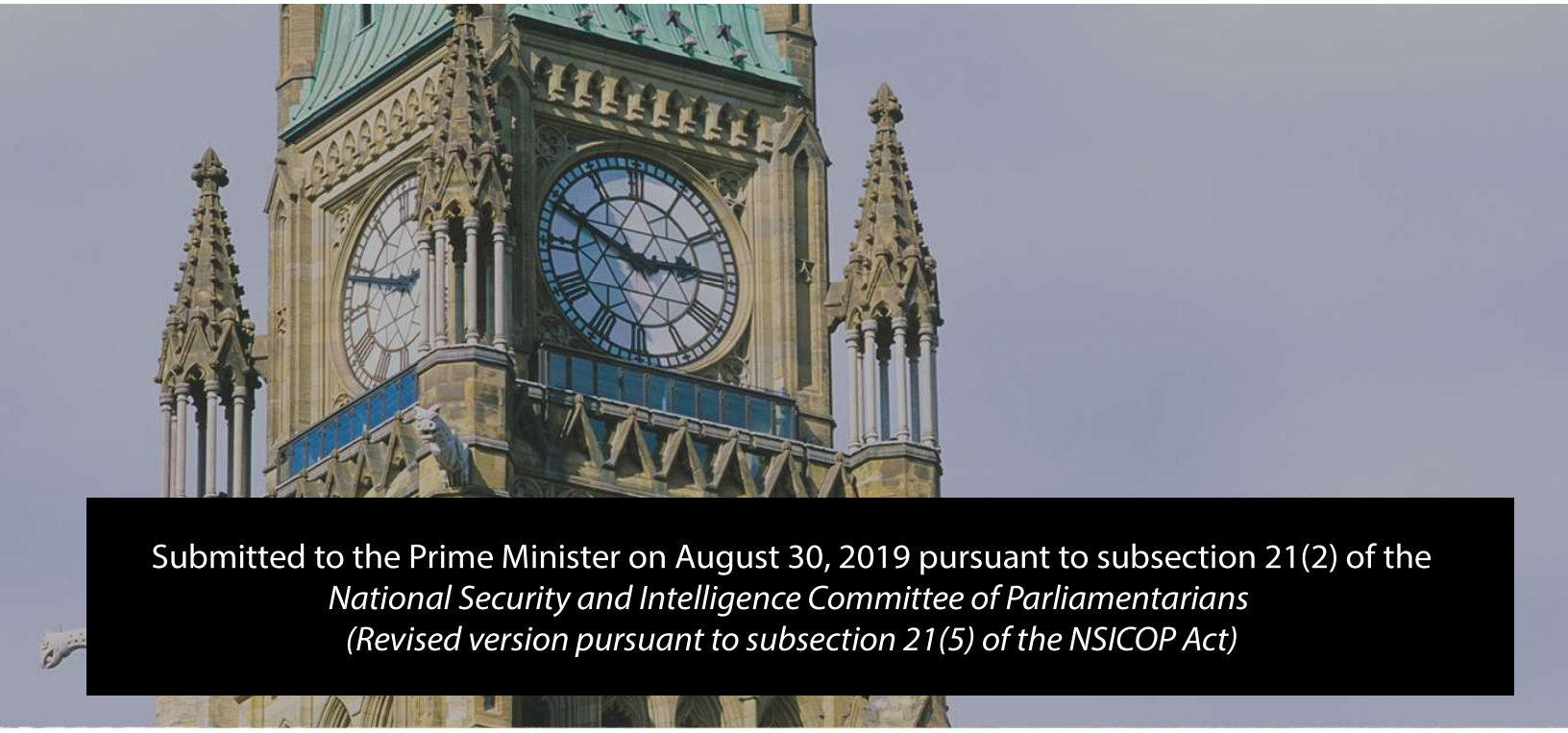
National Security and Intelligence Committee of Parliamentarians

Special Report on the Collection, Use, Retention and Dissemination of Information on Canadians in the context of the Department of National Defence and Canadian Armed Forces Defence Intelligence Activities



Submitted to the Prime Minister on August 30, 2019 pursuant to subsection 21(2) of the *National Security and Intelligence Committee of Parliamentarians*
(Revised version pursuant to subsection 21(5) of the NSICOP Act)

Canada

Ottawa, ON.

The National Security and Intelligence Committee of Parliamentarians

Special Report on the Collection, Use, Retention and Dissemination of Information on Canadians in the context of the Department of National Defence and Canadian Armed Forces Defence Intelligence Activities (Revised version pursuant to subsection 21(5) of the NSICOP Act)
CP104-2/2020E (Print)
ISBN 978-0-660-33057-0 (Print)

CP104-2/2020E-PDF
ISBN 978-0-660-33056-3 (Online)

Special Report on the Collection, Use, Retention and Dissemination of Information on Canadians in the Context of the Department of National Defence and Canadian Armed Forces Defence Intelligence Activities

The National Security and Intelligence Committee of Parliamentarians

The Honourable David McGuinty, P.C., M.P.
Chair

Submitted to the Prime Minister on August 30, 2019
Revised version tabled in Parliament in March 2020

Revisions

Consistent with subsection 21(2) of the National Security and Intelligence Committee of Parliamentarians Act (NSICOP Act), the Committee may submit a special report to the Prime Minister and the minister concerned on any matter related to its mandate. Consistent with subsection 21(5) of the NSICOP Act, the Prime Minister may, after consulting the Chair of the Committee, direct the Committee to submit to him or her a revised version of the special report that does not contain information the Prime Minister believes the disclosure of which would be injurious to national security, national defence or international relations or is information that is protected by solicitor-client privilege.

This document is a revised version of the Special Report provided to the Prime Minister on 30 August 2019. Revisions were made to remove information the disclosure of which the Prime Minister believes would be injurious to national security, national defence or international relations, or which constitutes solicitor-client privilege. Where information could simply be removed without affecting the readability of the document, the Committee noted the removal with three asterisks (***) in the text of this document. Where information could not simply be removed without affecting the readability of the document, the Committee revised the document to summarize the information that was removed. Those sections are marked with three asterisks at the beginning and the end of the summary, and the summary is enclosed by square brackets (see example below).

EXAMPLE: [*** Revised sections are marked with three asterisks at the beginning and the end of the sentence, and the summary is enclosed by square brackets. ***]

The Special Report includes the August 30, 2019 letter from the Chair of NSICOP to the Minister of National Defence. This letter was originally classified as SECRET//CEO as the attached report was classified at that time.

THE NATIONAL SECURITY AND INTELLIGENCE COMMITTEE OF PARLIAMENTARIANS

The Hon. David McGuinty, P.C., M.P. (Chair)

The Hon. Percy Downe, Senator

Mr. Emmanuel Dubourg, M.P.

The Hon. Diane Finley, P.C., M.P.

The Hon. Hedy Fry, P.C., M.P.

Ms. Gudie Hutchings, M.P.

The Hon. Frances Lankin, P.C., C.M., Senator

The Hon. Rob Nicholson, P.C., Q.C., M.P.

Mr. Murray Rankin, M.P.
(resigned August 1, 2019)

Ms. Brenda Shanahan, M.P.

The Hon. Vernon White, Senator

National Security and Intelligence Committee of Parliamentarians

Comité des parlementaires sur la sécurité nationale et le renseignement

Chair

Président

March 9, 2020

The Right Honourable Justin Trudeau, P.C., M.P.
Prime Minister of Canada
Office of the Prime Minister and Privy Council
Ottawa, ON
K1A 0A2

Dear Prime Minister,

On behalf of the National Security and Intelligence Committee of Parliamentarians, it is my pleasure to present you with our Special Report on the Collection, Use, Retention and Dissemination of Information on Canadians in the context of the Department of National Defence and Canadian Armed Forces Intelligence Activities. The unanimous Report includes four findings, one of which was entirely redacted, and three recommendations to clarify and improve the governance of this important and sensitive activity.

Consistent with subsection 21(5) of the *National Security and Intelligence Committee of Parliamentarians Act*, the Special Report was revised to remove information the disclosure of which would be injurious to national security, national defence or international relations, or is information subject to solicitor-client privilege.

Yours sincerely,

The Honourable David McGuinty, P.C., M.P.
Chair
National Security and Intelligence Committee of Parliamentarians

P.O. Box 8015, Station "T" / C.P. 8015, Succursale « T »
Ottawa, Canada K1G 5A6

National Security and Intelligence Committee of Parliamentarians

Chair

Comité des parlementaires sur la sécurité nationale et le renseignement

Président

SECRET//Canadian Eyes Only (with attachments)

August 30, 2019

The Honourable Harjit S. Sajjan, P.C., M.P.
Minister of National Defence
101 Colonel By Drive
Ottawa, Ontario
K1A 0K2

Dear Minister,

Pursuant to subsection 21(2) of the *National Security and Intelligence Committee of Parliamentarians Act*, I am pleased to submit to you the Committee's Special Report on the collection, use, retention and dissemination of information on Canadians by the Department of National Defence and Canadian Armed Forces in the conduct of defence intelligence activities. The Special Report includes four findings and three recommendations. A copy of this Special Report has also been provided to the Right Honourable Justin Trudeau, P.C., M.P., Prime Minister of Canada.

Please be advised that I have also written to the Attorney General, as required under section 31(1) of the *NSICOP Act*, to inform him of one of the Committee's findings regarding the Department of National Defence and Canadian Armed Forces' non-compliance with the *Privacy Act*.

Yours sincerely,

The Honourable David McGuinty, P.C., M.P.
Chair

Enclosure

P.O. Box 8015, Station "T" / C.P. 8015, Succursale « T »
Ottawa, Canada K1G 5A6

Table of Contents

Introduction **1**

Chapter 1: Operational Context **5**

Canadian citizens fighting abroad 5

Allied forces targeting Canadians 6

Deliberations by government officials 7

Overseas operation *** 8

Chapter 2: The Legal Framework **9**

Defence intelligence authorities 9

The Crown prerogative 9

Legal framework for defence intelligence activities conducted in Canada 10

Legal framework for defence intelligence activities conducted in international operations 11

Extraterritorial application of Canadian law 12

The *Criminal Code* 12

The *Privacy Act* 13

Canadian Charter of Rights and Freedoms 13

Chapter 3: Treatment of Information About Canadians Before the CANCIT Functional Directive **17**

Intelligence activities using the Internet 17

Signals intelligence 18

Human intelligence 19

Source handling and intelligence interrogation 19

Strategic debriefing 20

Biometrics 21

Counter-intelligence 21

Captured equipment and material / Captured equipment and documents 23

Sharing of CEM *** with DND/CAF and the CANCIT Functional Directive 24

Issues raised by the sharing of CEM with DND/CAF 25

Chapter 4: The CANCIT Functional Directive 27

Objectives and application of the CANCIT Functional Directive 27

Legal authority 27

Policy Direction 29

Chapter 5: The Committee's Assessment 31

DND/CAF policy framework on Canadian citizens 32

The extraterritorial application of the *Privacy Act* 34

Collection of information about Canadians 37

DND/CAF policy prohibitions on intentional collection of information about Canadians 37

The Crown prerogative 39

Conclusion 43

Findings 45

Recommendations 46

Annex A – The CANCIT Functional Directive 47

Annex B – List of Witnesses 57

Introduction

1. In 2018, the National Security and Intelligence Committee of Parliamentarians (the Committee or NSICOP) completed a review of the defence intelligence activities of the Department of National Defence and the Canadian Armed Forces (DND/CAF). The objective of that review was, in part, to improve Canadians' and Parliament's awareness and knowledge of the DND/CAF defence intelligence mandate and activities. It focused on the general authority framework and organizational structure of DND/CAF's defence intelligence program.[1] In the last stage of that review, DND/CAF provided the Committee with the Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information (CANCIT Functional Directive). The Committee determined that it did not have sufficient time to analyze the new directive for incorporation into its *Annual Report 2018*, but believed that it raised important issues that deserved further attention.

2. The Committee identified three reasons to conduct this review. First, the Committee wanted to reconcile the apparent contradiction between statements made by DND/CAF in 2018 and the purpose of the CANCIT Functional Directive. DND/CAF stated in briefings to NSICOP that it does not target Canadians in its defence intelligence activities.[2] Those statements appeared inconsistent with the title and content of the CANCIT Functional Directive. In short, on a plain reading, the CANCIT Functional Directive seemed to authorize DND/CAF to direct its defence intelligence activities at Canadians.

3. Second, the Committee wanted to understand the legal framework that governs the collection, use, retention and dissemination of information about Canadians by DND/CAF. As reported in the Committee's *Annual Report 2018*, the authority to use what DND/CAF describes as the full spectrum of defence intelligence activities comes through the *National Defence Act* (assistance to a government organization) or an exercise of the Crown prerogative. Activities conducted under the Crown prerogative are not authorized by an Act of Parliament. In contrast, all other Canadian intelligence agencies operate under a specific statutory regime that is tailored to their respective mandate, particularly where information about Canadians is involved.[3] The Committee wanted to revisit its previous assessment of DND/CAF authority to determine whether any adjustment was necessary to the findings and recommendations outlined in Chapter 4 the Committee's *Annual Report 2018*.

4. Finally, the Committee wanted to assess whether the legal and policy framework underpinning DND/CAF collection, use, retention and dissemination of information about Canadians gave rise to particular legal and operational risks.

---

[1] National Security and Intelligence Committee of Parliamentarians (NSICOP), *Annual Report 2018*.
[2] Department of National Defence and the Canadian Armed Forces (DND/CAF), statements to NSICOP Secretariat, November 1, 2018; DND/CAF, Comments to the Committee, December 4, 2018.
[3] See for example the sections 12 and 21 of the *Canadian Security Intelligence Act*, and Part V.1 of the *National Defence Act* (Communications Security Establishment). At the time of the submission of this report, Part V.1 of the *National Defence Act* had been repealed and replaced by the *Communications Security Establishment Act*, which came into force August 1, 2019. For clarity, this report refers to the authority structure under Part V.1 of the *National Defence Act*, which was in force during the period under review.

5. The terms of reference for the review stated four specific objectives:

- describe the DND/CAF authority and policy framework for the collection, use, retention and dissemination of information on Canadians;
- describe the circumstances in which, and purposes for which, the collection, use, retention and dissemination of information on Canadian citizens is permitted, versus those in which it is prohibited;
- describe the manner in which DND/CAF tracks and documents its collection, use, retention and dissemination of information on Canadian citizens; and
- assess the legal, policy and administrative frameworks under which the collection, use, retention and dissemination of information on Canadian citizens is permitted or prohibited.

6. On December 6, 2018, the Committee informed the Minister of National Defence of its decision to prepare a Special Report, under sub-section 21(2) of the *NSICOP Act*, of the collection, use, retention and dissemination of information on Canadians in the context of DND/CAF defence intelligence activities. On the same day, the Committee provided the Minister of National Defence with the terms of reference for this Special Report.

7. Between December 6, 2018, and August 23, 2019, the Committee reviewed the material received from DND/CAF (both classified and unclassified) in the context of the 2018 review, and received over 950 pages of new information for this Special Report, including legal opinions, ministerial letters, ministerial directives, functional and operational directives and orders, briefing notes, presentations, and operational authorizations and directions. The Committee supplemented this material with separate academic and legal research. DND/CAF officials appeared before the Committee once, met with the Secretariat on seven separate occasions, and provided a number of written responses to Committee questions. The Committee also received information from other government departments. This included the Communications Security Establishment regarding its policies to protect the privacy of Canadians; the Department of Justice regarding *** and the Canadian Security Intelligence Service (CSIS) regarding *** The views of Office of the Privacy Commissioner were also sought on one of the recommendations.

8. This report contains four sections. The first is a description of the context in which DND/CAF encounters information about Canadians in the conduct of its operations. The second explains the legal framework for those operations, drawing in large part from the Committee's 2018 Annual Report. The third describes the most relevant sections of the CANCIT Functional Directive. The Committee then provides its assessment, findings and recommendations. During the course of this review, the Committee encountered some challenges with DND/CAF. For example:

- DND/CAF stated that there were no emails among officials responsible for developing the directive over the course of a year. The absence of these emails prevented the Committee from determining the rationale behind the directive.

- In some cases, DND/CAF provided summaries of key information and not original source documents, which would have allowed the Committee to make its own assessment of the facts at issue.
- DND/CAF did not proactively provide documents relevant to the review that the Committee later discovered had been released through access to information requests.

9. The Committee made its assessment, findings and recommendations based on the record before it.

Chapter 1: Operational Context

10. The CANCIT Functional Directive was created to address issues arising out of an increasingly complex environment, including that DND/CAF would encounter enemy combatants who are also Canadians.[4] To the extent that intelligence supports operations, it is no longer a mere possibility that DND/CAF will encounter information about Canadians as part of its intelligence activities; it is likely unavoidable.

Canadian citizens fighting abroad

11. Canadian citizens have travelled abroad to join various groups that seek to attain their objectives through violent means. Of relevance to this review, these Canadians become involved with those groups through means that include online platforms used by terrorists and violent extremists to conduct recruitment and targeted indoctrination activities, and to encourage followers to carry out violence.[5] The latest data indicate that approximately 190 extremist travellers (also known as foreign fighters) with a connection to Canada are currently abroad, including in locations such as Iraq, Syria, Turkey, Afghanistan, Pakistan, North Africa and the Middle East.[6] Media reporting in April 2019 stated that Canadian terrorists have possibly killed or injured more than 300 people in other countries since 2012, and that citizens of 19 countries were killed in attacks that may have involved Canadian perpetrators.[7] Examples include the following:

- In July 2012, Hassan El Hajj Hassan, an alleged member of Hezbollah from Vancouver, is believed to have played a key role in plotting a targeted bus bombing in Bulgaria, killing five passengers and the driver.[8]
- In January 2013, Ali Medlej and Xristos Xatsiroubas, two Canadians from London, Ontario, took part in the attack on the Amenas gas plant in Algeria, which resulted in over 60 deaths.[9]
- In April 2013, Mahad Ali Dhore, a Canadian member of al-Shabaab, participated in the attack against the Somali Supreme Court building, which resulted in 34 deaths.[10]

---

[4] The CANCIT Functional Directive defines "Canadian citizen" as a Canadian citizen within the meaning of section 3 of the *Citizenship Act*, R.S.C. 1985, c. C-29; or a permanent resident within the meaning of section 2 the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27. The term "Canadian" is used throughout this report.

[5] Public Safety Canada, *2018 Public Report on the Terrorist Threat to Canada*, undated.

[6] Public Safety Canada, *2018 Public Report on the Terrorist Threat to Canada*, undated.

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

[8] Public Safety Canada, *2014 Public Report on the Terrorist Threat to Canada*. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2014-pblc-rpr-trrrst-thrt/2014-pblc-rpr-trrrst-thrt-eng.pdf.

[9] Royal Canadian Mounted Police (RCMP), *Terrorism and Violent Extremism Awareness Guide*, June 2016. www.rcmp-grc.gc.ca/wam/media/1731/original/1cb81f63911f002d67b340c08591bd31.pdf.

[10] Public Safety Canada, *2014 Public Report on the Terrorist Threat to Canada*, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2014-pblc-rpr-trrrst-thrt/2014-pblc-rpr-trrrst-thrt-eng.pdf.

12. As part of its contributions to international security, Canada has deployed DND/CAF to areas known to have attracted extremist travellers. In one case, DND/CAF obtained information about Canadians in the execution of deployed missions, which resulted in legal and operational issues for deployed forces.[11] In another case, DND/CAF worked with ***[12] These cases are discussed below.

Allied forces targeting Canadians

13. A September 16, 2015, briefing note to the Chief of Defence Staff provided some details on the strategic issues associated with the targeting of enemy combatants who are also Canadian citizens. It stated:

> As Canada is engaged in an armed conflict with ISIS [Daesh] and associated armed groups, DND/CAF operations under Op IMPACT [Canada's participation in the Global Coalition against Daesh] include both direct support to, as well as participation in, strikes against target packages including enemy combatants.[13] On occasion, these target packages consist of specifically identified individuals, with nationalities in some cases known prior to engagement. The Coalition targeting process ensures that all individuals engaged under Op IMPACT are ultimately enemy combatants.[14] *** Having such a process and therefore being actively involved with nations engaged in *** operations **increases the ability to share information**, and offer options to [Government of Canada] partners *** While the nationality of targeted individuals is, in the context of the Law of Armed Conflict (LOAC), not an issue, **domestic Canadian policy, political, and legal concerns may emerge**.[15] (emphasis added)

14. [*** This paragraph was revised to remove injurious or privileged information and to ensure readability. The paragraph states that DND/CAF is aware of such instances, including in areas where DND/CAF has operated, and was asked by an ally to provide further information. ***][16] ***[17]

---

[11] For a detailed description of operational and legal issues associated with this matter, see Chapter 3 of this special report, at paragraphs 75 to 79.

[12] See the section of this special report on ***

[13] Operation IMPACT was formed in September 2014. Beyond the military campaign, the Global Coalition is committed to tracking Daesh's financing and economic infrastructure, preventing the flow of foreign terrorist fighters across borders, supporting stabilization and restoration of essential public service to areas liberated from Daesh, and countering the group's propaganda (https://theglobalcoalition.org/en). DND/CAF operates an all-source intelligence centre as part of this operation. It gathers information from a variety of sources, and is responsible for collecting, synthesizing and analyzing this information. The resulting intelligence is then used for operational planning to protect coalition forces and determine how to conduct coalition operations. www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-impact.html.

[14] For DND/CAF, "targeting" is the process of selecting and prioritizing targets and matching the appropriate response, taking into account operational requirements and capabilities.

[15] DND/CAF, OP IMPACT – Canadian Citizens and Targeting of ISIS Combatants, Briefing note for the Chief of Defence Staff (CDS), September 16, 2015. In the context of the Committee's 2018 review of defence intelligence activities, documents provided by DND/CAF further described DND/CAF's role in coalition targeting, also defining *** DND, *** December 23, 2016.

[16] ***

[17] DND/CAF, OP IMPACT – Canadian Citizens and Targeting of ISIS Combatants, Briefing note for the CDS, September 16, 2015.

15. [*** This paragraph was revised to remove injurious or privileged information and to ensure readability. The paragraph continues to describe the content of a briefing note to the Chief of Defence Staff, which made three recommendations. ***]

- ***
- ***
- ***[18]

Deliberations by government officials

16. The participation of Canadians in armed conflicts against DND/CAF has been considered within the Government of Canada, including DND/CAF. In 2015, the National Security and Intelligence Advisor to the Prime Minister held discussions with senior government officials on the legality of using lethal force against Canadians in the context of the campaign against Daesh. While DND/CAF has stated that defence intelligence activities "generally do not give rise to risks to the rights and freedoms of Canadians,"[19] notes prepared in advance of these discussions for the Associate Deputy Minister and the Senior Associate Deputy Minister of National Defence indicate that the sharing of intelligence with allied nations was raised in the context of the extremist travellers phenomenon.[20]

17. *** expressed concerns over the sharing, with DND/CAF, of intelligence on Canadians involved with Daesh. DND/CAF stated in an internal briefing note that for *** this was "presumably due to concerns about how DND/CAF, or allies to whom the DND/CAF may pass information, may use the information for targeting purposes."[21] DND/CAF raised the following key issues, stressing the need to come to a common understanding in relation to the targeting of Canadians who participate in hostilities against Canada or allied nations:

- What is the applicable law?
- In cases where Canadians are identified as fighting for [Daesh], what conditions must be met for *** of the individuals involved?
- Where available intelligence on Canadians *** knowing that it will be used for targeting?

---

[18] DND/CAF, OP IMPACT – Canadian Citizens and Targeting of ISIS Combatants, Briefing note for the CDS, September 16, 2015.
[19] Murray Brewster, "A Parliamentary Committee is set to shine a light on the shadowy business of military intelligence," *CBC*, April 8, 2019; DND/CAF, Accountability Measures taken and considered with respect to the Defence Intelligence Function, Briefing note for the National Security Advisor to the Prime Minister, October 8, 2015.
[20] DND/CAF, Scenario Note for the Senior Associate Deputy Minister – 29 September Meeting on Canadian Citizens and targeting of ISIS Combatants; Scenario Note for the Senior Associate Deputy Minister – 9 October Meeting on Canadian Citizens and targeting of ISIS Combatants. Although the scenario notes are undated, DND/CAF confirmed that the notes were prepared in 2015.
[21] DND/CAF, Scenario Note for the Senior Associate Deputy Minister – 9 October Meeting on Canadian Citizens and targeting of ISIS Combatants. As noted in Footnote 14, "targeting" is the process of selecting and prioritizing targets and matching the appropriate response, taking into account operational requirements and capabilities. This can include a range of options, up to and including lethal targeting.

- Should a decision be made on any of these matters, what mechanism should be in place to guide the decision-making process?[22]

Overseas operation ***

18. [*** This paragraph has been revised to remove injurious or privileged information. It describes an overseas operation in which the collection of information about Canadians became an issue for Canadian authorities. ***][23] ***[24] ***[25]

19. [*** This paragraph was revised to remove injurious or privileged information and to ensure readability. The paragraph describes the objectives of DND/CAF's participation in a multinational operation, assessing that it represented a unique opportunity for Canada to better understand the scope of the threat posed by Canadian extremist travellers and violent extremist organizations to Canadian interests, both at home and abroad. ***] ***[26] ***[27]

20. [*** This paragraph was revised to remove injurious or privileged information and to ensure readability. The paragraph notes that the Committee received a contradictory record in regard to the DND/CAF authority to participate in this multinational operation, with DND/CAF asserting that it could do so under the Crown Prerogative and other documents which stated that DND/CAF could not do so under its own authorities. ***] ***[28] ***[29]

21. [*** This paragraph was revised to remove injurious or privileged information and to ensure readability. The paragraph states that Canada decided that DND/CAF could participate under another authority. ***] ***[30] ***[31]

---

[22] DND/CAF, Scenario Note for the Senior Associate Deputy Minister – 9 October Meeting on Canadian Citizens and targeting of ISIS Combatants.
[23] DND/CAF, CDS Tasking Order for ***
[24] DND/CAF, CDS Tasking Order for ***
[25] Letter from the ***.
[26] ***
[27] DND/CAF, Action Briefing Note for the MND ***
[28] DND/CAF, Answers provided to NSICOP questions related to *** in the course of the 2018 NSICOP review of DND/CAF defence intelligence activities.
[29] ***
[30] Letter ***
[31] Letter ***

Chapter 2: The Legal Framework

Defence intelligence authorities

22. The deployment of CAF members and DND employees, which includes the conduct of defence intelligence activities, is governed and constrained by Canadian and international law. In the context of the Committee's 2018 review of DND/CAF defence intelligence activities, the Judge Advocate General explained:

- All CAF operations are authorized by law.
- All CAF operations are conducted in accordance with the law.
- While the sources of legal authority may vary:
  - all domestic operations must have a legal basis in Canadian law, and be conducted in accordance with Canadian law; and
  - all international operations must have both a legal basis under Canadian law and a legal basis under international law, and must be conducted in accordance with both Canadian law and with the applicable international law.[32]

23. DND/CAF conducts defence intelligence activities under a unique and complex authority structure. The authority of DND/CAF to undertake the bulk of those activities is derived from exercises of the Crown prerogative, while other authorities can be found in domestic statutes. DND/CAF is also subject to a number of international legal instruments and binding customary international law, some of which may affect the conduct of defence intelligence activities. These activities are also subject to numerous policy instruments, including overarching government policies, ministerial directions and authorizations, internal policies and procedures, functional directives, and orders given through the military chain of command. The Committee's Annual Report 2018 described the authorities under which DND/CAF conducts its defence intelligence activities, and how those authorities support departmental and ministerial accountability for their use. The relevant portions of the Annual Report are summarized here for ease of reference.

The Crown prerogative

24. In addition to the authorities provided by the *Constitution Act, 1867* and the *National Defence Act*, the Crown prerogative is the main source of authority for the deployment of the CAF. It is also the source from which DND/CAF takes its authority to conduct associated defence intelligence activities. The Crown prerogative is a source of executive power and privilege accorded by the common law to the Crown, in circumstances in which the authority of the Crown is not otherwise limited.[33] British constitutional theorist A. V. Dicey described the Crown prerogative as the "residue of discretionary or

[32] DND/CAF, remarks of the Judge Advocate General to NSICOP, June 19, 2018.
[33] Peter W. Hogg, *Constitutional Law of Canada*, Looseleaf ed., *Thomson Carswell*, 1997.

arbitrary authority, which at any time is left in the hands of the Crown."[34] Put simply, the Crown prerogative is the authority exercised by the government to make decisions in areas where the "hands of the Crown" have not been tied by the Constitution, an act of Parliament or a court decision interpreting the scope of a governmental power.

25. In the most general terms, the authority to conduct defence intelligence activities is an accessory of the authority to deploy military forces. As DND/CAF stated, "[t]he authority to conduct defence intelligence activities is implicit when the DND/CAF is legally mandated, pursuant to legislation or an exercise of the Crown prerogative, to conduct military operations and other defence activities."[35] Neither the *National Defence Act* nor any other statute contains provisions that specifically govern the conduct of defence intelligence activities by DND/CAF in the context of the execution of its core mandate.

26. DND/CAF stated that the conduct of defence intelligence activities under the Crown prerogative is subject to the requirement for a "nexus," or a "reasonable connection," between defence intelligence activities and a defence mission, which is meant to serve as "a constraint on defence intelligence activities."[36] In 2013, DND/CAF formalized the requirement for a nexus in the Ministerial Directive on Defence Intelligence.

Legal framework for defence intelligence activities conducted in Canada

27. Defence intelligence activities may support DND/CAF domestic operations. These operations are authorized either by statute, or by an exercise of the Crown prerogative.

28. Where intelligence activities are used to support such domestic operations, their scope is circumscribed by law, by the specific responsibilities of various departments and agencies, and by the balance of jurisdiction between federal and provincial authorities. In terms of domestic legislation, DND identified several sources of law:[37]

- **The *National Defence Act*:** Section 273.6 of the Act permits DND/CAF to provide public service and assistance in law enforcement matters. Part VI of the Act defines when CAF can come to the Aid of the Civil Power (that is, to respond to riots or disturbances of the peace that cannot be handled without the assistance of DND/CAF).
- **The *Canadian Charter of Rights and Freedoms*:** DND/CAF intelligence activities must not violate the provisions of the Charter, particularly section 7 (the right to life, liberty and security of the person) and section 8 (the right to be secure against unreasonable search and seizure).

---

[34] *Reference as to the Effect of the Exercise of the Royal Prerogative of Mercy Upon Deportation Proceedings*, [1933] S.C.R. 269, at p. 272, per C. J. Duff, quoting A . V. Dicey, *Introduction to the Study of the Law of the Constitution*, 8th ed., *Macmillan and Co.*, 1915.
[35] DND, *** April 27, 2018.
[36] DND, Written submission to NSICOP, November 19, 2018.
[37] DND, *** April 27, 2018; Office of the Judge Advocate General, *The Law of Interrogations. The Issue of Torture and Ill-treatment*, Strategic Legal Paper Series, Issue 1, 2008; and DND, *** July 18, 2003.

- **The *Criminal Code*:** DND/CAF intelligence activities must not violate the *Criminal Code*, including sections dealing with the interception of private communications.
- **The *Access to Information Act* and *Privacy Act*:** DND/CAF intelligence activities and storage practices must comply with the provisions of the *Access to Information Act* and the *Privacy Act*.

29. In most cases, DND/CAF domestic operations are conducted in support of other government departments and agencies, and at the formal request of their minister. In such cases, these operations, including defence intelligence activities, are conducted pursuant to the legal authorities of the supported entity. As the Judge Advocate General stated, this means that "[w]hen acting in support of another organization, the Canadian Armed Forces have no more powers than those of the supported agency."[38] In short, DND/CAF can conduct an intelligence activity (for example, intercept communications) only to support another government department (for example, the Royal Canadian Mounted Police) if that department itself has the authority (for example, a court warrant) to conduct that activity.

Legal framework for defence intelligence activities conducted in international operations

30. Defence intelligence activities in support of DND/CAF international operations are mostly undertaken under the authority of the Crown prerogative. DND/CAF is also subject to instruments of international law that could involve defence intelligence activities, including the *United Nations Charter*, the *Geneva Conventions*, and other conventional or customary rules in the *Law of Armed Conflict*.

31. DND/CAF noted that the specific source of domestic or international law that may affect a defence intelligence activity varies depending on the circumstances of each case, including:

- the location of an operation;
- whether the operation is conducted at the invitation of a foreign state or under the auspices of a United Nations resolution;
- whether the operation is conducted in relation to a recognized international armed conflict, to which specific instruments of international law and international humanitarian law apply; and
- whether a particular activity is recognized as contrary to international law, including international humanitarian law.

[38] DND, Remarks of the Judge Advocate General, to NSICOP, June 19, 2018.

Extraterritorial application of Canadian law

32. Canadian law follows DND/CAF. However, it is not always clear whether a statute applies outside of Canada. This section contains examples of how Canadian law can apply extraterritorially. It also provides an example of a ***

The *Criminal Code*

33. Whether serving in Canada or deployed on operations abroad, CAF personnel are subject to the Code of Service Discipline, contained in Part III of the *National Defence Act*.[39] This Code also applies to DND personnel accompanying CAF on international missions. It extends the application of Canadian criminal law to foreign locations. This means that if CAF members (and DND employees, in certain cases) commit a criminal offence, they may be charged for a service offence in the Canadian military justice system.[40] The term "service offence" includes an offence under the *National Defence Act*, the *Criminal Code* or any other Act of Parliament, committed by a person while subject to the Code of Service Discipline.[41]

34. Some portions of the *Criminal Code* are directly relevant to defence intelligence activities. For example, signals intelligence (SIGINT) activities may carry a high risk of intercepting private communications, which constitutes a criminal act if the activity that resulted in the interception was done without judicial authorization (for example, a warrant). As the Code of Service Discipline extends the application of the *Criminal Code* to foreign territories, DND/CAF members who intercept communications originating from or destined for Canada could be subject to prosecution. While some offences do not apply to DND/CAF members,[42] there is no exception in the *Criminal Code* for interceptions occurring in the context of a lawfully authorized military mission.

35. Under Part V.1 of the *National Defence Act*, the Minister of National Defence could authorize CSE to intercept private communications if certain conditions prescribed in that Act were met.[43] Under such an authorization, Part VI of the *Criminal Code* did not apply in relation to an interception of a private communication.[44] This means that the interception of private communications under Part V.1 of the *National Defence Act*, when authorized by the Minister, was not a criminal offence. Where DND/CAF conducted SIGINT activities under the authority of CSE, DND/CAF personnel were subject to the Minister's authorizations, and were also exempted from the application of Part VI of the *Criminal Code* in that regard.[45] That said, DND/CAF also had to abide by the legislative obligations, policies and

---

[39] DND, Written submission to NSICOP, November 19, 2018.
[40] *National Defence Act*, s. 67.
[41] *National Defence Act*, s. 2.
[42] See for example section 117.08 of the *Criminal Code*, R.S.C., 1985, c. C-46.
[43] *National Defence Act*, s. 273.65(2).
[44] *National Defence Act*, s. 273.69.
[45] DND/CAF, Ministerial Directive on the Integrated SIGINT Operations Model.

procedures in place for CSE to protect the privacy of Canadians, including the absolute prohibition against directing their foreign intelligence SIGINT activities at Canadians or anyone in Canada.[46]

The *Privacy Act*

36. The *Privacy Act* is the statute that governs the personal information handling practices of federal government institutions, including DND/CAF.[47] The Act applies to all personal information that federal institutions collect, use and disclose. It also gives Canadians the right to access personal information held by these institutions.[48] For the most part, information collected as a result of intelligence activities, including defence intelligence activities, constitutes personal information within the meaning of the *Privacy Act*.[49]

37. There is no jurisprudence on whether the *Privacy Act* applies extraterritorially. [*** Paragraphs 37 to 40 have been revised to remove injurious or privileged information. Those paragraphs describe consultations among departments. ***] ***[50]

38. ***[51] ***[52]

39. ***

40. *** ***[53]

Canadian Charter of Rights and Freedoms

41. The Charter clearly applies to DND/CAF domestic intelligence activities.[54] It is unclear whether it applies to its extraterritorial defence intelligence activities. [*** The remainder of this paragraph was revised to remove injurious or privileged information. It discusses the extraterritorial application of the Charter. ***][55]

---

[46] *National Defence Act*, s. 273.64(2). At the time of the submission of this report, Part V.1 of the *National Defence Act* had been repealed and replaced by the *Communications Security Establishment Act*, which came into force August 1, 2019.
[47] *Privacy Act*, R.C.S., 1985, c. P-21.
[48] www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/.
[49] See the definition of "personal information," section 3 of the *Privacy Act*.
[50] ***
[51] *Privacy Regulations*, SOR/83-508.
[52] ***
[53] Remarks to NSICOP by the Deputy Legal Advisor and General Counsel, Department of National Defence and Canadian Forces Legal Advisor (Department of Justice), May 30, 2019.
[54] The "Charter applies to the Parliament of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon and Northwest Territories," *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11, para. 32(1)(*a*).
[55] DND/CAF, ***

42. Canadian law offers strong constitutional protections against government intrusions into the lives of Canadians. Should the Charter apply to the extraterritorial defence intelligence activities of DND/CAF, those activities would need to be compliant, for example, with section 8 of the Charter, which provides that "everyone has the right to be secure against unreasonable search and seizure." Generally, a search or a seizure will be reasonable if it is authorized by law (most often a statute), the law is reasonable, and the manner in which the search or seizure is carried out is also reasonable.[56] In most cases, this means that the state may not interfere with a reasonable expectation of privacy, unless the state's activity in question is authorized by a judge.

43. In the national security and intelligence context there are two statutes of relevance to this review (in addition to the *Criminal Code*, explained at paragraphs 33–35).[57] The first governs the activities of CSIS, the *CSIS Act*, which provides that CSIS, both inside and outside Canada, "shall collect, by investigation or otherwise, to the extent that is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada." The Director of CSIS may, if required in the context of such investigation, apply to a designated judge of the Federal Court for a warrant authorizing the Director of CSIS to use certain intrusive measures in the course of collecting information. The authorized activity may include the interception of the private communications of Canadians, or the seizure of devices that contain personal information. The designated judge may impose any condition deemed appropriate. Authorizations provided to CSIS by the Federal Court can apply to the information of or about Canadians who are inside or outside of Canada. Part VI of the *Criminal Code* (interception of private communications) does not apply to cases where the interception is authorized by the warrant.[58]

44. The second statute of relevance is Part V.1 of the *National Defence Act (Communications Security Establishment)*, which authorized a certain level of intrusion into the privacy of individuals. Among other things, Part V.1 of the Act gave CSE the mandate to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with the Government of Canada intelligence priorities.[59] It also prohibited CSE from directing its activities at Canadians located anywhere, or any person in Canada. These activities also had to be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information. Under the Act, the Minister of National Defence could authorize CSE to intercept private communications in the execution of its mandate, provided that the conditions set out in the Act were satisfied.

---

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

[57] There is no exception to the application of Part VI of the *Criminal Code* (interception of private communications) to DND/CAF in any context. By virtue of the Code of Service Discipline, Part VI applies to DND/CAF.

[58] *CSIS Act*, R.S.C., 1985, c. C-23, ss. 2, 12, 21, 21.1 and 26.

[59] In 2019, Bill C-59, An Act respecting national security matters, L.C. 2019, c. 13, Part 3, established the *CSE Act*, which provided CSE with the following mandate: 15(1) The Establishment is the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance. The Bill received Royal Assent on June 21, 2019, and came into force on August 1, 2019.

45. However, sources of lawful authority to interfere with Charter-protected rights are not necessarily limited to statutes. Canadian courts have recognized that in some limited cases, the common law may provide sufficient authority to justify a search or seizure.[60] Those cases have thus far been limited to the actions of law enforcement agencies. There is currently no jurisprudence suggesting the common law provides sufficient justification for the use of intrusive methods and techniques in the context of national security and intelligence activities, including defence intelligence activities.

[60] See for example *R. v. Caslake*, [1998] 1 S.C.R. 51.

Chapter 3: Treatment of Information About Canadians Before the CANCIT Functional Directive

46. DND/CAF stated that prior to the issuance of the CANCIT Functional Directive, "direction for handling [information about Canadians] was provided in discrete policies and directives related to specific intelligence disciplines and defence activities where there [is] a possibility that Canadian citizen information could be collected as part of a mandated DND/CAF operation or activity."[61] Of all the defence intelligence activities conducted by DND/CAF, five were considered the most relevant in the context of this special review with respect to the collection, use, retention or dissemination of information about Canadians. Explained in detail below, these are:

- intelligence activities using the Internet;
- signals intelligence (SIGINT);
- human intelligence (HUMINT);
- counter-intelligence; and
- captured equipment and material (as of April 1, 2019, known as captured equipment and documents).

Intelligence activities using the Internet

47. Intelligence activities using the Internet is defined by DND/CAF as "the use of Internet-based and Internet-enabled open source resources and platforms to discover, collect and leverage information for the purposes of generating or contributing to intelligence products."[62] The Chief of Defence Intelligence issued the Chief of Defence Intelligence Functional Directive: Framework for the Conduct of Intelligence Activities Using the Internet in February 2017. The directive stated that its purpose was to "enable the conduct of defence intelligence activities using the Internet by ensuring that such activity is consistent with Departmental mandate, and considers and mitigates the risk of *** [and stipulates] a standardized and consistent risk analysis process to ensure that appropriate authorities, technology and procedures are applied."[63]

48. The directive describes the authority basis for intelligence activities using the Internet as consistent with those for all other defence intelligence activities. In other words, the legal authority to conduct intelligence activities using the Internet is found in elements of the common law, specifically the Crown prerogative, in Canadian legislation (i.e., the *National Defence Act*) and in international law. It

[61] DND/CAF, Response to NSICOP request for information, March 25, 2019.
[62] DND/CAF, 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.

is derived from DND/CAF's authority to conduct mandated defence activities and operations approved by the Government of Canada.[64]

49. The directive includes key controls for DND/CAF's conduct of intelligence activities using the Internet, notably that:

- information cannot be collected solely on the basis that it is publicly available on the Internet – DND/CAF personnel, "acting as agents of the State [must ensure] that collection is lawful and consistent with their mandate;" and
- DND/CAF personnel shall not intentionally collect information on Canadians, except when authorized by a competent authority with a legal mandate to do so.

50. The directive does not explicitly prohibit the intentional collection of Canadian citizen information. Rather, the directive acknowledges in its description of the types of Internet-based activities and methods of acquiring information from the Internet that Canadian citizen information could be inadvertently or intentionally collected. The directive requires that DND/CAF personnel complete formal risk assessments to initiate an Internet-based intelligence operation, which must include assessments of whether DND/CAF personnel anticipate that personal information of Canadians would be intentionally or inadvertently collected. Where intentional collection is anticipated, DND/CAF personnel must demonstrate how that collection is permitted under the specific mandate of the mission in question.[65]

51. The directive also mentions the DND/CAF authority to provide Internet-based intelligence support to other federal departments and agencies, pursuant to section 273.6 of the *National Defence Act*. [*** The rest of this paragraph was revised to remove injurious or privileged information. This paragraph references an example of where DND/CAF provided such support to another government department. ***][66]

Signals intelligence

52. SIGINT is derived from the interception, collection, processing and analysis of communications and data links, including email, mobile and telephone communications. SIGINT also includes intelligence derived from electromagnetic emissions and instrumentation signals from things like radars and missile guidance and command systems.[67]

---

[64] DND/CAF, Chief of Defence Intelligence Functional Directive: Framework for the Conduct of Intelligence Activities Using the Internet.
[65] DND/CAF, Chief of Defence Intelligence Functional Directive: Framework for the Conduct of Intelligence Activities Using the Internet.
[66] DND/CAF, Response to NSICOP request for information, March 25, 2019.
[67] In the Canadian intelligence community, signals intelligence (SIGINT) collection is performed by both CSE under Part A of its mandate (foreign intelligence) and by DND/CAF as part of its deployed operations under delegated CSE authorities. DND/CAF, Information briefing to the NSICOP Secretariat on the "Integrated SIGINT Operations Model," July 23, 2018.

53. Prior to August 1, 2019, DND/CAF drew its authority to conduct SIGINT activities from the Crown prerogative, or through the statutory authority of the Communications Security Establishment (CSE), which was then found in Part V.1 of the *National Defence Act*.[68] For deployed operations, the Minister of National Defence had delegated the authority to conduct SIGINT activities from CSE to the CAF in accordance with the Ministerial Directive on the Integrated SIGINT Operations Model. This meant that DND/CAF SIGINT activities, conducted under CSE authorities, were subject to the same restrictions contained in Part V.1 of the *National Defence Act*, including the prohibition against directing intelligence activities at Canadians.[69] These activities were also subject to relevant ministerial authorizations, and were subject to review for lawfulness by the CSE Commissioner.[70] The prohibition against directing intelligence activities at Canadians was subject to one exception: when CSE provided technical and operational assistance to federal law enforcement and security agencies pursuant to subsection 273.64(1)(*c*) of the *National Defence Act*. CSE requests for assistance from DND/CAF would have been subject to the limitations imposed by law on the assisted agency or department (such as the RCMP or CSIS).[71]

Human intelligence

54. HUMINT is intelligence derived from the collection and analysis of information from human sources. HUMINT activities are conducted by specialized DND/CAF personnel. The DND/CAF HUMINT Policy Framework refers to several specialties in relation to the conduct of HUMINT activities including: source handling and intelligence interrogation, and the conduct of strategic debriefing.

Source handling and intelligence interrogation

55. Source handling operations are controlled HUMINT activities conducted by specialized units and include *** in order to collect and provide information. The Chief of Defence Intelligence Functional Directive: CF Policy Framework for the Conduct of HUMINT Activities governs source handling operations.

---

[68] At the time of the submission of this report, Part V.1 of the *National Defence Act* had been repealed and replaced by the *Communications Security Establishment Act*. For clarity, this report refers to the authority structure under Part V.1 of the *National Defence Act*, which was in force during the period under review.

[69] In the Canadian intelligence community, SIGINT collection is performed by both CSE under Part A of the CSE mandate (foreign intelligence) and by DND/CAF as part of its deployed operations under delegated CSE authorities. DND/CAF, Information briefing to the NSICOP Secretariat, "Integrated SIGINT Operations Model," July 23, 2018. CSE noted that the CAF also conducts SIGINT activities under CSE authorities that are not done directly in support of deployed operations (e.g., ***).

[70] Not every annual report from the Office of the CSE Commissioner covers the activities of the Canadian Forces Information Operations Group. CAF SIGINT activities are not, as a rule, all reviewed by the CSE Commissioner – they are, however, *subject* to review by the Commissioner. Communications Security Establishment. Written submission to NSICOP. October 1, 2018. Moreover, should DND/CAF conduct SIGINT activities under the Crown prerogative, DND/CAF would not be subject to the limitations provided in Part V.1 of the *National Defence Act* and would not be subject to review. CSE feedback on CANCIT draft report, July 21, 2019.

[71] DND/CAF, Statement of responses to NSICOP requests for information, March 25, 2019. For its part, CSE could not identify an instance where DND/CAF assisted CSE in the fulfillment of a request for assistance under section 273.64(1)(c) of the *National Defence Act*. CSE feedback on CANCIT draft report, 9 August 2019.

56. An intelligence interrogation is defined as the controlled, systematic and legally compliant process of using DND/CAF-approved approaches, strategies and ploys to question detainees taken into custody during the course of international operations to collect information to fulfill intelligence requirements. Intelligence interrogations are governed by the 2014 Defence Intelligence Functional Directive: CF HUMINT Intelligence Interrogation Operations in International Operations.

57. Neither source handling operations nor intelligence interrogations may be directed at nor otherwise involve a Canadian. If a Canadian is inadvertently involved in a source handling operation or if information is collected about a Canadian, the operation must be suspended and the incident brought to the attention of the operational commander. Similarly, an intelligence interrogation must be suspended if it is determined that the subject of the interrogation is a Canadian. The incident must be brought to the attention of the chain of command as soon as possible.

Strategic debriefing

58. DND/CAF defines debriefing as the voluntary questioning of individuals who may possess knowledge of defence intelligence interest to obtain usable information or confirm previously collected information in response to defence and military intelligence requirements. "Strategic debriefing" is defined as the voluntary questioning, through a deliberate and systematic process, of individuals who may possess information relevant to strategic and operational intelligence requirements. These activities are governed by the 2015 Defence Intelligence Functional Directive: Strategic Debriefing (Strategic Debriefing Functional Directive).

59. The Strategic Debriefing Functional Directive states that strategic debriefings may take place in Canada or abroad. It also identifies three groups of individuals who may possess information of intelligence value that would warrant the conduct of strategic debriefings:

- *** the Commander of Canadian Forces Intelligence Command must authorize these briefings;
- *** the Minister of National Defence and the Chief of Defence Staff must authorize these briefings on a case-by-case basis; and
- *** the Minister of National Defence and the Chief of Defence Staff must authorize these briefings on a case-by-case basis.

60. The Strategic Debriefing Functional Directive states that the legal authority to conduct this type of activity is derived, as are all defence intelligence activities, from Canadian legislation (i.e., the *National Defence Act*), international law and elements of the common law, specifically the Crown prerogative. Accordingly, any methods used in the conduct of strategic debriefing remain subject to applicable Canadian and international law, and government and ministerial policies and directives. This type of activity also requires the existence of a nexus between the nature and scope of the activity and a lawfully authorized defence operation or activity.

Biometrics

61. A DND/CAF order for Operation IMPACT prohibits the intentional collection of biometrics from Canadians and permits the collection of biometrics only from foreign nationals seeking entry into DND/CAF-controlled areas.[72] The order states that if biometric data about a Canadian is inadvertently collected, and the Canadian is deemed to pose a threat, the data shall be segregated from the rest of the data. DND/CAF personnel are then required to consult with the chain of command to determine whether the information could be shared with any Canadian government organization. If the Canadian whose data has been collected is not deemed to pose a threat, the data must be immediately deleted from all systems.

Counter-intelligence

62. DND/CAF defines counter-intelligence as those activities concerned with identifying and counteracting threats to the security of DND employees, DND/CAF members, and DND/CAF property and information; the threats are posed by hostile intelligence services, organizations or individuals, who are or may be engaged in espionage, sabotage, subversion, terrorist activities, organized crime or other criminal activities.[73] DND/CAF stated that counter-intelligence operations are one of two activity areas currently mandated and authorized to intentionally collect information about Canadians (the other being another intelligence activity) ***[74]

63. DND/CAF uses different authorities to conduct counter-intelligence activities. When deployed on operations, DND/CAF explained that the Canadian Forces National Counter-Intelligence Unit conducts counter-intelligence activities pursuant to a relevant exercise of the Crown prerogative.[75]

64. Domestically, DND/CAF stated that the authority to conduct counter-intelligence activities is found in the Policy on Government Security, which is issued by the Treasury Board of Canada Secretariat under the authority of section 7 of the *Financial Administration Act*. In application of the authority granted to deputy heads under this policy, the Vice Chief of Defence Staff issued the Defence Administrative Orders and Directives (the 8002 series) to meet the obligations of the Chief of Defence Staff and the Deputy Minister, as deputy heads, to manage security activities within DND/CAF.[76] The Chief of Defence Intelligence has also issued two functional directives on counter-intelligence investigations. Together, the functional directives and the 8002 Series established the framework for the National Counter-Intelligence Program and creates the Counter-Intelligence Oversight Committee. They

---

[72] DND/CAF, Biometrics – [Operation] IMPACT, Concept of Operations, July 22, 2015.
[73] DND/CAF, Defence Administrative Order and Directive (DAOD 8002-0), Counter-Intelligence, www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/8000-series/8002/8002-0-counter-intelligence.html.
[74] DND/CAF, Response to NSICOP request for information, March 25, 2019.
[75] DND/CAF, remarks to NSICOP, May 30, 2019.
[76] DND/CAF, Defence Administrative Order and Directive – DAOD 8002 – Table of Contents, www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/8000-series/8002.html.

also grant authority to the Canadian Forces National Counter-Intelligence Unit to collect, collate and assess counter-intelligence security threat information to provide security intelligence, security threat information and early warnings to DND/CAF senior managers and commanders.

65. DND/CAF explained that the Canadian Forces National Counter-Intelligence Unit obtains CANCIT information in the following circumstances:

- when identifying and monitoring threats to the security of DND/CAF;
- when conducting Security Intelligence Liaison Program activities as the office of primary concern for the collection of security intelligence;
- through approved access to information requests by the Canadian Forces National Counter-Intelligence Unit (identified as an investigative body in the *Privacy Act*);
- received from other government departments or agencies in accordance with *the Security of Canada Information Sharing Act*;[77] and
- via exchanges with the Financial Transactions and Reports Analysis Centre on financial information relating to personnel who are subjects of an active Canadian Forces National Counter-Intelligence Unit investigation, in accordance with section 55.1(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.[78]

66. DND/CAF stated that its recordkeeping system is not designed to produce statistics on the magnitude of the Canadian Forces National Counter-Intelligence Unit's collection, retention, use and dissemination of information about Canadians.[79] However, DND/CAF reported that between January 1 and March 14, 2019, the unit generated *** counter-intelligence reports, *** of which (80%) contained information about Canadians, and *** of which DND/CAF shared the contents of orally with Canadian security partners.

67. DND/CAF described this data sample as representative of the amount of CANCIT information the unit might collect or share with Canadian security partners in a given 10-week period. DND/CAF stated that information is shared with security partners for two reasons: first, to determine if partners have any adverse information concerning the persons of interest to the Canadian Forces National Counter-Intelligence Unit; and second, to determine if security partners have any information that indicated if a threat was posed by or to the individual. Counter-intelligence information, including information about Canadians, may be shared with domestic security partners in accordance with the *Security of Canada Information Sharing Act* and under subsection 8(2)(*a*) of the *Privacy Act*. Consistent with the *Privacy Act*,

---

[77] During the period under review, the *Security of Canada Information Sharing Act* (SCISA) was renamed the *Security of Canada Information Disclosure Act* (SCIDA), when *An Act respecting national security matters* (known as Bill C-59) received Royal Assent on June 21, 2019.

[78] DND/CAF, Response to NSICOP request for information, March 25, 2019.

[79] DND/CAF noted that it currently uses a Microsoft Access database to log records of its activities, stating that statistics must be manually generated from the database. The National Counter-Intelligence Unit has formally identified a need for new systems and sophisticated software to manage the information held by the unit. DND, Response to NSICOP request for information, March 25, 2019.

the Canadian Forces National Counter-Intelligence Unit maintains a personal information bank for the collection, retention and use of Canadian citizen information in support of its activities.[80]

68. Although DND/CAF stated that it does not share actual or potential information about Canadians with international partners, the department noted that it could legally disseminate it, "if the disclosure is authorized under the *Privacy Act*, in accordance with the Charter as the case may be, and in compliance with the Ministerial Directive on Avoiding Complicity in Mistreatment by Foreign Entities." Any proposed international sharing of information would undergo consultation with legal advisors and strategic policy advisors.[81]

Captured equipment and material / Captured equipment and documents

69. Until recently, captured equipment and material (CEM) was governed in Canada by the 2012 Chief of Defence Intelligence Functional Direction: *** (2012 CEM Functional Direction). In July *** DND/CAF directed that the functional direction be revised, due to "a defence intelligence policy gap with respect to intelligence sharing derived from analysis of CEM."[82] At the time, the Chief of Defence Intelligence issued the Interim Defence Intelligence Policy Guidance in Support of *** Among other things, the interim policy guidance stipulated that the *** will share intelligence with *** only if the Canadian department or agency from which the intelligence was derived deemed that intelligence releasable.[83] As of April 1, 2019, the 2012 CEM Functional Direction has been replaced by the Chief of Defence Intelligence Functional Directive: Exploitation of Captured Equipment and Documents (2019 CED Functional Directive).[84]

70. The terms CEM and CED both include documents, media or equipment recovered from a captured person, during a search of a location or, more generally, during the conduct of an operation. The exploitation of CEM is a standard intelligence activity among modern militaries, and provides decision-makers with intelligence concerning the capabilities and intentions of opposing forces. It may also provide intelligence for the planning and conduct of subsequent operations, targeting and the initiation of other intelligence collection activities.[85]

71. Both the 2012 CEM Functional Direction and the 2019 CED Functional Directive define exploitation as including the systematic retrieval and analysis of captured equipment, documents and media. Exploitation may involve the extraction and processing of information of a technical, tactical or

---

[80] DND MIS 085, Personal information bank.
[81] DND/CAF, Response to NSICOP request for information, March 25, 2019.
[82] Letter from the Chief of Defence Intelligence to the ***
[83] DND/CAF, Interim Defence Intelligence Policy Guidance in Support of ***
[84] The Chief of Defence Intelligence Functional Directive: Exploitation of Captured Equipment and Documents was approved on January 10, 2019, came into force on April 1, 2019, and was not disclosed to the Committee until July 19, 2019. This new functional directive does not materially change the Committee's factual analysis.
[85] DND/CAF, Chief of Defence Intelligence Functional Direction: *** November 21, 2012; and Chief of Defence Intelligence Functional Directive: Exploitation of Captured Equipment and Documents, April 1, 2019.

procedural nature, through the use of specific capabilities. Although the 2019 CED Functional Directive does not enumerate those capabilities, the 2012 CEM Functional Direction outlined that those could include ***[86]

72. The 2012 CEM Functional Direction was silent on how to handle information about Canadians. By contrast, the 2019 CED Functional Directive provides that "if collection, handling, disclosure, or release of Canadian citizen information occurs, [the CANCIT Functional Directive] applies."

Sharing of CEM *** with DND/CAF and the CANCIT Functional Directive

73. The absence of clear direction on the handling of information about Canadians *** was an important impetus for the development of the CANCIT Functional Directive. Generally, DND/CAF attributed the need for this directive to changes in the operational environment, explaining that the risk of inadvertently collecting information about Canadians had been increasing in recent years. DND/CAF cited three developments that increased that risk:

- emerging intelligence capabilities, including the increased conduct by DND/CAF of intelligence activities using the Internet;
- the rise of CEM recovered in the battlefield by both Canadian and coalition forces; and
- the challenge of an increasing number of Canadian citizens in DND/CAF areas of operation (e.g., extremist travellers).[87]

74. However, DND/CAF cited one specific *** event that triggered the development of the CANCIT Functional Directive. At some point in [*** The following two sentences were revised to remove injurious or privileged information and to ensure readability. The two sentences describe the event. ***] ***[88] In fact, DND/CAF noted that in the initial scoping of the policy requirements for the directive, some DND/CAF personnel believed that DND/CAF could not collect information about Canadians in any context. DND/CAF explained that this perception led intelligence personnel to request guidance *** on how to handle information about Canadians that was [*** related to the event ***].[89] DND/CAF stated that the department developed the CANCIT Functional Directive as proactive guidance to provide DND/CAF personnel with clear direction as to when the collection of information about Canadians was permitted. DND/CAF also wanted to outline the procedures on the reporting, logging and destruction of information about Canadians when it is detected or collected inadvertently.[90]

---

[86] DND/CAF, Chief of Defence Intelligence Functional Direction: *** November 21, 2012; and Chief of Defence Intelligence Functional Directive: Exploitation of Captured Equipment and Documents, April 1, 2019.
[87] DND/CAF, Response to NSICOP request for information, March 25, 2019.
[88] DND/CAF, *** Intelligence Sharing Update, Briefing note for the CDS [Chief of Defence Staff] and the Deputy Minister, December 22, ***
[89] DND/CAF, Response to NSICOP request for information, March 25, 2019.
[90] DND/CAF, Remarks to NSICOP, May 30, 2019.

Issues raised by the sharing of CEM with DND/CAF

75. The sharing of CEM *** with Canada raised immediate issues for DND/CAF regarding its ability to lawfully share information with other Canadian government organizations, and the suitability of the legal and policy framework underpinning the *** DND/CAF has stated that defence intelligence activities often involve highly perishable operational intelligence, meaning that its value diminishes with time.[91] In a briefing note to the Chief of Defence Staff and the Deputy Minister, DND/CAF officials stated that the information found *** should have been shared as quickly as possible with Canadian law enforcement and security agencies, but that sharing was delayed by the complexities of different domestic information sharing laws and policies. They described this situation as an example of broader challenges associated with the collection, handling, sharing and exploitation of CEM.[92]

76. The briefing note identified three overarching issues related to information sharing and the exploitation of this information within Canada:

- Differing mandates of partner agencies: CSIS, the RCMP and CSE have unique national security mandates. Each has different policies and requirements for receiving information from external entities.
- Sharing of large volumes of information: Existing intelligence-sharing instruments, such as the *Security of Canada Information Sharing [*now *Disclosure] Act,* were not created to deal with large volumes of information, or information the nature of which has not been previously reviewed to determine its content.
- *Privacy Act* requirements surrounding the exploitation of the information by DND/CAF in Canada: If the exploitation of the information *** occurs in Canada, *Privacy Act* requirements would need to be met.[93]

77. The issue of *Privacy Act* requirements is particularly important. [*** This paragraph was revised to remove injurious or privileged information and to ensure readability. The paragraph notes that DND/CAF was aware that once the intelligence was in Canada, *Privacy Act* obligations would be triggered and it would have to meet a number of obligations and put in place required infrastructure. These obligations included determining the scope of personal information that DND/CAF possessed, determining what personal information of Canadians existed, ensuring that the information was used only for the purpose for which it was obtained, and that measures were put in place to protect all personal information from unauthorized access. There was also a requirement under the *Privacy Act* to create a personal information bank to hold all personal information.[94] ***] ***[95]

---

[91] DND/CAF, Accountability Measures Taken and Considered with Respect to the Defence Intelligence Function, Briefing note for the National Security Advisor to the Prime Minister, October 8, 2015.
[92] DND/CAF, *** Intelligence Sharing Update, Briefing note for the CDS and the Deputy Minister, December 22, ***
[93] DND/CAF, *** Intelligence Sharing Update, Briefing note for the CDS and the Deputy Minister, December 22, ***
[94] See the *Privacy Act*, section 10(1).
[95] DND/CAF, ***

78. [*** Paragraphs 78 and 79 were revised to remove injurious or privileged information and to ensure readability. The two paragraphs detail how DND/CAF and another government department agreed to cooperate. ***][96]

79. ***[97]

[96] Letter from the CDS and the Deputy Minister to the ***
[97] Memorandum to the CDS and the Deputy Minister, ***

Chapter 4: The CANCIT Functional Directive

Objectives and application of the CANCIT Functional Directive

80. The CANCIT Functional Directive is an order for all officers and non-commissioned members of the CAF, and a directive for all employees of DND. The stated purpose of the CANCIT Functional Directive is to:

- ensure clarity on the legal and policy constraints for the collection of Canadian citizen information when conducting defence intelligence activities;
- provide guidance for instances where Canadian citizen information is inadvertently collected by DND/CAF when conducting defence intelligence activities; and
- establish general parameters for the collection of Canadian citizen information for defence intelligence purposes in operational and training environments.[98]

81. DND/CAF stated that the CANCIT Functional Directive is intended to apply to both the intentional and inadvertent collection of information about Canadians, occurring in the context of all DND/CAF intelligence operations and activities (inside and outside Canada), except those activities already governed by existing directives regarding the collection of information about Canadians.[99] Prior to the CANCIT Functional Directive, directions for handling information about Canadians were addressed in individual policies and directives related to specific intelligence activities, including signals intelligence, human intelligence and counter-intelligence, which are still in force (see Chapter 3). Accordingly, DND/CAF stated that the CANCIT Functional Directive does not apply to those specific activities. DND/CAF also stated that "the Directive is very clear. DND/CAF personnel may only deliberately collect information on Canadian citizens for intelligence purposes under two circumstances: one, in support of a mandated defence operation or activity – and currently this [authorization for deliberate collection] only applies to counter-intelligence operations; [and two], in support of another government department or agency, pursuant to an authorized request for assistance under section 273.6 of the *National Defence Act*."[100] Notwithstanding these statements, the CANCIT Functional Directive does not qualify or limit its application in reference to any directives for other intelligence activities, nor does it state that it applies only to those defence intelligence activities that do not have pre-existing guidance regarding the collection of CANCIT information.

Legal authority

82. The CANCIT Functional Directive states that the authority to conduct defence intelligence activities is implicit when DND/CAF is legally mandated to conduct military operations and other defence

---

[98] DND/CAF, Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information, August 31, 2018.
[99] DND/CAF, Remarks to NSICOP, May 30, 2019.
[100] DND/CAF, Remarks to NSICOP, May 30, 2019. In the second circumstance noted, currently only *** falls into this category.

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. This is subject to the caveat that any means used in the conduct of defence intelligence activities remain subject to applicable Canadian and international laws, and government policies and ministerial directives.

83. The CANCIT Functional Directive states that DND/CAF operations and activities shall not involve the collection of information about Canadians for defence intelligence purposes. This is subject to two exceptions:

- the collection occurs in support of mandated defence operations and activities;[101] or
- the collection occurs in support of another department or agency, subject to the authority, mandate and requirements, as prescribed by law, of the supported Canadian department or agency to collect the information.

84. DND/CAF explained that the CANCIT Functional Directive does not provide any new authority to collect information about Canadians in support of its mandated operations and activities. That authority comes from the lawful mandate or mission that is approved at the ministerial, Cabinet or prime ministerial level, which is normally the result of the exercise of prerogative powers. DND/CAF further stated that, at the same time, the CANCIT Functional Directive does not impede or limit the ability of DND/CAF to conduct defence intelligence activities. DND/CAF cited section 273.6 of the *National Defence Act* as the source of authority for providing assistance to other departments and agencies.[102]

85. [*** Paragraphs 85, 86 and 87 were revised to remove injurious or privileged information. They describe information provided to DND/CAF. ***] ***[103]

- ***[104]
- ***
- ***
- ***

86. ***

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

[101] The term "Operations" is defined in section 3.8 of the Functional Directive as "the carrying out of service, training, or administrative military mission; the process of carrying out combat (or non-combat) military actions." This definition comes from the Defence Terminology Bank.
[102] DND/CAF, Remarks to NSICOP, May 30, 2019.
[103] DND/CAF, *** August 24, 2018.
[104] ***

87. ***[105]

Policy Direction

88. The Policy Direction section of the CANCIT Functional Directive provides direction on the various general and specific conditions with respect to information about Canadians that must be met while conducting defence intelligence activities. Generally, operational commanders authorizing defence intelligence activities must coordinate with the Chief of Defence Intelligence to assess the risk of encountering Canadians, or information about Canadians, as part of the activity or mission being supported. In all cases, information about Canadians must have a direct and immediate relationship with, and be demonstrably necessary to, an authorized operation or activity.

89. Although intended to apply to both intentional and inadvertent collection of information about Canadians,[106] the CANCIT Functional Directive does not contain any provision dealing specifically with intentional collection. It is, however, very specific on what is expected to be done with inadvertently collected information:

- the chain of command and the Canadian Forces Intelligence Command Release and Disclosure Coordination Office must be notified of the collection, unless reporting protocols specific to the collection activity apply;
- the information must be deleted from DND/CAF databases once it is confirmed that it cannot be held for defence intelligence purposes to support mandated defence operations and activities, or lawfully passed to another Canadian government department or agency;
- all instances of collection must be logged; and
- training exercises involving defence intelligence components must include mitigation plans for the inadvertent collection of information about Canadians.

90. Finally, the CANCIT Functional Directive states that information about Canadians may be shared with other Canadian government departments and agencies if the disclosure is authorized by law, including the *Privacy Act*, the *Security of Canada Information Sharing Act*, as the case may be, and the Charter. Although the directive does not explicitly permit sharing with foreign entities, it does require that logs documenting the sharing of information about Canadians with both domestic and foreign entities be maintained and that shared information be deleted from DND/CAF databases.

91. DND/CAF explained that before the CANCIT Functional Directive was issued in August 2018, there was no requirement to document and provide logs detailing the instances of sharing information about Canadians with other domestic government departments and foreign entities. Under the current directive, any proposed sharing would undergo consultation with legal advisors and strategic policy

[105] DND Deputy Legal Advisor and General Counsel and Canadian Forces Legal Advisor (Department of Justice), Remarks to NSICOP, May 30, 2019.
[106] DND/CAF, Remarks to NSICOP, May 30, 2019.

advisors. All DND/CAF release and disclosure authorities and officers undergo formal training and accreditation on information sharing policies and procedures. Only those DND/CAF personnel who complete this training and have been accredited in the DND/CAF training system database are authorized to share intelligence and information with domestic departments and foreign entities. Handling information about Canadians is covered in that training. In general, all defence intelligence information contains clear and relevant security classifications, control markings and special use, as well as handling caveats. Any restrictions and sharing controls are clearly marked on documents.[107]

[107] DND/CAF, Response to NSICOP request for information, March 25, 2019.

Chapter 5: The Committee's Assessment

92. This Special Report on the collection, use, retention and dissemination of information on Canadians in the context of DND/CAF defence intelligence activities was triggered by the promulgation of the CANCIT Functional Directive on August 31, 2018, and its provision to the Committee on October 26. As stated in the Committee's terms of reference, the objectives of the Special Report were to:

- describe the DND/CAF authority and policy framework for the collection, use, retention and dissemination of information on Canadians;
- describe the circumstances in which, and purposes for which, the collection, use, retention and dissemination of Canadian citizen information is permitted, versus those in which it is prohibited;
- describe the manner in which DND/CAF tracks and documents its collection, use, retention and dissemination of Canadian citizen information; and
- assess the legal, policy and administrative frameworks under which the collection, use, retention and dissemination of Canadian citizen information is permitted or prohibited.

93. This Special Report has addressed the first three of these objectives:

- **DND/CAF authority and policy framework**: In the absence of clear statutory provisions for defence intelligence, DND/CAF defence intelligence activities are largely conducted under the authority of the Crown prerogative. In practice where DND/CAF faces the possibility of encountering information about Canadians, DND/CAF relies on authorities under the Integrated SIGINT [Signals Intelligence] Operations Model for its SIGINT activities (see paragraphs 35 and 53) and partnerships with other federal government departments and agencies for its other activities (such as *** see paragraphs 18–21 and 69–79 respectively) through a request for assistance pursuant to section 273.6 of the *National Defence Act*. DND/CAF defence intelligence activities are also subject to several policy documents, mostly in the form of functional directives, several of which include directions on the handling of information about Canadians. The CANCIT Functional Directive, intended to apply to all defence intelligence activities, is the latest addition to the policy suite. (Chapters 1–4)
- **Circumstances permitting and prohibiting the handling of CANCIT information:** The intentional collection of information about Canadians is currently authorized only in the context of the DND/CAF counter-intelligence program, and where DND/CAF is providing assistance to another department or agency pursuant to section 273.6 of the *National Defence Act*. In all other cases, DND/CAF adopts a cautious approach, most often opting to *** in which information about Canadians was inadvertently encountered. (Chapters 3–4)
- **Tracking and documenting the use of CANCIT information:** Prior to the CANCIT Functional Directive, there was no requirement to track how information about Canadians was handled. Given the limited amount of available data, the Committee cannot comment on this aspect of the Special Report. (Paragraphs 89–91)

94. The Committee turns next to its assessment of the legal, policy and administrative frameworks under which the collection, use, retention and dissemination of Canadian citizen information is permitted or prohibited. The Committee focuses its assessment in three areas. The first is the trigger for this Special Report: DND/CAF's current policy framework to handle information about Canadians. The second area is the issue of the extraterritorial application of the *Privacy Act*. The third area is DND/CAF's reliance on the Crown prerogative for the conduct of its defence intelligence activities, particularly when those activities involve the collection of intelligence about Canadians.

DND/CAF policy framework on Canadian citizens

95. The main purpose of the CANCIT Functional Directive is to "[e]nsure clarity on the legal and policy constraints around the collection of Canadian citizen (CANCIT) information when conducting defence intelligence activities."[108] For the reasons that follow, the Committee believes that the CANCIT Functional Directive has not achieved this objective, and lacks sufficient clarity with respect to its scope and to DND/CAF authorities for the collection of information about Canadians when conducting defence intelligence activities.

96. With respect to scope, the CANCIT Functional Directive was drafted as an overarching direction to DND/CAF. This is evident from language used throughout the document:

- the directive applies to all officers and members of the CAF and all employees of DND, not only those of units responsible for specific defence intelligence activities;
- the "purpose" of the directive refers to "defence intelligence activities" generally; and
- the definitions cited in the directive are generic and drawn from DND/CAF official nomenclature (e.g., defence intelligence, information, intelligence, operations).

97. Despite the directive's statements in regard to its scope of application, DND/CAF sought to limit its general application in the course of the review. DND/CAF explained that, in practice, directives and orders governing other defence intelligence activity areas – such as signals intelligence (SIGINT) and human intelligence (HUMINT) – continue to be in force and must be read in conjunction with the CANCIT Functional Directive.[109] DND/CAF also stated that the need for the CANCIT Directive stemmed from issues related to the handling of captured equipment and material (CEM) *** However, the CANCIT Functional Directive does not make references to SIGINT, HUMINT, CEM or other defence intelligence activity areas, nor the need to read its guidance in conjunction with any other relevant functional directives. In short, the CANCIT Functional Directive does not define which defence intelligence activities are included in its scope, nor which directives take precedence with respect to the handling of CANCIT information. As discussed in paragraph 8, the Committee was unable to verify why the CANCIT

[108] DND/CAF, Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information, August 31, 2018.
[109] DND/CAF, Remarks to NSICOP, May 30, 2019.

Functional Directive was required, given existing guidance in other functional directives, nor establish what problems it was meant to address or resolve.

98. The lack of clarity in the policy framework also manifests itself in the characterization of DND/CAF authorities. The CANCIT Functional Directive states:

> DND/CAF operations and activities shall not involve the collection of CANCIT information for defence intelligence purposes except where:
> - Collection occurs in support of mandated defence operations and activities; or
> - 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.[110]

99. Although the CANCIT Functional Directive appears to prohibit the collection of information about Canadians, the Committee is concerned that the first exception to that prohibition negates it entirely. On a plain reading, the language used in the directive strongly suggests that DND/CAF personnel are permitted to collect information about Canadians in all cases where a defence intelligence activity occurs in support of mandated operations. As with other parts of the CANCIT Functional Directive, the language refers to all defence intelligence activities. It does not identify specific defence intelligence activities, some of which, most notably SIGINT activities, have explicit statutory prohibitions against intentionally collecting the communications of Canadians, including in the context of mandated operations. Moreover, the CANCIT Functional Directive definition of "operations" includes a broad range of military activities, again suggesting that the collection of information about Canadians is permitted on all military missions.

100. On the broader record provided to the Committee during its 2018 review of defence intelligence activities and this Special Report, it is clear that DND/CAF does not, in fact, use the Crown prerogative to collect information about Canadian citizens as part of its defence intelligence activities in the context of mandated operations.[111] The Committee is concerned, however, by the ambiguity in DND/CAF directives and policies about its authorities to do so. In short, direction about authorities to collect information in the conduct of defence intelligence activities, especially where they may involve information about Canadians, should be clearly stated.

101. The Committee believes that the authorities for the second type of collection, in support of another government department and under its authorities, are clearer. DND/CAF stated that such support is provided under the authority of 273.6 of the *National Defence Act*. The Committee is

---

[110] DND/CAF, Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information, August 31, 2018.

[111] The 2018 review demonstrated that several defence intelligence activities include clear restrictions or prohibitions on such activity – most notably, signals intelligence (SIGINT) and human intelligence (HUMINT) activities. See NSICOP, *Annual Report 2018*, paragraphs 180 and 181, www.nsicop-cpsnr.ca/reports/rp-2019-04-09/2019-04-09_annual_report_2018_public_en.pdf.

satisfied, through its familiarity with the request made by [*** another government organization to DND/CAF ***] that appropriate mechanisms are in place to obtain such authorities.

102. However, the Committee returns to a theme raised in its 2018 Annual Report: important limitations on intelligence activities being embedded in policy documents rather than statute.[112] The requirement in the CANCIT Functional Directive (and using similar language, in the Ministerial Directive on Defence Intelligence) that intelligence support to another government department is subject to the authority of the requesting department is a self-imposed restriction. Section 273.6 of the *National Defence Act* provides that the "the Governor in Council, or the Minister [of National Defence] on the request of the Minister of Public Safety and Emergency Preparedness or any other Minister, may authorize the Canadian Forces to perform any duty involving public service." The term "public service" is not defined, and there is no restriction on what DND/CAF may do. In contrast, the authority of the Communications Security Establishment (CSE) to provide assistance is limited, through express statutory language, to the powers of the assisted department or agency.[113] It is not clear to the Committee why limitations on this type of assistance should be found in policy for one organization and statute for another; statutory clarity should exist for both.

The extraterritorial application of the *Privacy Act*

103. During the course of this review, the Committee became aware of two issues of significant concern relating to the *Privacy Act*. The first is that DND/CAF takes an inconsistent approach to the application of the *Privacy Act*. In the area of domestic intelligence collection, particularly counter-intelligence activities, DND/CAF applies the *Privacy Act* for the sharing of information with other government departments with respect to personnel security issues, and the maintenance of a personal information bank (see paragraph 67). More generally, DND/CAF appears to apply the *Privacy Act* in the context of sharing of intelligence with other government departments. The CANCIT Functional Directive itself cites the *Privacy Act* as a reference, and states that "CANCIT information may be shared with other Canadian government departments and agencies if the disclosure is authorized by law, including the *Privacy Act*."

104. [*** This paragraph has been revised to remove injurious or privileged information. However, the Committee concluded through the course of its review that DND/CAF believes that the *Privacy Act* does not apply to its overseas operations. The Committee examined a case study that, in the Committee's opinion, showed that DND/CAF believes that the *Privacy Act* does not apply to its overseas operations. The *Privacy Act* has been in force since 1983 and does not contain exceptions regarding its application to DND/CAF activities outside of Canada. The Committee believes that the Minister of National Defence should clarify his department's position, and the Committee makes further recommendations on this issue at the end of the report. ***][114] ***[115]

---

[112] NSICOP, *Annual Report 2018*, paragraph 251.
[113] *National Defence Act*, 1985 R.S.C., c. N-5, s. 273.64(3).
[114] DND/CAF, ***

105. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes the Committee's second and related concern. ***]

106. Owing to its unique mandate, DND/CAF has two legal advisors: the Judge Advocate General and the Department of Justice. Under the *National Defence Act*, the Judge Advocate General is the legal advisor to the Governor General, the Minister of National Defence, the Department of National Defence and the Canadian Armed Forces in matters relating to military law and military justice, both highly specialized areas of expertise.[116] Parliament enacted the mandate of the Judge Advocate General in the *National Defence Act* in 1998.

107. On the other hand, the Minister of Justice and Attorney General is charged with the provision of advice "to the heads of the several departments of the Government on all matters of law connected with such departments."[117] The mission of the Department of Justice is to:

- support the Minister of Justice in working to ensure that Canada is a just and law-abiding society with a system of justice that is accessible, efficient and fair;
- provide high-quality legal services and counsel to the government and to client departments and agencies; and
- promote respect for rights and freedoms, the law and the Constitution.[118]

108. The role of the Department of Justice includes helping "the federal government develop policy and to draft and reform laws as needed." These responsibilities reflect "the dual role of the Minister of Justice, who is also by law the Attorney General of Canada. In general terms, the Minister is concerned with the administration of justice, including in such areas as criminal law, family law, human rights law and Aboriginal justice. The Attorney General is the chief law officer of the Crown, responsible for all litigation for the federal government."[119] In short, the Department of Justice is the government's 'law firm' on broader questions of law and the Constitution.

109. Concurrent with the decision to place the Judge Advocate General on statutory footing in 1998, the Department of Justice created the DND/CAF Legal Advisor, charged with giving legal advice on some matters previously within the purview of the Judge Advocate General. In principle, that meant that the Judge Advocate General would provide advice to the Department of National Defence, the Canadian Armed Forces and the Minister of National Defence on specialized areas of military law and operations, and the Department of Justice would provide advice on broader issues of law and the Constitution. In areas of overlap, the two organizations would work together to identify common principles and provide

---

[115] See Exclusions and Schedule 3 of the *Privacy Act*, https://laws-lois.justice.gc.ca/eng/acts/p-21/fulltext.html.
[116] *National Defence Act*, 1985 R.S.C., c. N-5, s. 9.1. See also *National Defence Act*, 1985 R.S.C., c. N-5, s. 10.1, which provides that, for greater certainty, section 9.1 is not in derogation of the authority of the Minister of Justice and Attorney General under the *Department of Justice Act*.
[117] *Department of Justice Act*, 1985 R.S.C., c. J-2, s. 5(*b*).
[118] Department of Justice, "Our Mission," www.justice.gc.ca/eng/rp-pr/cp-pm/about-aprop/index.html.
[119] Department of Justice, "Our role," www.justice.gc.ca/eng/rp-pr/cp-pm/about-aprop/index.html.

consistent advice. While this approach may produce conflict in practice,[120] it is to the benefit of DND/CAF to receive legal advice from organizations with expertise in relevant areas of law. It seems reasonable, for example, that the legal advice of the Judge Advocate General would have primacy in relation to issues relating to the *Law of Armed Conflict*, also known as International Humanitarian Law. However, to the extent that DND/CAF activities implicate more general public law issues that may also arise for other agencies in different settings (e.g., the consular activities of Global Affairs Canada, visa applications made to immigration officers outside of Canada), the need for government lawyers to speak with one voice becomes acute.

110. [*** This paragraph was revised to remove injurious or privileged information. It discusses the Committee's assessment of the role of the Department of Justice. ***]

[120] As early as 1999, a rift "became perceptible between the DND and the Judge Advocate General respecting the provision of legal services." This included "examples of differing advice being given by the two offices in respect of the same matter, usually unwittingly." The then-JAG noted that "[s]uch unfortunate results are difficult to avoid with one government institution receiving advice from two sources, one internal but independent [JAG], the other external." Office of the JAG, *JAG Report (1998–99)*, August 4, 1999, www.Lareau-law.ca/Pitzul88-89.pdf.

Collection of information about Canadians

111. In recent missions, DND/CAF has obtained information about Canadians who may be members of armed extremist groups, such as Daesh. Like some citizens of our closest allies, Canadians have travelled to conflict zones to promote their objectives through violence. [*** The following two sentences have been revised to remove injurious or privileged information and to ensure readability. The sentences state that DND/CAF is aware of such instances, including in areas where DND/CAF has operated, and was asked by an ally to provide further information. DND/CAF also obtained intelligence about Canadians who may be involved in terrorist activities against Canada under the authority of another department. ***] In and of themselves, these instances may be isolated and may reinforce DND/CAF's contention that its defence intelligence activities rarely implicate Canadians. Nevertheless, these cases raise an important issue: should DND/CAF have explicit authority to collect, use, retain and disseminate information about Canadians where it may be appropriate to do so, including in circumstances where the use of lethal force against the concerned individuals is contemplated?

DND/CAF policy prohibitions on intentional collection of information about Canadians

112. Setting aside for the moment the caveat in DND/CAF's CANCIT Functional Directive that the collection of CANCIT information could occur in support of mandated defence operations and activities authorized under the Crown prerogative, DND/CAF has a clear policy bias against intentionally collecting information about or from Canadians in the context of its defence intelligence activities.

- DND/CAF conducts its SIGINT activities under CSE's authority, whose activities are subject to a blanket statutory prohibition against directing intelligence activities at Canadians.[121]
- Current DND/CAF activities to collect *** information about Canadians who may pose a threat to Canada are currently conducted under ***[122]
- DND/CAF has formalized a process through which [*** another department ***] shares back information that could be of interest to DND/CAF.
- DND/CAF has implemented operational policies and directions that it may not conduct HUMINT activities in Canada, nor direct its HUMINT activities at Canadians anywhere.[123]
- DND/CAF stated unequivocally that it does not share information about Canadians with Canada's allies.[124]

Under those standards, Canadian extremist travellers who may be present in DND/CAF areas of operations ***

---

[121] In the Canadian intelligence community, SIGINT collection is performed by both CSE under Part A of its mandate (foreign intelligence) and by DND/CAF as part of its deployed operations under delegated CSE authorities or the Crown prerogative. DND/CAF, Information briefing to the NSICOP Secretariat on the "Integrated SIGINT Operations Model," July 23, 2018.

[122] DND/CAF, CDS Tasking Order for ***

[123] DND/CAF, Defence Intelligence Functional Directive: CF HUMINT Intelligence Interrogation Operations in International Operations, 2014; Defence Intelligence Functional Directive: Strategic Debriefing, 2015; and Concept of Operations titled Biometrics – [Operation] IMPACT, July 22, 2015.

[124] DND/CAF, Response to NSICOP request for information, March 25, 2019.

113. These policy restrictions are difficult to reconcile with the operational reality described in Chapter 1 of this Special Report. The Committee recognizes that there are sensitivities associated with the potential consequences of military action on Canadians, even where the use of force is not contemplated. However, the threat posed by Canadian extremist travellers calls for a proportional response. The Committee is not convinced that the current *** approach to defence intelligence activities that involve Canadians, or information about them, constitutes an appropriate response to the threat posed by Canadian extremist travellers.

114. The government frequently deploys CAF members and DND employees to participate in international operations, most commonly as part of a coalition of countries. Where there are Canadians physically present in the area of operations who may pose a threat to coalition forces, it is incumbent on Canada to use its intelligence resources to help coalition forces understand the threat, [*** The rest of this sentence and the two following were revised to remove injurious or privileged information. The sentences describe the Committee's concerns with DND/CAF's approach. ***]

115. [*** This paragraph was revised to remove injurious or privileged information and to ensure readability. In the absence of clear authorities, DND/CAF looks to other domestic partners for authority to conduct intelligence activities. In some cases, this is perfectly legitimate: Parliament has provided statutory mechanisms for security and intelligence organizations to support the activities of other government departments where they have unique capabilities or powers. In other cases, it is less than ideal. This Special Report discussed an example where DND/CAF obtained information which contained CANCIT information and was uncertain it could possess or analyze that information. Working with another government department in these circumstances is not always effective, as those departments may not understand the intelligence or operational requirements of DND/CAF. There is also no guarantee that the department would detect in this information details that would be directly relevant to a military operation or that it would subsequently share information in a form that would be useful in a military context. Finally, DND/CAF's reliance on the authority of others may create challenges. This is incompatible with the fluidity of military operations, in which the value of operational intelligence declines over time (for example, the location of an individual or the timeframe for an event to occur). ***] ***[125]

116. When it encounters intelligence about Canadians who may be taking part in hostilities, DND/CAF should have no doubt concerning its authority to obtain that intelligence, determine its relevance, and share it with other government organizations or, if appropriate, allied nations.

[125] DND/CAF. Letter of the Chief of Defence Staff and Deputy Minister of National Defence to ***

The Crown prerogative

117. As noted, the CANCIT Functional Directive includes a caveat that the collection of information about Canadians may occur in support of mandated operations and activities authorized under the Crown prerogative. Indeed, DND/CAF relies on the Crown prerogative for all of its defence intelligence activities, except where it acts under the statutory authority of another department or agency. The question for the Committee was, if the Crown prerogative provides an implicit authority for DND/CAF to conduct defence intelligence activities in the context of a deployed operation, why in practice has it not also constituted a sufficient authority for DND/CAF to collect, use, retain and disseminate Canadian citizen information in the same context? In short, why doesn't DND/CAF direct its intelligence activities at Canadians?

118. It appears that the Crown prerogative is not sufficient for those purposes. While the Crown prerogative provides some implicit authority for defence intelligence activities conducted in support of DND/CAF-specific missions, that authority is uncertain on whether it permits DND/CAF to collect, use, retain and disseminate information about Canadians. As a result, DND/CAF collects information about Canadians only during the conduct of its counter-intelligence program, under the authority to the *Financial Administration Act*, or when conducting activities under the legal authority of another department, pursuant to section 273.6 of the *National Defence Act*.[126] For other defence intelligence activities, DND/CAF relies on the statutory authority of other departments and agencies regarding the handling of information about Canadians that may be encountered. Those authorities are well-grounded in legislation and jurisprudence, but were not designed for the specific needs of the military.

119. The applicability of the Charter to DND/CAF's defence intelligence activities is another source of uncertainty. In the current state of the law, the Charter does not typically apply extraterritorially, and *** However, the current position of the Supreme Court of Canada is that the Charter may apply in certain circumstances, particularly if Canadian state actors are in breach of their obligations under international law. In the future, this could well include the actions of DND/CAF in a foreign nation.

120. If the Charter were ever found to apply to the defence intelligence activities of DND/CAF outside Canada, the Committee believes that the argument that the Crown prerogative provides sufficient authority to collect information about Canadians would be unpersuasive. From a legal policy perspective, there is evidence that Parliament and successive governments believe, insofar as Canadian intelligence activities are involved, that safeguards must be in place where the state collects information about Canadians even where there is no certainty that the Charter applies. This is evident for Canada's two primary intelligence organizations: CSE and CSIS.

---

[126] The Committee notes that the term "counter-intelligence" in this context should be narrowly understood to include DND/CAF activities relating to its internal security posture under the Policy on Government Security, which are comparable to the activities of all departments and agencies of the Government of Canada. DND/CAF does not have powers, for example, to intercept communications, and instead, relies on CSIS, the RCMP or other law enforcement activities to conduct related investigations via formal requests for assistance to obtain a warrant to intercept communications.

121. The statutory scheme under which CSE conducts its activities prohibits CSE from targeting Canadians, even outside of Canada.[127] Recognizing that CSE activities carry the risk of inadvertently collecting information about Canadians, the scheme directs the agency to put in place measures to protect the privacy of Canadians in the use and retention of intercepted communications.[128] This scheme was recently amended by Parliament to add a new oversight mechanism for CSE, the Intelligence Commissioner, whose mandate will be to review the conclusions upon which the Minister of National Defence authorizes CSE to conduct a mandated activity, and to approve the authorization if the Minister's conclusions are reasonable, including those regarding measures to protect the privacy of Canadians.[129] Similar restrictions are in place for situations in which there is a risk that private communications of Canadians could be intercepted.[130] Similarly, Parliament recently amended the *CSIS Act* to extend the jurisdiction of a designated judge of the Federal Court to issue a warrant authorizing CSIS to take investigatory actions outside Canada.[131] Although this amendment was meant to address specific jurisdictional issues surrounding certain CSIS activities, it also mitigates risks where a Charter-protected right may be infringed by requiring a warrant in specific circumstances.

122. In short, relying on the Crown prerogative as authority to collect, use, retain and disseminate Canadian citizen information is not a viable option. Rather, the Committee reiterates the rationale it provided in its 2018 Annual Report for the government to consider providing explicit legislative authority for the conduct of defence intelligence activities (see Chapter 4, *Annual Report 2018*, especially "Defence intelligence: The question of legislation," paragraphs 241–252). On the basis of this review, the Committee offers two further reasons to establish statutory authority for DND/CAF to conduct defence intelligence activities.

123. First, the current approach to defence intelligence activities, conducted under the umbrella of the Crown prerogative and a collection of directives and other instruments, creates uncertainty. In the worst instances, DND/CAF is unsure that it has the legal authority to do things that, from a policy or operational perspective, it should be able to do. [*** This sentence was revised to remove injurious or privileged information. The sentence notes that the Committee commended DND/CAF. ***] significant energy is directed at resolving them. Internal and external consultation undertaken to address legal doubt may contribute to operational delay, which itself may be prejudicial to the safety of DND/CAF members and Canada's national interests. Additionally, DND/CAF solutions may be imperfect, or involve awkward workarounds where DND/CAF relies on the authority of other departments and agencies. While these authorities may provide DND/CAF a legal 'safe harbour,' they come at the expense of ***

124. Second, ambiguous legal authorities are doubtful in a democratic system governed by the rule of law. Parliament has never contemplated what DND/CAF should do in the area of defence intelligence,

---

[127] *National Defence Act*, R.S.C., 1985, c. N-5, s. 273.64(2)(*a*).
[128] *National Defence Act*, R.S.C., 1985, c. N-5, s. 273.64(2)(*b*).
[129] Bill C-59, An Act respecting national security matters, L.C. 2019, c. 13, Part 2, assented to on June 21, 2019, and in force as of August 1, 2019.
[130] *National Defence Act*, R.S.C., 1985, c. N-5, s. 273.65.
[131] *Protection of Canada from Terrorists Act*, L.C., 2015, c. 9, s. 8.

and has never weighed issues of defence intelligence against issues of Charter-protected rights. As a result, defence intelligence is an anomaly among the other forms of intelligence in Canada. While it is true that the Crown prerogative is a source of some authority, it is not a transparently democratic source of legal authority. There is a credibility, and a social licence, that arises when an elected legislature speaks through legislation. State powers that have never been prescribed by legislation are uncommon, and the more invasive they are, the more they might reasonably attract controversy. If done properly, legislating DND/CAF's military intelligence mandate would address these concerns while preserving the flexibility it needs to execute its missions.

Conclusion

125. The Committee prepared this Special Report for three reasons. The first was to reconcile DND/CAF's assertion that it does not direct its defence intelligence activities at Canadians with a plain language reading of the CANCIT Functional Directive, which suggests that DND/CAF does. The second was to understand DND/CAF's legal framework governing information on Canadians to determine whether the Committee's 2018 recommendations should be adjusted. The third was to determine whether DND/CAF's legal framework gave rise to any legal or operational risks.

126. On the basis of the record before the Committee, it is clear that DND/CAF does not *currently* direct its defence intelligence activities at Canadians, except in specific circumstances where it has clear authority (counter-intelligence) or where it provides assistance to other government organizations under their authority (a case studied in this review). That clarity is not reflected in the CANCIT Functional Directive. Rather, the CANCIT Functional Directive reflects the assertion by DND/CAF that a decision by the government under the Crown prerogative could at some point provide DND/CAF with authority to direct its defence intelligence activities at Canadians.

127. The Committee does not believe that this assertion is reasonable. Canadian law has strong protections against unreasonable search and seizure and provisions to protect the privacy rights of Canadians. These are grounded in statutes that apply to every major security and intelligence organization. If the government decided to permit DND/CAF to direct its defence intelligence activities at Canadians, using the Crown prerogative may not prove to be an adequate source of authority. In its 2018 Annual Report, the Committee recommended that the government give serious consideration to providing explicit legislative authority for the conduct of DND/CAF defence intelligence activities. For the reasons outlined in this Special Report, the Committee now believes that it is insufficient for the government to only consider this question; rather, the government should provide DND/CAF with a clear statutory authority to conduct its defence intelligence activities in the context of deployed operations, including to collect information on Canadians.

128. This Special Report has also identified legal and operational risks which the Committee believes should be addressed. The first risk relates to the Committee's conclusion that DND/CAF's believes that the *Privacy Act* does not apply to its operations abroad, although DND/CAF alleges that it applies the spirit of the Act *** Here, too, the Committee's view is that DND/CAF's position is unjustifiable, ***

129. The second risk is that Canadian law may not be clear enough *** when Canadians are present in a DND/CAF theatre of operations. These instances may be rare, but they have occurred. When they occur, they raise significant policy, legal and operational issues. The Committee believes that Canadians who have travelled abroad to pursue their objectives through violent means should not be shielded from the legitimate intelligence activities of Canada's security and intelligence organizations. It also believes that the government has a responsibility to help to identify those individuals and take the necessary measures to stop them. In that context, DND/CAF intelligence personnel should be clear

about their authorities to obtain, collect, analyze and disseminate information about Canadians, subject to clear and reasonable statutory limitations that are consistent with the Charter, whether or not it applies outside Canada.

Findings

130. The Committee makes the following findings:

F1. The policy framework that the Department of National Defence / Canadian Armed Forces (DND/CAF) follows for the collection, use, retention and dissemination of information on Canadians needs clarification. (Paragraphs 95–102)

F2. DND/CAF is not fully compliant with the *Privacy Act* in relation to intelligence activities taking place outside Canada, activities to which the Committee believes the *Privacy Act* applies. (Paragraphs 103–104)

F3. ***

F4. The Crown prerogative may not prove to be an adequate source of authority for DND/CAF to conduct its defence intelligence activities, particularly where they involve information about Canadians. (Paragraphs 117–124)

Recommendations

131. The Committee makes the following recommendations:

R1. The Department of National Defence / Canadian Armed Forces (DND/CAF) rescind the Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information and, in consultation with the Privacy Commissioner, review all of its functional directives and other DND/CAF policy instruments that are relevant to the collection, use, retention and dissemination of information about Canadians to ensure consistent governance of these activities.

R2. To resolve the issue of the extraterritorial application of the Privacy Act, the Minister of National Defence should ensure DND/CAF complies with the letter and spirit of the Privacy Act in all of its defence intelligence activities, whether they are conducted in Canada or abroad.

R3. The Minister of National Defence introduce legislation governing DND/CAF defence intelligence activities, including the extent to which DND/CAF should be authorized to collect, use, retain and disseminate information about Canadians in the execution of its authorized missions.

Annex A – The CANCIT Functional Directive

(available only in English)

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;

1.1.2 Provide guidance for instances where CANCIT 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 CANCIT 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 CANCIT 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 CANCIT 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

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 CANCIT 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 CANCIT 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).

3.7 **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 CANCIT 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 CANCIT information that must be met while employing defence intelligence capabilities.

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	• Issuing functional direction on intelligence activities involving the collection, use, and sharing of CANCIT information that is lawful and policy compliant;

	• 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)	• 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	• 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	• 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	• Ensuring intelligence activities comply with CDI-issued functional direction and applicable laws and policies, including on deployed operations;

Commanders	• 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.E.G. Bishop
Rear-Admiral
Chief of Defence Intelligence

August 2018

Annex B – List of Witnesses

Department of Justice

- Deputy Legal Advisor and General Counsel, Canadian Forces Legal Advisor

Department of National Defence/Canadian Armed Forces

- Director General, Operations, Strategic Joint Staff
- Assistant Chief of Defence Intelligence, Canadian Forces Intelligence Command
- Acting Deputy Judge Advocate General Operations
- Executive Director, National Security and Intelligence Review and Oversight Coordination Secretariat

Academic

- Craig Forcese