la Défense nationale doit veiller à ce que le MDN/FAC respecte la lettre et l'esprit de la *Loi sur la protection des renseignements personnels* dans toutes ses activités du renseignement de défense, au Canada et à l'étranger.
- R3. Le ministre de la Défense nationale présente un projet de loi régissant les activités du renseignement de défense du MDN/FAC, notamment pour déterminer dans quelle mesure le MDN/FAC est autorisé à recueillir, à utiliser, à conserver et à communiquer de l'information sur des Canadiens dans l'exécution de ses missions autorisées.

Annexe A – La directive fonctionnelle CANCEL

(Disponible uniquement en anglais)

UNCLASSIFIED

Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information

1.0 IDENTIFICATION

File Number: 2003-0

Effective Date: 31 August 2018

Supersedes: N/A

Office of Primary Responsibility: Director General Intelligence Policy and Partnerships (DGIPP)

Approval Authority: Chief of Defence Intelligence (CDI)

References:

- A. *Charter of Rights and Freedoms*
- B. *National Defence Act*
- C. *Privacy Act*
- D. *Citizenship Act*
- E. *Immigration and Refugee Protection Act*
- F. *Security of Information Sharing Act*
- G. *Treasury Board Directive on Privacy Practices*
- H. *Ministerial Directive on Defence Intelligence*, September 2013
- I. *Ministerial Directive on Defence Intelligence Priorities*, February 2017
- J. *Ministerial Directive on Avoiding Complicity in Mistreatment by Foreign Entities*, November 2017
- K. DAOD 1000-10, *Policy Framework for Corporate Administration Management*
- L. DAOD 1002-0, *Personal Information*
- M. DAOD 1002-3, *Management of Personal Information*
- N. *CDI Functional Directive: Intelligence and Intelligence-derived Information Sharing with External Entities*, June 2010

PURPOSE

1.1 The purpose of this directive is to:

- 1.1.1 Ensure clarity on the legal and policy constraints around the collection of Canadian citizen (CANCIT) information when conducting defence intelligence activities;

1/8

UNCLASSIFIED

UNCLASSIFIED

- 1.1.2 Provide guidance for instances where CANCEL information is inadvertently collected by the Department of National Defence (DND) and the Canadian Armed Forces (CAF) when conducting defence intelligence activities; and
- 1.1.3 Establish general parameters for the collection of CANCEL information for defence intelligence purposes in operational and training environments.

1.2 This functional directive does not deal with personal information management procedures or requirements relating to the collection of CANCEL information.

APPLICATION

1.3 This CDI directive is an order for all officers and non-commissioned members of the CAF and a directive for all employees of DND.

APPROVAL AUTHORITY

1.4 This Functional Directive is issued on the authority of the CDI, under the delegated authority of the Deputy Minister (DM) and the Chief of the Defence Staff (CDS) to issue functional direction in respect of defence intelligence matters in accordance with refs H (*Ministerial Directive on Defence Intelligence*) and K (DAOD 1000-10 *Policy Framework for Corporate Administration Management*).

OFFICE OF PRIMARY RESPONSIBILITY

1.5 DGIPP is the Office of Primary Responsibility for this directive, and all issues pertaining to the collection of CANCEL information when conducting defence intelligence missions and/or activities.

TABLE OF CONTENTS

1.6 This document contains the following subjects:

- 1.0. Identification**
- 2.0. Introduction**
- 3.0. Definitions**
- 4.0. Legal Authority**
- 5.0. Policy Direction**
- 6.0. Gender Perspectives**

UNCLASSIFIED

7.0. Information Management

8.0. Roles and Responsibilities

9.0. Approval

2.0. INTRODUCTION

2.1 Emerging technologies and capabilities are increasing the possibility that CANCEIT information may be inadvertently collected as part of mandated CAF missions and/or activities. The use of the Internet to conduct open source intelligence (OSINT) collection, for example, is a valuable intelligence enabler that may also raise privacy considerations in relation to the collection of social media information.

2.2 Technological developments have also changed the information flow related to intelligence sharing with allies and partners. Information movement is being facilitated through multinational interagency centres, enabling rapid sharing between points of collection to military and other government departments and agencies for further action. This construct increases the chance of DND/CAF inadvertently collecting CANCEIT information incidental to mission mandates and areas of operation.

3.0 DEFINITIONS

3.1 **Canadian citizen:** refers to a Canadian citizen within the meaning of s.3 of the *Citizenship Act* (R.S., 1985, c. C-29); or a permanent resident within the meaning of the s. 2(1) of the *Immigration and Refugee Protection Act* (2001, c.27).

3.2 **Collection:** the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate process unit for use in the production of intelligence (Defence Terminology Bank record number 3796).

3.3 **Defence intelligence:** all intelligence from the tactical to the strategic level in support of military operations and planning (Defence Terminology Bank record number 47286).

3.4 **Dissemination:** the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it (Defence Terminology Bank record number 4100).

3.5 **Exploitation:** the systematic retrieval and analysis of equipment, documents, and media (definition retained from the *CDI Functional Directive: Exploitation of Captured Equipment and Documents*).

3.6 **Information:** unprocessed data of every description which may be used in the production of intelligence (Defence Terminology Bank record number 18621).

3/8

UNCLASSIFIED

UNCLASSIFIED

3.7 **Intelligence:** the product resulting from the collection, processing, analysis, integration and interpretation of available information concerning foreign states, hostile or potentially hostile forces or elements, geography and social and cultural factors that contributes to the understanding of an actual or potential operating environment. The term “intelligence” also applies to the activities that result in the product and to the organizations engaged in such activities (Defence Terminology Bank record number 738).

3.8 **Operations:** the carrying out of service, training, or administrative military mission; the process of carrying out combat (or non-combat) military actions (Defence Terminology Bank record number 27068).

3.9 **Sanitizing:** Removing sensitive information from a document to reduce its sensitivity; or, erasing sensitive data from storage media (Defence Terminology Bank record number 12139 and 20963)

4.0 LEGAL AUTHORITY

4.1 The authority to conduct defence intelligence is implicit when the CAF is legally mandated to conduct military operations and other defence activities pursuant to legislation or an exercise of the Crown Prerogative, and where a clear nexus has been established between the nature and scope of the defence intelligence activity and the mandated mission. However, any means and methods used in the conduct of defence intelligence activities remain subject to applicable Canadian and international laws, as well as Government of Canada and Ministerial policies and directives.

4.2 DND/CAF operations and activities shall not involve the collection of CANCECIT information for defence intelligence purposes except where:

4.2.1 Collection occurs in support of mandated defence operations and activities; or

4.2.2 Collection, in support of another department or agency, is subject to the authority, mandate and requirements, as prescribed by law, of the supported Canadian department or agency to collect the information.

5.0 POLICY DIRECTION

General

5.1 DND and CAF personnel are tasked with employing intelligence capabilities as required to support mandated defence operations and activities. The paragraphs below provide direction on various conditions with respect to CANCECIT information that must be met while employing defence intelligence capabilities.

UNCLASSIFIED

5.2 Operational Commanders authorizing defence intelligence activities must coordinate planning with CDI to assess the risk of encountering CANCITs and/or CANCIT information as part of the activity and/or mission being supported.

5.3 CANCIT information collected must have a direct and immediate relationship with, and be demonstrably necessary to, an authorized operation or activity.

Inadvertent Collection

5.4 Where CANCIT information has been inadvertently collected as part of defence intelligence activities, the responsible J2, designated Release and Disclosure Authority (RDA), or force employing Command J2 will advise the chain of command and the Canadian Forces Intelligence Command (CFINTCOM) Release and Disclosure Coordination Office (RDCO), except where:

5.4.1 The collection activity has existing reporting protocols under a CDI Functional Directive or other CDI-issued direction.

5.5 CANCIT information collected inadvertently shall be deleted from DND/CAF databases once it is confirmed that the information cannot be held for defence intelligence purposes to support mandated defence operations and activities, or lawfully passed to another Canadian government department or agency. In addition:

5.5.1 Instances of inadvertently collected CANCIT information shall be logged. A copy of the log(s) shall be sent to the CFINTCOM RDCO upon completion of the relevant tour or activity, or at least once per year.

5.6 DND/CAF training exercises involving defence intelligence components must include mitigation plans for the inadvertent collection of CANCIT information, to be developed in consultation with CDI, and include the following general principles:

5.6.1 Commanders are responsible for ensuring that risks associated with defence intelligence collection for training purposes are assessed and mitigated prior to the commencement of exercises;

5.6.2 The deployed J2 or designated RDA is responsible for overseeing investigations into incidents of inadvertent collection of CANCIT information during training exercises, and reporting these incidents to CDI; and

5.6.3 The deployed J2 or designated RDA is responsible for assessing content collected during training exercises to determine the requirements for sanitization and/or deletion as appropriate.

Information Sharing

5.7 CANCIT information may be shared with other Canadian government departments and agencies if the disclosure is authorized by law, including the *Privacy Act*, the *Security of Information Sharing Act*, as the case may be, and the *Charter of Rights and Freedoms*.

5.8 Logs documenting all sharing of CANCIT information collected through defence intelligence activities to other domestic government departments and foreign entities must be maintained. A copy of the log(s) shall be sent to the CFINTCOM RDCO upon completion of the relevant tour or activity, or at least once per year.

5.9 Inadvertently collected CANCIT information that is shared with other Canadian government departments and agencies and foreign entities shall be managed in accordance with para 5.5.

6.0 GENDER PERSPECTIVES

6.1 In accordance with Treasury Board Secretariat requirements, this directive has been considered for its potential impact on various groups of women and men. There are no foreseen impact differentials based on gender.

7.0 INFORMATION MANAGEMENT

7.1 All applicable domestic laws and Government of Canada policies pertaining to information collection and management apply to the information holdings of all elements of the defence intelligence community.

7.2 Information management of personal information collected for defence intelligence purposes must comply with the *Privacy Act* where applicable. Appropriate care must also be taken to ensure that the collection, use, retention and disposal of personal information is conducted in accordance with the *Treasury Board Directive on Privacy Practices*; DAOD 1002-0 *Personal Information*; and DAOD 1002-3 *Management of Personal Information*.

8.0 ROLES AND RESPONSIBILITIES

8.1 The following table identifies the responsibilities and accountabilities associated with implementing this policy:

The...	is responsible and accountable for...
Chief of Defence Intelligence	<ul style="list-style-type: none">• Issuing functional direction on intelligence activities involving the collection, use, and sharing of CANCIT information that is lawful and policy compliant;

UNCLASSIFIED

	<ul style="list-style-type: none">• Reporting to the DM/CDS instances where CANCIT information is collected, as required, with recommended courses of action;• Exercising oversight of intelligence activities involving the potential collection, use and sharing of CANCIT information, including reporting on significant issues or concerns including in relation to compliance with functional direction;• Establishing processes for reporting the collection, use, and sharing of CANCIT information;• Establishing processes for sharing CANCIT information with other government departments and foreign partners; and• For domestic activities, consulting with the Directorate of Access to Information and Privacy to ensure that privacy concerns are identified, assessed and mitigated.
Assistant Deputy Minister (Policy)	<ul style="list-style-type: none">• Providing policy advice to ensure compliance with DND/CAF policies and formal agreements, applicable government and departmental policies and objectives; and• Providing policy advice on defence intelligence activities where there is the potential for collection, use, and sharing of CANCIT information.
DND/CF Legal Advisor	<ul style="list-style-type: none">• Providing legal advice to CDI on Government of Canada legal positions regarding the collection, use and sharing of CANCIT information; and• Liaising with the Judge Advocate General as required.
Judge Advocate General	<ul style="list-style-type: none">• Providing legal advice on defence intelligence activities where there is the potential for collection, use and sharing of CANCIT information;• Provide legal advice to Operational and Environmental Commanders on matters regarding defence intelligence activities; and• Liaising with DND/CF Legal Advisor as required.
Operational and Environmental	<ul style="list-style-type: none">• Ensuring intelligence activities comply with CDI-issued functional direction and applicable laws and policies, including on deployed operations;

UNCLASSIFIED

Commanders	<ul style="list-style-type: none">• Reporting instances of collection of CANCIT information to the CFINTCOM RDCO;• Establishing subordinate policies, doctrine, directives and concepts, subject to CDI review, of operations where the potential collection of CANCIT information is identified; and• Provide subject matter expertise assistance, analytical support and production advice as necessary;
------------	--

9.0 APPROVAL

9.1 This functional direction takes immediate effect and shall remain in effect until otherwise directed.



S.F.G. Bishop
Rear-Admiral
Chief of Defence Intelligence

August 2018

UNCLASSIFIED

Annexe B – Liste des témoins

Ministère de la Justice

- Conseiller juridique et avocat général adjoint, Conseiller juridique des Forces canadiennes

Ministère de la Défense nationale/Forces armées canadiennes

- Directeur général – Opérations, État-major interarmées stratégique
- Chef du renseignement de la défense adjoint, Commandement du renseignement des Forces canadiennes
- Juge-avocat général adjoint – Opérations
- Directeur exécutif, Secrétariat de la coordination de l'examen et de la surveillance de la sécurité nationale et du renseignement

Milieu universitaire

- Craig Forcese

