

# PRIVACY AND RETENTION ISSUES OF DEFENCE INTELLIGENCE

by Captain Paul G. Rivard and Sergeant Joe Faragone

## Introduction

The ongoing international campaign against terrorism,<sup>1</sup> coupled with an evolving security environment, have resulted in an increased demand for intelligence in Canada, particularly for the Department of National Defence (DND) and the Canadian Forces (CF).<sup>2</sup> Consequently, a heightened scrutiny of privacy and access to information issues has emerged, due, in part, to an increase in media attention,<sup>3</sup> and also from recent occurrences surrounding intelligence use.<sup>4</sup>

Canada's armed forces have specific and vital needs in terms of intelligence to support CF operations – domestic, continental, and international – across the full spectrum of operations. When the Cabinet has to make a decision with respect to sending Canadian troops abroad, it requires timely and accurate intelligence.<sup>5</sup> Within DND, the mandate of the Chief of Defence Intelligence (CDI) is, “[to] provide intelligence services to DND and the CF in support of defence planning and military operations and to support other government departments as it relates to the security of Canada.”<sup>6</sup>

Intelligence support to operations is complex, and involves different levels of information requirements.<sup>7</sup> In order to create a secure environment for operations as well as to ensure force protection, CF members need strategic intelligence so that they can comprehend the global context. At the operational level, members need information on the intentions and capabilities of the belligerents, and on the local terrain, climate, and the means of transportation and communication. Finally, at the tactical level, members need to understand the particular conflict or peace situation in question in the local context.<sup>8</sup>

National security activities have the potential to adversely affect rights and freedoms.<sup>9</sup> This is, in part, because these activities may involve the most intrusive powers of the state: electronic surveillance; search and seizure of property; information collection and exchange with domestic and international security and intelligence and law enforcement agencies; and, potentially, the detention and prosecution of individuals.<sup>10</sup>

As a government management responsibility,<sup>11</sup> every CF member and DND employee in contact with defence intelligence must be knowledgeable of the appropriate privacy and retention issues. The intent of this opinion piece is to identify aspects of privacy and retention issues surrounding intelligence responsibilities; and to propose appropriate remedies.

## Intelligence

Defence intelligence is a term associated with data, information, and intelligence applicable to the military. In Canada, the authority to attain and retain defence intelligence is broadly established under the *National Defence Act*. Historically, military intelligence has focused primarily on the battle space and its operational, tactical, and strategic variables: enemy plans, intentions and order of battle; targeting; damage assessment; and field security.<sup>12</sup>

The NATO definition of intelligence is: “The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.”<sup>13</sup> Information operations is a more encompassing term, defined as, “continuous military operations within the Military Information Environment (MIE) that enable, enhance and protect the commanders decision-making cycle and mission execution to achieve an information advantage across the full range of military operations. They include interacting with the Global Information Environment (GIE) and exploiting or attacking an adversary's information and decision systems.”<sup>14</sup>

Another definition, relative to joint intelligence, describes intelligence as:

“Intelligence, in a military context, is the product of our knowledge and understanding of the physical environment; weather, demographics and culture of the operational area, the activities, capabilities and intentions of an actual or potential threat, or any other entity or situation with which the Canadian Forces is concerned. Intelligence is fundamental to the planning and conduct of operations, and to force protection, through all dimensions of conflict as it allows the commander to gain control of the threat or situation and mastery of the environment.”<sup>15</sup>

Within this same context, the following illustration demonstrates a relationship among data, information, and intelligence, and expresses the concept that a high *volume* of input results in a lower *yield*.<sup>16</sup>

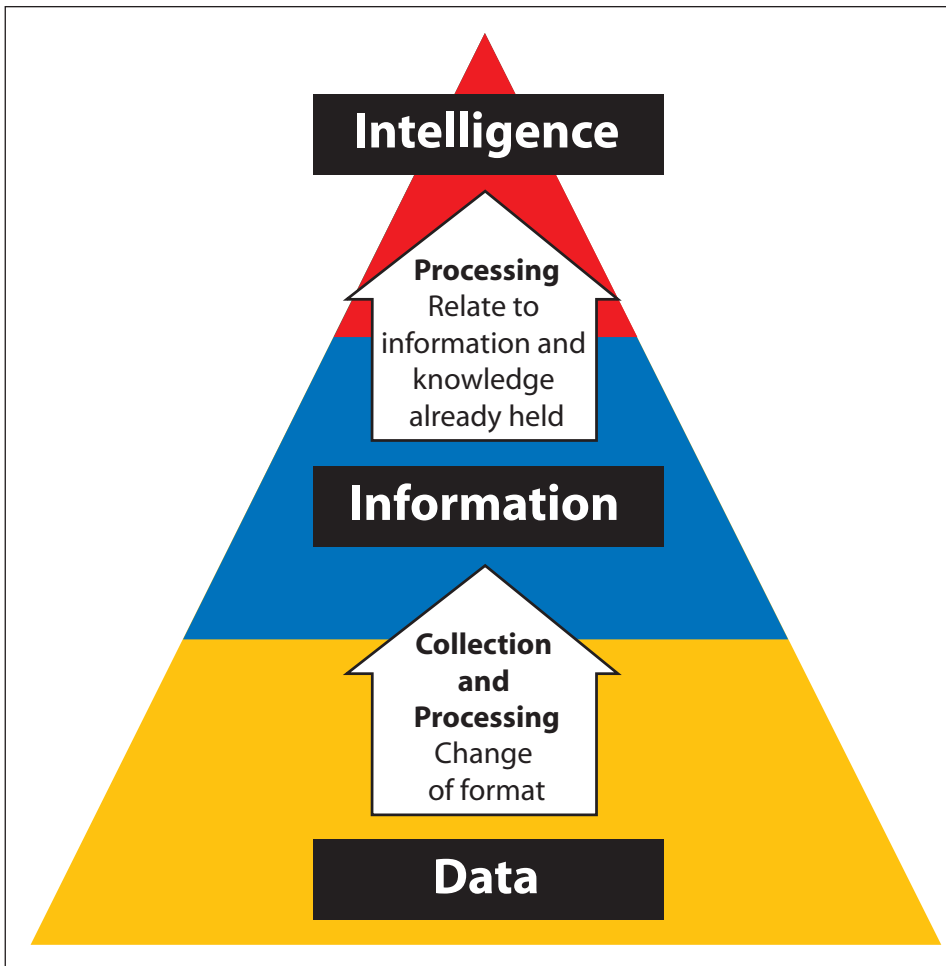


Figure 1 – Information and Intelligence Relationship

- Imagery Intelligence (IMINT) is intelligence derived from imagery acquired by photographic, radar, electro-optical, infra-red, thermal, and multi-spectral sensors, which can be ground-based, seaborne, or airborne through overhead platforms.<sup>18</sup>
- Signals Intelligence (SIGINT) is the generic term used to describe Communications Intelligence (COMINT) and Electronic Intelligence (ELINT) when there is no requirement to *differentiate* between these two categories of intelligence, or it can represent *fusion* of the two categories. Communications intelligence (COMINT) is intelligence derived from electromagnetic (EM) communications and communications systems by other-than-intended recipients. ELINT is intelligence derived from EM and non-communication transmissions by other-than-intended recipients.

To be concise, intelligence is the product of the analysis of raw data and information input. Good intelligence is that product that provides a better understanding or knowledge of any issue. The trick to obtaining or creating prime intelligence is to identify needs, and then to simplify the solution for use at the suitable level. Therefore, intelligence is *use driven*.

Some concerns with respect to the privacy and retention issues of intelligence that has been sought, obtained, held, and distributed by the military can be visualized in the following diagram. It relates significant concerns to each of the four major categories of the intelligence cycle.

**Collection**

Although several definitions of intelligence categories exist, within the CF four types of intelligence categorize the majority of intelligence collection means:<sup>17</sup>

- Human Intelligence (HUMINT) is a category of intelligence obtained from information collected from and provided by human sources. This intelligence is derived from interviews or from interrogation, and the resultant collection may be applied to both Psychological Operations (PSYOPS) and Security Intelligence (SI).

- Technical Intelligence (TECHINT) is intelligence concerning technological developments, and the performance and operational capabilities of material, which have or may *eventually* have a practical application for military purposes. It is associated with scientific intelligence at the national level. This includes the collection of documents that are defined as any recorded information, regardless of its physical form or characteristics.

Privacy considerations with respect to the origin of intelligence are influenced significantly by collection from either domestic or international environments. Issues with respect to privacy considerations are anticipated to increase as the CF takes on a greater role in domestic operations. This is exacerbated by an increase in the use of technology, resulting in an enhanced Network Enabled Operations Capability.<sup>19</sup>

**Retention**

The question arises of what intelligence to retain? Depending upon the use of the intelligence, the *form* of retention also becomes important. In the case of information used for a briefing, it may only be important

## VIEWS AND OPINIONS

to retain the final product of intelligence, that is, the brief itself. On the other hand, if collection is intended to bolster an evidentiary case, such as war crimes, then the full draft notes of the collection may be required and stored under specific standards and conditions. Thus, the *intent* of the end use of collection will determine what information and intelligence to retain, and consequently, the format of the product.

The *type* of holdings will also be determined by end use. Should hard copies of originals be required, as in some litigation cases, then an extensive and specialized storage area is necessary. Alternately, electronic media storage of images, records, and documents may suffice for the retention of most collected materials. This is a system proven to be high volume and cost effective, and it provides a tool for the rapid recovery and tracking of information.

A tracking system for information must ensure that only appropriate access is granted to authorized users, a complex issue in the world of diverse communications methods, multiple database users, and high tempo operations. Policy must interrelate clearly who has access or a “need to know,” ownership, and proprietary rights.

Also, to comply with the intent of privacy, it is essential that a disposal or destruction schedule must be associated with each holding. Retention duration ought to include whether the holding is to be reviewed, destroyed, or archived at the expiration of a specified period.

### Dissemination

Dissemination is the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. Appropriate disclosure requires the need to limit which sources and agencies receive information. Further than the established *need-to-know*, under privacy, the *authorization-to-know* must be established. With the diversity and high volume of information and intelligence, the Canadian military must be sufficiently transparent to demonstrate how it effectively coordinates control of intelligence materials.

After dissemination, control is exerted through formal agreements as defined in law, and signed agreements known as memoranda of understanding (MOUs), or less formal “gentlemen’s agreements.”<sup>20</sup> A wide variety of agreements is extended to domestic, foreign, and international sources and agencies. Attached caveats indicate the appropriate action to

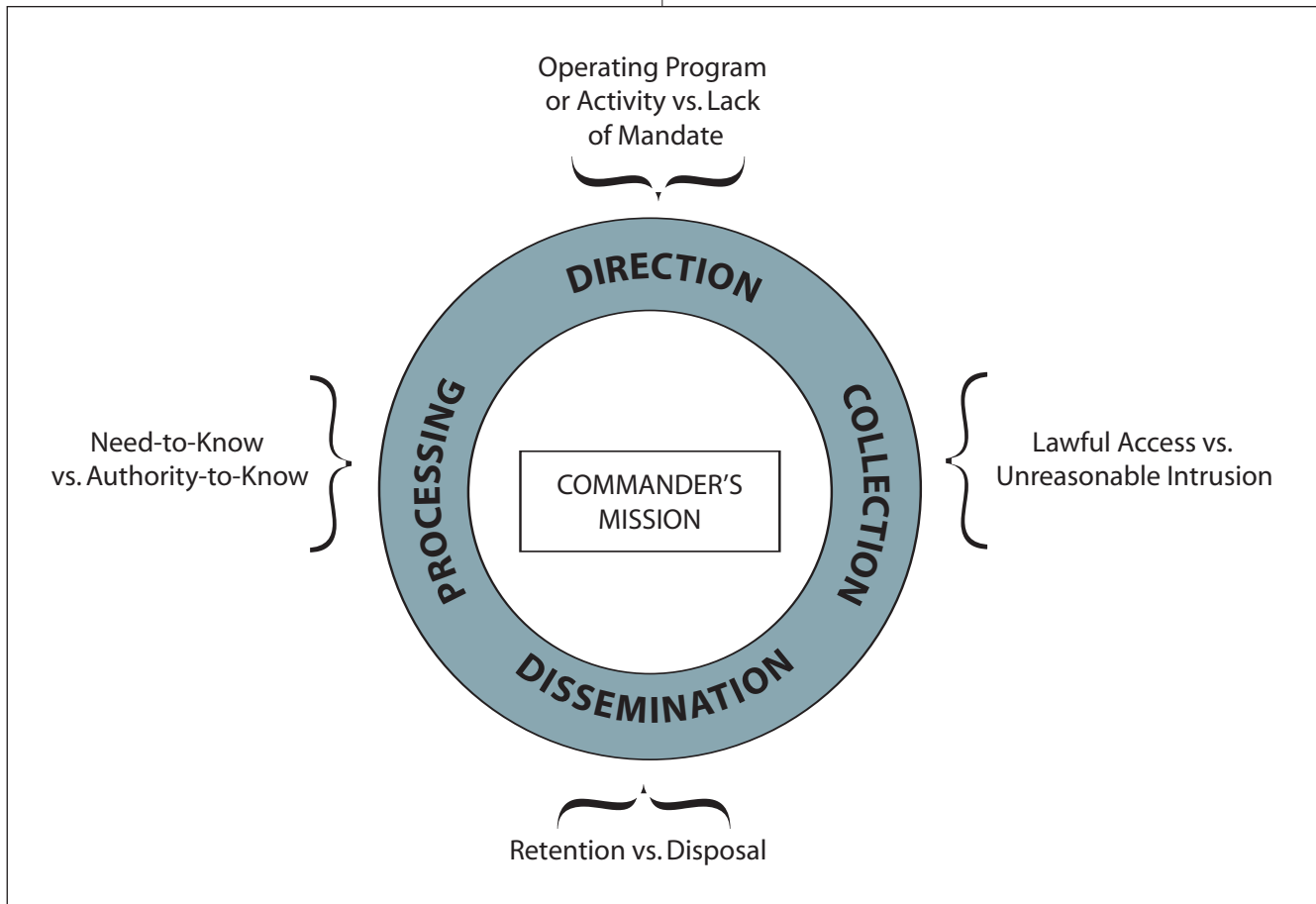


Figure 2 – Privacy Concerns in Relation to the Intelligence Cycle

be taken if the holder can comply no longer with the ability to control documentation. Hence, some general procedures exist so that intelligence product control might be assured through dissemination to public or safeguarded domains.

One of the National Defence Security Instructions, NDSI 26, outlines security aspects of "Access to and Release of Information." Herein, where generic direction is provided, such as a condition applicable to the release of information, the requirements of the Privacy and Access to Information Acts are respected. A framework is necessary to provide a pathway for continuous change in intelligence, and the exchange of intelligence, particularly in an increasingly complex world.<sup>21</sup>

### Privacy

The in-force provisions of the *National Defence Act* make limited reference to privacy or retention, primarily within the milieu of information regarding the Communications Security Establishment.<sup>22</sup> Legislation concerning intelligence collection, retention, and dissemination is multifaceted. Related privacy direction is provided, in part, in the *Privacy Act*, *Security of Information Act*, *Access to Information Act*, and *Personal Information Protection and Electronic Documents Act*. Importantly, the *Privacy Act* specifies that, "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution."<sup>23</sup>

The consequence of revealing safeguarded information is outlined in the *Security of Information Act*, as follows:

"14(1) Every person permanently bound to secrecy commits an offence who, intentionally and without authority, communicates or confirms special operational information."<sup>24</sup>

However, within this same act, some interpretation exists on whether an individual has an obligation to disclose information under certain circumstances, stating that information should be safeguarded, unless:

"15(1)(b) the public interest in disclosure outweighs the public interest in non-disclosure."<sup>25</sup>

Alternately, the *Access to Information Act* includes provisions to safeguard information injurious to the defence of Canada:

"15(1) The head of a government institution may refuse to disclose any record requested under this Act that contains information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities..."<sup>26</sup>

A balance between protecting information and *disclosure* is stated in the purpose of the *Personal Information and Electronic Documents Act*, namely, to *enhance* the exchange of information while *limiting* intrusive techniques:

"3. The purpose of this [Part] is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."<sup>27</sup>

The National Security Policy states that the government will ensure that its own systems are structured to better share information on threats, and this is a complex project that requires the integration of many different information systems. It must be undertaken in a way that respects the privacy rights of Canadians.<sup>28</sup>

Some concerns with respect to the need to restore Parliament as the center of decision-making were addressed in 2004 through the creation of an Interim Committee of Parliamentarians on National Security.<sup>29</sup> It was noted that the Canadian intelligence community employs thousands of people, expends hundreds of millions of dollars annually, and is subject to only very limited parliamentary scrutiny. This committee's mandate is articulated succinctly as follows:

"The committee will have the authority to scrutinize the intelligence community in pursuance of [the above] goals. The intelligence community includes all present and future departments, agencies and review bodies, civilian and military, involved in the collection, analysis, and dissemination of intelligence, for the purpose of Canada's national security."<sup>30</sup>

Moreover, the committee identified a need to manage the requirement for secrecy, wherein security and privacy are considered:

"The committee shall make reports directly to Parliament only after consultation with the Government to ensure that no classified information is disclosed. The Government shall have the right to review the committee's reports before they are tabled in Parliament, and to black out, but not edit or delete, such classified information as it deems necessary. The committee will also respect its obligations with regard to the disclosure of personal information as required by the *Privacy Act*."<sup>31</sup>

As an example of the intent to comply with litigation, the Communications Security Establishment (CSE) Annual Report (2004/2005) identified several forward-looking privacy concerns related to intelligence.<sup>32</sup>

## VIEWS AND OPINIONS

“One of the underlying principles guiding review is the anticipation of problem areas before they arise. That means looking beyond the issue of whether an unlawful activity has occurred, to whether one might occur and what measures can be put in place to prevent it. I believe this type of proactive and preventive approach is essential in balancing the undisputable need for security and intelligence activities with the fundamental privacy rights we have come to expect in Canada.”<sup>33</sup>

Contained within the Annual Report to Parliament (2004/2005) on the Privacy Act, the Privacy Commissioner noted that some have cited the act as a barrier to sharing critical personal information.<sup>34</sup> On the other hand, the Commissioner stated that this act does not need to be reformed to facilitate information sharing, but rather, it needs to be reformed to counter greater surveillance and intensive transactional data collection. In this same report, privacy was described as a risk management issue. And privacy management frameworks are considered of vital importance in helping federal institutions manage risk.<sup>35</sup> The Commissioner further recommended that the Treasury Board explore a model government-wide privacy management framework.

An overview of open source literature has shown that generalities of values and principles exist in some Canadian legislation and policies, but administrative specifics are either lacking, not centrally located, or not readily accessible. To protect privacy rights, the Privacy Commissioner has voiced similar concerns and an increased oversight need in the *Anti-Terrorism Act*.<sup>36</sup>

Given present circumstances, it is difficult to determine easily those administrative procedures that ensure lawful collection, retention, and dissemination of defence intelligence *versus* acts of unreasonable intrusion.

### Conclusions

**D**ND/CF personnel involved in defence intelligence rely upon the policies, procedures, guidelines, and regulations provided through national command direction in order to collect, retain, and disseminate information and intelligence appropriately.

After a review of privacy and retention issues that affect defence intelligence, we propose that the Canadian military requires a unique oversight mechanism.<sup>37</sup> This proposal is intended to clarify and streamline the increasingly complex issues that surround the flow of intelligence to or from domestic and international entities. An improved mechanism of public transparency, accountability, and assurance is needed. That is not to say that safeguarded information should be disclosed to the general public, but, rather, the mechanism is needed to provide an oversight and transparency service similar to those of the

Office of the Commissioner of Communications Security Establishment, Security Intelligence Review Committee, or the Inspector General for Canadian Security Intelligence Service.

It is proposed that this oversight mechanism, selected from intelligence professionals, be mandated, on a continuous basis, to study the network of agreements and direction that likely exist to handle defence intelligence.

Necessarily, a process of consultation would be expected at several levels that would include subject matter experts. Such a mechanism would be expected to deliberate privacy and retention issues within the context of intelligence monitoring, review, and accountability, and to suggest policy amendments and forward-looking corrective / preventative measures.

It is recommended that this overview mechanism report on an annual basis, in order to provide continuous oversight,<sup>38</sup> and, where appropriate, to contribute to the mandate of the Committee of Parliamentarians on National Security.

In the new millennium, an approaching wave of questions has appeared on the horizon directed toward those who are associated with national security and defence intelligence. We suggest that the Canadian military prepares, at all levels of leadership, for the type of scrutiny that inevitably will arise. In being so prepared, we will be able to assure critics and supporters alike.

Proposed proactive methods to prepare for, and contend with, privacy and retention issues of defence intelligence:

- Create an oversight mechanism, selected from intelligence professionals, which contribute in the mandate of the Committee of Parliamentarians on National Security.
- Centralize or initiate policy and direction that describes administrative specifics of professional conduct.
- Train staff, at all appropriate levels, who are in contact with defence intelligence.
- Communicate to the government and public any program associated with the Canadian military that complies with the intent of accountability and transparency.

---

Captain Rivard, a reservist, is an Intelligence Officer with the Cameron Highlanders of Canada, and has undergraduate and postgraduate degrees in science. He is also a graduate of the Canadian Land Force Command and Staff College.

Sergeant Faragone is an Intelligence Analyst with the Cameron Highlanders. He has undergraduate degrees in political science and public policy/public administration respectively, and is a Master of Arts in War Studies candidate at the Royal Military College of Canada.

## NOTES

1. Government of Canada, Department of National Defence, *Department of National Defence 2005-2006, Report on Plans and Priorities* <[http://www.vcds.forces.gc.ca/dgsp/pubs/rep-pub/ddm/rpp/rpp05-06/sec2d1\\_e.asp#1](http://www.vcds.forces.gc.ca/dgsp/pubs/rep-pub/ddm/rpp/rpp05-06/sec2d1_e.asp#1)> .
2. The evolving security environment is well documented in several Government of Canada publications, namely:  
*Securing an Open Society: Canada's National Security Policy (April 2004)*, <[http://www.pco-bcp.gc.ca/default.asp?Page=Publications&Language=E&doc=NatSecurnat/natsecurnat\\_e.htm](http://www.pco-bcp.gc.ca/default.asp?Page=Publications&Language=E&doc=NatSecurnat/natsecurnat_e.htm)>;  
*Canada's International Policy Statement: A Role of Pride and Influence in the World (2005)*, <<http://www.dfait-maeci.gc.ca/cip-pic/ips/ips-en.asp>>;  
*Defence Policy Statement* <[http://www.forces.gc.ca/site/reports/dps/index\\_e.asp](http://www.forces.gc.ca/site/reports/dps/index_e.asp)>;  
*Strategic Assessment 2004* <[http://www.forces.gc.ca/admpol/eng/doc/strat\\_2004/index\\_e.htm](http://www.forces.gc.ca/admpol/eng/doc/strat_2004/index_e.htm)>;  
*Military Assessment 2002* <[http://www.vcds.forces.gc.ca/dgsp/pubs/rep-pub/dda/milassess/2002/intro\\_e.asp](http://www.vcds.forces.gc.ca/dgsp/pubs/rep-pub/dda/milassess/2002/intro_e.asp)>; and,  
*Chief of Defence Staff Action Team 1 Report* <<http://www.cds.forces.gc.ca/cft-tfc/00native/CAT%201%20Exec%20Sum%20Eng.pdf>>.
3. Wesley Wark, "Silence won't keep us safe: Security is a major problem in the U.S., Britain and Australia; there's no reason Canada should be any different," in *Ottawa Citizen*, 17 January 2006, p. A15; Elenor Sloan, "Secure Canada. Or Else," in *Maclean's*, 7 November 2005, p.10; Jeremy Loome, "You Are The Target On A Quiet Street, A Man Is Plotting To Kill You," in *Ottawa Sun*, 11 September 2005; CFRA-AM, Steve Madely Show, Interview With Senator Colin Kenny, Ottawa, 19 July 2005; Steven Chase and Simon Tuck, "National security bill not aimed at energy takeovers: Emerson," in *Globe and Mail*, 15 July 2005; Nathan VanderKlippe, "Alert maintains vigilance," in *Regina Leader-Post*, 8 November 2004, pp. D6, D8; CBO-FM, "Public Safety: Are We Getting It Right?" on *Ottawa Morning*, 19 October 2004; and Joel J. Sokolsky, "Defending the homeland," in *National Post*, Comment, 10 June 2004.
4. Maher Arar Affair details at Arar Commission, <<http://www.ararcommission.ca/eng/index.htm>>; "RCMP raid on Ottawa Citizen," reporter Juliet O'Neill, at <[http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20040803/Arar\\_Federalgovernment\\_040801?s\\_name=&no\\_ads](http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20040803/Arar_Federalgovernment_040801?s_name=&no_ads)>.
5. Jérôme Mellon, *The Missing Agency: The Case for a Canadian Foreign Intelligence Service*, 2<sup>nd</sup> Edition, 2003, p. 11, at <<http://circ.jmellon.com/docs/view.asp?id=370>>.
6. <[http://dcds.mil.ca/cdi/default\\_e.asp](http://dcds.mil.ca/cdi/default_e.asp)>.
7. Jérôme Mellon, p.12.
8. Jessica M. Davis, "From Kosovo To Afghanistan: Canada And Information Operations," in *Canadian Military Journal*: August 2005, Vol. 6, No. 3, pp. 33-42.
9. Government of Canada, *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar Policy Review, National Security And Rights And Freedoms, A Background Paper to the Commission's Consultation Paper, December 10, 2004*; and, Government of Canada, The McDonald Commission Report. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and security under the law: Second Report*, 2 volumes, 1981.
10. Douglas L. Bland and Roy Rempel, "A Vigilant Parliament: Building Competence for Effective Parliamentary Oversight of National Defence and the Canadian Armed Forces," in *Policy Matters* 5, No. 1(2004), Montreal: Institute for Research on Public Policy, at <<http://www.irpp.org/pm/archive/pmvol5no1.pdf#search='canada%20national%20defence%20oversight'>>.
11. Hugh D. Segal, "*National Security, The Public Interest And How We Govern: A Time For Innovation*," in *Canadian Military Journal*: Summer 2001. Vol. 2, No. 2, pp. 39-49.
12. Martin Rudner, "The Future of Canada's Defence Intelligence," in *International Journal of Intelligence and CounterIntelligence*: Winter 2002, Vol. 14, No. 4, pp. 540-564.
13. Government of Canada, National Defence. Land Force Information Operations. *Intelligence Field Manual*, OPI: DAD 5, 2000-09-01, B-GL-352-002/FP-001, p. 2.
14. Government of Canada, National Defence. *Land Force Information Operations. Information Operations*, B-GL-300-005/FP-001, OPI: DAD 5, 1999-01-18, p. 15.
15. Government of Canada, National Defence. *Joint Doctrine Manual. Joint Intelligence Doctrine*, B-GJ-005-200/FP-000, J2 Plans Pol, 2003-05-21, at <[http://www.dcds.forces.gc.ca/jointDoc/pages/j7doc\\_docdetails\\_e.asp?docid=20](http://www.dcds.forces.gc.ca/jointDoc/pages/j7doc_docdetails_e.asp?docid=20)>, p. 1-1.
16. *Ibid.*, pp.1-3.
17. Government of Canada, National Defence. *Land Force Information Operations. Field Manual Intelligence*, B-GL-357-001/FP-001, OPI: DAD 5, 2001-01-30, pp. 6-9.
18. Brian G. Whitehouse and Daniel Hutt, "Ocean Intelligence In The Maritime Battlespace: The Role Of Spaceborne Sensors and HF Radar," in *Canadian Military Journal*: Spring 2004, Vol. 5, No. 1, pp. 35-42.
19. Government of Canada, National Defence. Canada Command backgrounder Documentation. June 24, 2005; Government of Canada, National Defence. *Network Enabled Operations* at <[http://www.drdc-rddc.gc.ca/newsevents/events/neoeps\\_e.asp](http://www.drdc-rddc.gc.ca/newsevents/events/neoeps_e.asp)>.
20. Stéphane J. Lefebvre, "International Cooperation: Difficulties and Dilemmas," paper presented at the Colloque Renseignement et Sécurité internationale, Laval University, Quebec City, Canada, 20 March 2003, p. 14.
21. Deborah G. Barger, *Technical Report: Toward A Revolution In Intelligence Affairs*. National Security Research Division, RAND Corporation, 2005, p. iii.
22. Government of Canada, Department of Justice. *National Defence Act. Consolidated Statutes and Regulations*, at <<http://laws.justice.gc.ca/en/n-5/86182.html>> updated to 31 August 2004. Part V.1. Communications Security Establishment. Sections 273.61 to 273.7.
23. Government of Canada, Department of Justice. *Privacy Act. Consolidated Statutes and Regulations*, at <<http://laws.justice.gc.ca/en/P-21/95414.html>>, updated to 31 August 2004, Section 4.
24. Government of Canada, Department of Justice, *Security of Information Act. Consolidated Statutes and Regulations*, at <<http://laws.justice.gc.ca/en/O-5/101934.html>>, updated 31 August 2004, Section 14.
25. *Ibid.*, Section 15.
26. Government of Canada, Department of Justice. *Access to Information Act. Consolidated Statutes and Regulations*, at <<http://laws.justice.gc.ca/en/A-1/text.html>>, updated to 31 August 2004, Section 15.
27. Government of Canada, Department of Justice. *Personal Information and Electronic Documents Act. Consolidated Statutes and Regulations*, at <<http://laws.justice.gc.ca/en/P-8.6/93366.html>> updated to 31 August 2004, Section 3.
28. Government of Canada, Privy Council Office. *Chapter 2 – Building an Integrated Security System* at <[http://www.pco-bcp.gc.ca/default.asp?Language=E&Page=publications&Sub=natsecurnat&Doc=natsecurnat\\_e.htm#ch3](http://www.pco-bcp.gc.ca/default.asp?Language=E&Page=publications&Sub=natsecurnat&Doc=natsecurnat_e.htm#ch3)>.
29. Government of Canada, Parliament. *Interim Committee of Parliamentarians on National Security. Report of the Interim Committee of Parliamentarians on National Security*, Ottawa, 2004.
30. *Ibid.*, p.12.
31. *Ibid.*, p.15.
32. Government of Canada, Communications Security Establishment. *Office of the Communications Security Establishment Commissioner Annual Report 2004-2005*, April 2005.
33. *Ibid.*, p.5.
34. Government of Canada, Privacy Commissioner of Canada. *Report on the Privacy Act – Annual Report to Parliament 2004-2005*, at <[www.privcom.gc.ca](http://www.privcom.gc.ca)> p.12.
35. *Ibid.*, p.31.
36. Government of Canada, Privacy Commissioner of Canada. *Contained surveillance and increased oversight needed in Anti-Terrorism Act to protect against loss of privacy rights* News Release 9 May 2005 at <[http://www.privcom.gc.ca/media/nr-c/2005/nr-c\\_050509\\_e.asp](http://www.privcom.gc.ca/media/nr-c/2005/nr-c_050509_e.asp)>.
37. Sean Henry, *Parliament and the Military*, The Conference of Defence Associates Institute. 16<sup>th</sup> Annual Seminar, 27 January 2000, at <<http://www.cda-cdai.ca/seminars/2000/summary.htm>>.
38. Government of Canada, National Defence. *On A Proposed Reform To Increase Parliamentary Oversight Of Defence*, Institute for Defence Resources Management – Economic Note Series 03 / 04, at <[http://www.rmc.ca/academic/poli-econ/idrm/notes/0304\\_e.html](http://www.rmc.ca/academic/poli-econ/idrm/notes/0304_e.html)>. Date modified 2005/10/11.