



**“CONNECTING THE DOTS” AND THE CANADIAN  
COUNTER-TERRORISM EFFORT - STEADY PROGRESS  
OR TECHNICAL, BUREAUCRATIC, LEGAL AND  
POLITICAL FAILURE?**



[www.cdfai.org](http://www.cdfai.org)

**“Connecting the Dots” and the Canadian Counter-terrorism Effort – Steady  
Progress or Technical, Bureaucratic, Legal and Political Failure?**

By

**Eric Lerhe (Cmdre ret'd)**

Fellow of the Canadian Defence & Foreign Affairs Institute

and

Doctoral Candidate at Dalhousie University

March, 2009

Prepared for the Canadian Defence & Foreign Affairs Institute  
1600, 530 – 8<sup>th</sup> Avenue SW, Calgary, AB T2P 3S8

[www.cdfai.org](http://www.cdfai.org)

© Canadian Defence & Foreign Affairs Institute

**Other Publications Written For Or Assisted By:**

**The Canadian Defence & Foreign Affairs Institute**

**Canada-U.S. Relations in the Arctic: A Neighbourly Proposal**

Brian Flemming  
December, 2008

**President Al Gore and the 2003 Iraq War: A Counterfactual Critique of Conventional “W”isdom**

Frank Harvey  
November, 2008

**Canada and the United States: What Does it Mean to be Good Neighbours?**

David Haglund  
October, 2008

**Redeployment as a Rite of Passage**

Anne Irwin  
April, 2008

**The 2007 Ross Ellis Memorial Lectures in Military and Strategic Studies: Is there a Grand Strategy in Canadian Foreign Policy?**

David Pratt  
March, 2008

**Military Transformation: Key Aspects and Canadian Approaches**

Elinor Sloan  
December, 2007

**CFIS: A Foreign Intelligence Service for Canada**

Barry Cooper  
November, 2007

**Canada as the “Emerging Energy Superpower”: Testing the Case**

Annette Hester  
October, 2007

**A Threatened Future: Canada’s Future Strategic Environment and its Security Implications**

J.L. Granatstein, Gordon S. Smith, and Denis Stairs  
September, 2007

**Report on Canada, National Security and Outer Space**

James Fergusson and Stephen James  
June, 2007

**The Information Gap: Why the Canadian Public Doesn’t Know More About its Military**

Sharon Hobson  
June, 2007

**Conflict in Lebanon: On the Perpetual Threshold**

Tami Amanda Jacoby  
April, 2007

**Canada in Afghanistan: Is it Working?**

Gordon Smith  
March, 2007

**Effective Aid and Beyond: How Canada Can Help Poor Countries**

Danielle Goldfarb  
December, 2006

**The Homeland Security Dilemma: The Imaginations of Failure and the Escalating Costs of Perfecting Security**

Frank Harvey  
June, 2006

**An Opaque Window: An Overview of Some Commitments Made by the Government of Canada Regarding the Department of National Defence and the Canadian Forces; 1 January 2000 – 31 December 2004**

David J. Bercuson, Aaron P. Plamondon, and Ray Szeto  
May, 2006

**The Strategic Capability Investment Plan: Origins, Evolution and Future Prospects**

Elinor Sloan  
March, 2006

**Confusing the Innocent with Numbers and Categories: The International Policy Statement and the Concentration of Development Assistance**

Denis Stairs  
December, 2005

**In the Canadian Interest? Assessing Canada's International Policy Statement**

David J. Bercuson, Derek Burney, James Fergusson, Michel Fortmann/Frédéric Mérand, J.L. Granatstein, George Haynal, Sharon Hobson, Rob Huebert, Eric Lerhe, George Macdonald, Reid Morden, Kim Richard Nossal, Jean-Sébastien Rioux, Gordon Smith, and Denis Stairs  
October, 2005

**The Special Commission on the Restructuring of the Reserves, 1995: Ten Years Later**

J.L. Granatstein and LGen (ret'd) Charles Belzile  
September, 2005

**Effective Defence Policy for Responding to Failed And Failing States**

David Carment  
June, 2005

**Two Solitudes: Quebecers' Attitudes Regarding Canadian Security and Defence Policy**

Jean-Sébastien Rioux  
February, 2005

**In The National Interest: Canadian Foreign Policy in an Insecure World**

David J. Bercuson, Denis Stairs, Mark Entwistle, J.L. Granatstein, Kim Richard Nossal, and Gordon S. Smith  
October, 2003

**Conference Publication: Canadian Defence and the Canada-US Strategic Partnership**

September, 2002

**To Secure A Nation: The Case for a New Defence White Paper**

David J. Bercuson, Jim Fergusson, Frank Harvey, and Rob Huebert  
November, 2001

Publications are available at [www.cdfai.org](http://www.cdfai.org) or call Katharine McAuley at (403) 231-7624

## **EXECUTIVE SUMMARY**

Since the 9-11 attacks on the United States, Canada has made significant investments in its counter-terrorist capabilities. A \$9.5 billion budget, a new “super” department charged with public security, various coordination centres, numerous integrated enforcement teams, and our first national security policy also suggest we now have a cohesive federal response. This paper will argue that suggestion is not supported by the evidence. In the most critical areas of intelligence sharing and coordination – “connecting the dots” – progress is doubtful. The paper also examines claims that technical problems, inadequate funding and legal restrictions were the cause. Ultimately, the paper rejects these factors and turns to the quality of government leadership.

## SOMMAIRE

Depuis les attaques du 11 novembre sur les États-Unis, le Canada a beaucoup investi dans ses capacités de contre-terrorisme. Un budget de 9,5 milliards de \$, un nouveau « super » ministère chargé de la sécurité publique, divers centres de coordination, de nombreuses équipes intégrées d'application des lois et notre première politique nationale sur la sécurité nous portent à croire que nous avons maintenant une réponse fédérale cohésive. Cette étude fait valoir que cette suggestion ne repose sur aucune preuve tangible. Dans les domaines les plus critiques du partage et de la coordination des renseignements – « en reliant les points les uns aux autres » - on peut douter qu'il y ait progrès. L'étude examine aussi les allégations qui rejettent la cause sur des problèmes techniques, une insuffisance de fonds et des restrictions juridiques. En bout de piste, l'étude rejette ces facteurs et braque les projecteurs sur la qualité de leadership du gouvernement.

In many ways the progress Canada has made in counter-terrorism has been significant. Since September 11, 2001, the RCMP, the Canadian Security Intelligence Service (CSIS), the older Office of Critical Infrastructure Protection and Emergency Preparedness, and a new Canadian Border Service Agency (CBSA) were brought together to make the 'super' department of Public Security and Emergency Preparedness Canada. Large elements of airport security were passed to the new Canadian Air Transport Security Authority. A series of new security centres emerged including the Government Operations Centre, CSIS' Integrated National Security Assessment Centre,<sup>1</sup> CBSA's National Risk Assessment Centre and three multi-departmental Marine Security Operations Centres.<sup>2</sup> In addition, successive governments have funded over 23 Integrated Border Enforcement Teams and several Integrated National Security Enforcement Teams. These initiatives were backed up by Canada's first national security policy, *Securing an Open Society* and a \$ 9.5 billion budget.<sup>3</sup>

However impressive this all may be, there is mounting evidence that progress has stalled in the coordination of this massive counter-terrorism effort; therefore, this paper will examine why expert opinion attaches such high importance to achieving a coordinated national anti-terrorist effort.<sup>4</sup> The paper will then examine the extent that technical problems, inadequate funding, legal barriers and a want of direction are hampering Canada from achieving it. My concluding prescriptions will then concentrate on those areas likely to have the highest payoff in terms of improving coordination. Throughout, the focus will be on the need to coordinate and share data within Canada and not the parallel problem of doing so with other states.

## CONNECTING THE DOTS

Since the 2001 attacks on the United States, the term "connecting the dots" emerged as the key element in counter-terrorist defence. The United States' 9-11 Commission loosely defined it as the ability of analysts to "draw relevant intelligence from anywhere in the government" on a developing attack, see the relationships between key elements, and identify the opportunities to defeat it.<sup>5</sup> The Commission's central argument was that the 2001 attacks were preceded by some ten separate "missed opportunities" where, had the CIA and the FBI shared data on the 9-11 plotters, analysts would have been able to connect the dots and thwart the attacks.<sup>6</sup> The Commission concluded:

The importance of integrated, all source analysis cannot be overstated. Without it, it is not possible to "connect the dots." No component holds all the relevant information.<sup>7</sup>

---

<sup>1</sup> The Integrated Threat Assessment Centre (ITAC) replaced the INSAC in 2004/5.

<sup>2</sup> In addition, the Financial Transactions Reports Analysis Centre of Canada's (FINTRAC) mandate was expanded to include a watch over terrorist activity.

<sup>3</sup> See Canada, *Securing an Open Society: Canada's National Security Policy*, (Ottawa: Privy Council Office, 2004). and Canada, *Budget 2001 –Budget Plan Chapter 5 Enhancing Security for Canadians*, (Ottawa, Department of Finance, 2001). See also Canada, *Report of the Auditor General to the House of Commons, Chapter 3 National Security in Canada-The 2001 Anti-Terrorism Initiative*, (Ottawa, Office of the Auditor General, 2004 Mar.), p. 10 where it is clear most of the money was spent in support of the national security task.

<sup>4</sup> The most prominent of these can be found in Canada, *Canadian Security Guide Book 2007 Edition, Coasts - a Report of the Standing Senate Committee on Defence and Security*, (First Session, 39<sup>th</sup> Parliament, March 2007, and Avis, Peter, Captain (N), *Canadian Maritime Domestic Security – Interoperability, Best Practices, and Dead Ends*, a paper presented at the CFPS 2008 Maritime Security Conference, Halifax N.S., 11 Jun 2008.

<sup>5</sup> See United States, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York, NY: W.W. Norton & Company, Inc., 2004), p. 400, 408 and 416.

<sup>6</sup> *Ibid.* p. 355-6.

<sup>7</sup> *Ibid.* p. 408.

Testimony before the ongoing Commission of Inquiry into the Air India bombing reintroduced Canadians to this key term. It now seems clear RCMP and CSIS ignored accurate information on the Sikh terrorist threat from the Indian government and our own External Affairs officials. Five days before Air India flight 182, when CSIS did elevate the threat warning of Sikh terrorism to “high,” this warning was not passed on to the RCMP teams at Pearson and Mirabel.<sup>8</sup> Testifying at the Air India inquiry in June 2007, retired Deputy Commissioner Jensen of the RCMP concluded that the attack “might have been prevented” if police and intelligence agencies had shared their data. He was confident that “somewhere there were some dots that could have been linked and should have been linked.”<sup>9</sup>

## THE CANADIAN COUNTER-TERRORIST EFFORT

### Problems

CSIS and the RCMP have reportedly improved their data sharing, and the Attorney General claimed in 2007 that data was now shared “regularly” between the two.<sup>10</sup> The profusion of centres and integrated teams federally would also suggest that such cooperation is widespread; however, this may not be a completely accurate assumption.

Somewhat surprisingly, airport security, and the data sharing needed to support it, is still problematic. In 2004 the Office of the Auditor General made clear “criminal intelligence data were not used to screen applicants for clearance to restricted areas” yet in December, 2008 the RCMP’s report on Project Spawn, its assessment of organized crime’s penetration of Canada’s airports, confirmed the problem continues today.<sup>11</sup> The report outlined that the Canadian Border Services Agency would not provide the RCMP the names of persons involved in drug seizures citing broad information disclosure restrictions within the *Customs Act*.<sup>12</sup> In addition, Transport Canada denied the RCMP information on those airport employees holding both a restricted area pass and a criminal record. This denial was based on legal arguments related to privacy and it effectively precluded the RCMP from linking those employees to its organized crime data;<sup>13</sup> however, the greatest concern was the report’s admission that other security clearance problems “could be” tied to the fact that “the RCMP and CSIS share insufficient information with Transport Canada to aid in its deliberations and decisions.”<sup>14</sup>

Even when intelligence data is provided by the RCMP and CSIS on such things as the terrorist threat, in 2007 the Senate Committee found that Transport Canada did not provide the CATSA personnel at the airports “direct access” to the terrorist intelligence material

---

<sup>8</sup> MacQueen, Ken, and John Geddes, “Air India: After 22 years, now’s the time for truth – like 9/11 it might never have come off if Canada’s experts had heeded the signs.” *Macleans*, (28 May 2007) at <http://www.macleans.ca> accessed 7 Jul. 2007.

<sup>9</sup> Bolan, Kim, “Police failures resulted in Air India disaster: inquiry,” CanWest News Service, (18 Jun 2007) at <http://www.canada.com/> accessed 17 Jul. 2007. See also Sallot, Jeff, “Air India Bombing: Intelligence breakdown left dots unconnected, ex Mountie says,” *The Globe and Mail*. (19 Jun. 2007), p. A8.

<sup>10</sup> Canada, “Final Submission of the Attorney General of Canada, Vol. III of III,” (undated), *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*, p. 174-176.

<sup>11</sup> Canada, *Report of the Auditor General to the House of Commons, Chapter 3 National Security in Canada-The 2001 Anti-Terrorism Initiative*, (Ottawa, Office of the Auditor General, Mar 2004), p. 2 and Canada, *Project SPAWN - A Strategic Assessment of Criminal Activity and Organized Crime Infiltration at Canada’s Class 1 Airports*, (Ottawa, RCMP, 10 Dec 2008).

<sup>12</sup> Section 107 of the act was cited. I will return to this point. See also RCMP, *SPAWN*, p. 5.

<sup>13</sup> RCMP, *SPAWN*, p. 5. By the way the exchange restrictions did not end here, and the Project reported such mundane data as the “job category of employees” and statistical data on the number of airport employees with criminal records was also denied them. See RCMP, *SPAWN*, p. 15.

<sup>14</sup> *Ibid*, p. 16

available. Instead, a cumbersome process routed the RCMP and CSIS data through Transport Canada and then CATSA's headquarters to arrive at the front line screening teams at the airports as a written daily brief.<sup>15</sup> Transport's response to the Senate committees also suggested no plans were being made to change this. The Committee also suspected the data sharing bottleneck may be related to "one more Ottawa turf war."

Similar problems hazard coordination and data exchange in the maritime approaches to Canada. The 2004 National Security Policy directed the forming of multi-department Marine Security Operations Centers (MSOC) on the Atlantic and Pacific coasts and the St. Lawrence. It also mandated they be "headed by Canadian Forces Maritime Command" and that "the centres will include staff from the CBSA, Transport Canada, the RCMP, and the Canadian Coast Guard."<sup>16</sup> The Atlantic MSOC was staffed the next year, but progress elsewhere was slow. Three years later, the Pacific MSOC was fully manned, possibly spurred on by the Senate Committee's critiques of slow progress; however, the MSOC in the Great Lakes is still at "interim" status due to a lack of RCMP funding that was only corrected in Budget 2008.<sup>17</sup> In 2008, only the RCMP and DND were in attendance with the three other agencies absent.

Even when all the departments assemble, not all can share data. While in a perfect data sharing structure each agency would have access to the other's database to allow instantaneous "dot" connection across the government's data systems, technology and legal concerns are reportedly hampering that effort.<sup>18</sup> These combined maritime centres hoped to overcome this by collecting the various departments' officers with their separate databases into a single room where face-to-face exchanges might move the information instead. Regrettably, even this sub-optimal approach was occasionally thwarted with an officer at one MSOC claiming in 2006 that, "anything collected under the auspices of the *Customs Act* cannot be shared with any other department. It can be as benign as the name of a ship."<sup>19</sup> This, of course, dooms any effort to connect all the elements of the myriad data that can provide warning of a developing terrorist attack. In response to these barriers, the Department of National Defence has recently started 'war gaming' cross-government legal activities within its maritime exercises. In 2007, for example, legal teams from across government and the United States participated in exercise FRONTIER SENTINEL, an attempt to isolate the legal barriers in the operations that cross-departmental and national boundaries. When an exercise event failed because of a perceived legal or procedural impediment these teams either resolved the impasse or recorded it for later analysis and, one hopes, correction.<sup>20</sup>

The Maritime Information Management Data Exchange System (MIMDEX) project offered another potential solution to local data sharing problems as well as providing critically needed inter-regional secure connections between the eight federal agencies and

---

<sup>15</sup> CATSA's airport teams appear to get their data from the two officials working within CATSA who are charged with processing the RCMP and CSIS data that was relayed by Transport Canada and then transcribing it into daily and weekly briefs. These then appear to make their way to the agency's airport teams. See Senate, Canadian Security Guide Book 2007, p. 64 -65. The OAG had also raised similar concerns in their 2004 (Mar) Chap 3, p. 20 and in a redacted 2006 OAG report held only by the Senate Committee.

<sup>16</sup> Canada, , *Securing an Open Society*, p. 37-38.

<sup>17</sup> See the RCMP's description of its "interim MSOC" at <http://www.rcmp-grc.gc.ca/mari-port/faq-eng.htm#2> (accessed 17 Jan 2009.)

<sup>18</sup> See particularly, Avis, Canadian Maritime Domestic Security, p. 7 and 8 of 9.

<sup>19</sup> Thatcher, Chris, "A pan-government approach to marine security," *Vanguard* (Knowledge Center, Defence) (2006).

<sup>20</sup> See Belleveau, Bruce, Captain (N), *Marine Security - Frontier Sentinel*, a briefing presented at the CFPS 2008 Maritime Security Conference, Halifax N.S., 11 Jun 2008. Regrettably, the government has not released the details of legal problems encountered to the public.

departments that have over-water responsibilities. Conceived in 2004, and supported by the two separate Senate reports urging "priority" action, the government agreed to provide a "fully operational" MIMDEX system by 2007; however, in 2009, there is still no MIMDEX system and the project is completely stalled.<sup>21</sup> Captain (N) Avis, an officer engaged in this file, suggested its problems are related to heightened concerns over privacy sparked by the Arar Commission.<sup>22</sup>

The Financial Transactions Reports Analysis Centre of Canada (FINTRAC), the unit responsible for tracking criminal and terrorist money transfers and laundering, provides similar lessons in the need for government agencies to have access to each other's databases and the difficulties encountered in providing it; however, this initiative does provide several offsetting positive elements. One of the most important assessed the Canadian money tracking effort against the international standards set by the G-8 sponsored Financial Action Task Force (FATF). In 2004, Finance Canada completed a five year evaluation of its anti-laundering effort, and its report argued convincingly that it had met the vast majority of those international FATF standards.<sup>23</sup> The Finance report did not indicate where it did not, but its table of "International Comparisons" suggests Canada's FINTRAC is the only one of the four national financial intelligence units (FIU) reviewed that does not allow its national law enforcement and security agencies "direct access to the FIU database." Rather, the Canadian entry reads, "No. This is the case due to Charter and privacy laws."<sup>24</sup> This is not further explained. Also not explained is how the reverse ability of FINTRAC to access Canadian national security and law enforcement databases does not involve such legal problems.<sup>25</sup>

That evaluation also took the unusual step of conducting interviews with its "partners" in the RCMP, CSIS, Canadian Border Services Agency and the Canadian Revenue Agency. These agencies reported that FINTRAC's approach to data sharing was overly "risk averse" and that it had set the security/privacy balance "too strongly in favour of privacy concerns."<sup>26</sup> The evaluation then examined the enabling legislation more closely and found that the limited amount of data that was allowed to be exchanged – name, alias, exporter/importer, date of birth, address and citizenship – needed to be broadened. The evaluation found that this limited data set provided no clue to the cooperating law enforcement and national security agencies as to the context surrounding the money transaction under scrutiny. In response to the report, the government amended the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* in late 2006 to authorize the transfer of a significantly expanded data set. This would include such transaction-specific data as the criminal record and relevant criminal charges of those involved, their financial interests in it, and the indicators of a money laundering offense or terrorist activity associated with the transaction.<sup>27</sup> While there is no evidence to suggest this, one has the impression the readiness of government to amend the money laundering legislation the following year owed much to this very effective evaluation and its use of international standards, its readiness to

---

<sup>21</sup> See Canada, (Senate) *Canadian Security Guide Book 2007*, Chapter 5 – Problem 7 "Slow Progress in Information Sharing."

<sup>22</sup> Avis, *Canadian Maritime Domestic Security*. p. 7. Peter Avis has since retired from government but remains active in the academic community that focuses on national security. See also Captain(N) Peter Ellis "Walking the Talk? Implementation of the 2004 National Security Policy," A Paper Prepared at the Canadian Forces College, (26 May 2008), footnote 105.

<sup>23</sup> Canada, Finance Canada, *Year Five Evaluation of the National Initiatives to Combat Money Laundering and Interim Evaluation of Measures to Combat Terrorist Financing FINAL REPORT*, (Ottawa: Finance Canada (Report prepared by Ekos Research), 30 Nov. 2004), p. v.

<sup>24</sup> The comparison countries were the United Kingdom, Australia and the United States. See Finance, *Year Five Evaluation*, Annex A, Appendix I.

<sup>25</sup> Finance, *Year Five Evaluation*, Annex A, p. 4 of 20.

<sup>26</sup> Finance, *Year Five Evaluation*. p. 44.

<sup>27</sup> Canada, *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, (2006), Article 55(7).

tackle legal detail, and its meaningful engagement with other data-sharing partners. Note, however, that legal concerns still deny other agencies direct access to the FINTRAC database and the most rapid method of “connecting the dots.”

### **Strategic Problems**

Regrettably, the revisions to the money laundering legislation represented one of the rare indicators of federal data sharing progress. There could be many more; however, one would be more likely to accept that my examples of current airport, maritime and money tracking shortcomings are isolated examples if one had a sense that the overall federal security architecture was well designed and highly coordinated.

This is not the case. Today, no system links all the federal players within a secret network. As far back as 2004, Public Safety Canada advertised their “Public Safety and Security Information Sharing and Interoperability” project that would include all the new national security players and traditional law enforcement agencies within such a system.<sup>28</sup> By 2007 their Report on Plans and Priorities had downgraded this project to a more modest effort that would develop a “framework for interoperability” and “long range vision.”<sup>29</sup> Given that, the needed secure data connectivity between departments is likely years away; as with the equally stalled marine MIMDEX system, legal issues are apparently involved.<sup>30</sup>

Similarly, the problem of absentee participants in ‘whole of government’ units, like the Maritime Security Operations Centres, appears, if not widespread, relatively common. The Intelligence Service’s Integration Threat Assessment Centre (ITAC) has the task of overcoming the past “inconsistent” federal ability to “share information and conduct effective analysis” according to the Service’s website.<sup>31</sup> Yet today that site also shows it lacks the on-site participation of Citizenship and Immigration Canada despite the fact that it supported the concept in 2004.<sup>32</sup> In its response to the Auditor General’s report urging participation, Citizenship Canada explained its absence was due to “the lack of permanent funding.”<sup>33</sup> As with the case of the Maritime Security Operations Centres, the presence of every department on-site is critical given the above-noted lack of a secure network linking departments. CSIS, in particular, has had significant difficulties in communicating with others as their 2004 response to the Auditor General outlined:

The Service remains committed to working with lead agencies on interoperability, that would improve the programme from a point of view of reliability and timeliness, thus ensuring better

---

<sup>28</sup> OAG, *National Security*, 2004, Chap. 3, p. 21 - PSEPC response.

<sup>29</sup> Canada, “Public Safety and Emergency Preparedness Canada, RPP 2006-7, Section II – Analysis of Programme Activities, Emergency Management [sic] and National Security (Policing, Law Enforcement And Interoperability)” (Ottawa: Treasury Board Secretariat, 2007).

<sup>30</sup> Avis, Peter, Captain (N), “The importance of Information Sharing to the Interdepartmental Security Approach,” [WWW.frontline-canada.com](http://WWW.frontline-canada.com), July/Aug 2005, p. 33.

<sup>31</sup> Canada, CSIS, *Backgrounder No. 13 - The Integrated Threat Assessment Centre (ITAC)*, Apr. 2007. at <http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr13-eng.asp> accessed 13 Jan 2009. ITAC has replaced the Integrated National Security Assessment Centre (INSAC).

<sup>32</sup> The ITAC website FAQ only list CSIS, CBSA, Transport Canada, and the RCMP as “participating departments.” See <http://www.itac-ciem.gc.ca/fq/index-eng.asp> accessed 12 Feb 2009. A telephone inquiry confirmed, however, that Public Safety Canada had since joined as a permanent representative.

<sup>33</sup> OAG, *National Security*, 2004, Chap. 3, p. 16. As the elements of the border control functions of Citizen and Immigration Canada was passed to CBSA between Dec 2003 and April 2004, an argument could be made that all of necessary security functions dealing with immigration are now provided by the ITAC’s CBSA representative. I doubt this was the case given Immigration’s response supported the need for them to be in ITAC (then INSAC) and they claimed only a lack of funding prevented them from doing so. It is also clear from the OAG’s comments at the same page that they saw a need for both customs and immigration representation.

accuracy. The Service, which is fully automated internally, is inhibited from electronically interfacing with the recipients (the RCMP, CBSA, and Foreign Affairs) due to their inability to receive information in that format.<sup>34</sup>

Similarly, the Integrated Border and Security Enforcement Teams were also missing key representatives from other agencies prompting the Auditor General to question the perceived “discretionary” nature of participating in them.<sup>35</sup> When policy directed departments to participate in these combined teams and centres no one was monitoring and enforcing compliance.<sup>36</sup>

## SOURCES OF THE PROBLEM

### Technical Problems

In addition to compliance enforcement, this review has found problems that were blamed on inadequate budgets, bureaucratic “turf wars,” and technology. For example, the above formatting interface problems that limited CSIS’ ability to share. The Auditor General has also shown that “incompatible coding” weakened the Immigration department’s terrorist watch list system while “interoperability deficiencies” affected the processing of lost passport data.<sup>37</sup> However serious, these problems are not related to problematic or out of date “technology,” nor was the information sharing challenge beyond what today’s technology could provide: NATO’s ability to rapidly exchange secret data amongst its twenty-four militaries and the international banking system’s daily transfer of hundreds of billions of dollars with error-free confidential precision attests. Equally, the Australian Maritime Identity System extracts secret shipping, customs, immigration, and intelligence data from across their government to provide an integrated picture of its offshore area.<sup>38</sup> Further, secret-level communication across and between governments does not require exotic technology or special software. In 2006, the Canadian Forces Experimentation Centre successfully tested a world-wide multi-level encrypted digital information sharing system that ran on Microsoft Word and Outlook within Window’s Server 2003 operating system. Significantly the trial system permitted participants to restrict selected sensitive material to smaller networks within the larger secret network.<sup>39</sup>

The various technological “incompatibilities” at CSIS and Citizenship Canada, and the ongoing inability to develop both the maritime and national secure data exchanges, do not, therefore, represent technical failure. The failure is one of leadership. The 2004 Auditor General’s report agreed, and blamed, these interoperability breakdowns on “a lack of central

---

<sup>34</sup> OAG, *National Security*, 2004, Chap. 3, p.33. This was related to the problem of incomplete or erroneous terrorist watch lists for air travel.

<sup>35</sup> OAG, *National Security*, 2004, Chap. 3, p. 15-16. RCMP, *SPAWN*, p. 7 also suggests that the needed immigration officials may still be absent. However, CBSA may be providing that missing component. Doubt remains only because the initial Citizenship and Immigration 2004 response regarding IBETs indicated they were unwilling to participate because the teams’ mandate focused on “drugs and contraband.”

<sup>36</sup> OAG, *National Security*, 2004, Chap. 3, p.14 and See also Canada, *Canada’s Coastlines, The Longest Under-Defended Borders in the World, Report of the Standing Senate Committee on Defence and Security*, Chapter 5, (Second Session, 37<sup>th</sup> Parliament, Oct 2003), p 4 of 20.

<sup>37</sup> *Ibid*, p.20, 30.

<sup>38</sup> Avis, *Canadian Maritime Domestic Security*. p. 7-8. See also Australia, Customs, “Australian Maritime Identification System,” at <http://www.customs.gov.au/site/page.cmf?u=5644> accessed 12 Feb. 2009.

<sup>39</sup> Titus Laboratories, “Canadian Forces Experimentation Centre helps secure information with Microsoft RMS,” (2006) at [http://www.titus-labs.com/includes/PDF/CWID\\_Titus\\_final.pdf](http://www.titus-labs.com/includes/PDF/CWID_Titus_final.pdf) accessed 12 Feb 2009.

direction.”<sup>40</sup> This involved a failure to set cross-government data exchange standards and a failure to monitor departmental performance. One can easily trace the evolution of this failure. The Associate Deputy Minister-level Interoperability Working Group, formed in Oct 2001 to provide such leadership, “ceased to exist after June 2002” according to the Auditor General who also found “no evidence that central direction had reassigned its responsibilities elsewhere.”<sup>41</sup> Within Public Safety Canada a new “Public Safety Interoperability Directorate” attempted to provide cross-departmental guidance thereafter, but it was “defunct” by 2008.<sup>42</sup> A very much lower level group – the Interoperability and Technology Interest Group – is now in place, but it operates without mandate and given the lifespan of such groups there should be little reason to expect the long term direction the data sharing problem requires.

### **Inadequate Funding**

Agencies blamed a lack of funds for delays in the creation of one integrated centre and the failure to provide personnel for another. As with technology one is quickly given cause to question this reason for failed coordination. Essentially, both the central agencies, in this case the Privy Council, Treasury Board and Finance, and the individual departments have consistently favoured ‘bricks and mortar’ projects and personnel increases spent within narrow departmental silos, over anti-terrorism projects that crossed departmental borders and improved communications. For example, the first \$7.7 billion budgeted in 2001 went to the following:

- \$2.2 billion – Air Transport Safety including creating CATSA, hardening aircraft cockpit doors, and providing airport security zone screening and strengthening.
- \$1.0 billion – Improvements for immigrant screening, refugee claimants, visitors and a fraud-proof permanent resident card.
- \$1.6 billion – Improvements to critical infrastructure protection and the anti-terrorism force JTF-2.
- \$1.2 billion – Improve border security and crossing infrastructure.
- \$1.6 billion – Increased intelligence and police officers, marine security and improved coordination and information sharing.<sup>43</sup>

A closer examination of the last \$1.6 billion shows that only \$76 million or 0.1% of the budget went to “coordination and information sharing” and half of this figure was for Integrated Border Enforcement Teams; however, over the following seven years successive budgets raised the total anti-terrorist spending to \$9.5 billion. Moreover, there was an increase in the number of initiatives directly related to cross-government information sharing. This would include:

---

<sup>40</sup> OAG, *National Security*, 2004, Chap. 3, p.20, 30. The problem of inadequate direction and compliance monitoring can also complicate internal departmental coordination. The *Report of the Auditor General to the House of Commons, Chapter 4 National Defence –C4ISR*, (Ottawa, Office of the Auditor General, 2005 Apr.), p. 13 shows DND has significant problems with officials “bypassing” the committee structure that were put in place to coordinate technical requirements and enforce their compliance. Equally, the *Status Report of the Auditor General to the House of Commons, Chapter 4 Managing the Coast Guard Fleet*, (Ottawa, Office of the Auditor General, 2007 Feb.), p. 10-11 revealed extensive problems with that agency’s central technical direction and broad failures to ensure Coast Guard regions followed it.

<sup>41</sup> *Ibid*, p. 20.

<sup>42</sup> Interview, Peter Avis, via telephone, 19 Jan 2009 and notes held by author.

<sup>43</sup> Canada, *Budget 2001 – Budget Plan Chapter 5*. All the remaining data is from this source unless otherwise noted.

- \$32.5 million – Canadian Public Safety Information Network.<sup>44</sup>
- \$9.0 million – Public Safety and Security Information Sharing and Interoperability project.<sup>45</sup>
- \$16.2 million – Marine Security Coordination Fund that included \$7.5M for MIMDEX.
- \$38.0 million – Satellite equipment and access for multiple departments.<sup>46</sup>
- \$99 million – Real Time Identification (digitization and electronic transfer of finger prints and criminal records between departments).<sup>47</sup>

These improvements totalled \$195 million, but this still represents a very modest 2% of the \$9.5 billion allocated.<sup>48</sup> This share does not seem to recognize the overriding priority for coordination and data sharing called for by the 9-11 Commission and those appearing before the Air India Commission. It certainly does not reflect the scope of the ongoing coordination problem in Canada outlined in this paper.<sup>49</sup>

In this regard, this unbalanced allotment portends continued difficulty for systems like the Interoperability Project. Here it is hard to accept that the \$9 million allocated for a pilot project that seeks to link all the federal security apparatus' multiple stand-alone departmental systems, some of which have already consumed "hundreds of millions" in development costs, will suffice.<sup>50</sup> As a result, it is equally difficult to accept the rationale that any data sharing effort suffered due to a lack of funding.<sup>51</sup> Rather, this section demonstrates the need for strong leadership, especially in terms of prioritization, over the funds already assigned. In that sense, it matches the earlier call for better technical leadership.

### Legal Restrictions

Where this study found two coordination problems tied to funding issues and four related to technology, on eleven separate occasions institutions attributed their data sharing failures to legal restrictions. That there are significant legal safeguards is not surprising. The public is concerned over the dangers posed by the ongoing electronic assault on their privacy by both

<sup>44</sup> OAG, *National Security*, 2004, Chap. 3, p.11 and *Budget 2001* p. 4 of 14.

<sup>45</sup> OAG, *National Security*, 2004, Chap. 3, p.11 and *Budget 2001* p. 22.

<sup>46</sup> Kearney, George, LCDR, "New Approach to Maritime Security," *Frontline Magazine*, (Aug. 2004), p. 12. He also indicates the two naval-led MSOCs will cost a combined \$ 95 million. The Great Lake MSOC will cost \$18 million.

<sup>47</sup> Canada, *RCMP RPP 2008-2009 Table 10 – Major Crown Projects – RTID* at <http://www.tbs-sct.gc.ca/rpp/2008-2009/inst/rcm/rcam14-eng.asp> accessed 22 Jan 2009.

<sup>48</sup> A more generous listing could also include some elements of the integrated centres and teams. Here the linkage to improving data flow is less direct, and enforcement team funding likely included a hefty dose of funding for personnel costs. Only a few these new officers will be focused on "connecting the dots" and enforcement is likely the teams' overriding priority. Nevertheless, the centres and teams do facilitate coordination and a case could be made for an expanded list which would include some of the \$404 million assigned to MSOCs (\$113 million); the Government Operations Centre, the Integrated Threat Assessment Centre, National Risk Assessment Centre (\$113 million); and the various integrated border and national security enforcement teams (\$135 million – IBETs, \$43.5 million – INSETs). (See *Budget 2001* p. 4 and 6 of 14). The addition of the all the costs for these centres and teams raises coordination and sharing related expenses to \$599 million or 6.4 % of the total funding but this is still an inadequate share for the reasons outlined above.

<sup>49</sup> See also OAG, *National Security*, 2004, Chap. 3, p. 22.

<sup>50</sup> *Ibid.*

<sup>51</sup> For a detailed look at the problem of determining just how much money is "enough" for counter-terrorism see Frank Harvey's *The Homeland Security Dilemma: The Imaginations of Failure and the Escalating Costs of Perfecting Security*, (Calgary: CDFAI, 2006).

commerce and government, and the Arar affair undoubtedly reinforced this. A strong *Privacy Act* is unquestionably needed and this should, and does, limit the type and amount of data Canadian government agencies can transfer and share. Yet, the number of times that agencies cited the *Act* or *the Charter* as a reason for not sharing data at all has caused the experts to probe this rationale.<sup>52</sup> The Auditor General's 2004 report on national security tackled this directly:

We noted that privacy concerns were often cited as the reason why agencies could not exchange information. However, officials were not able to show us any legal opinions, specific references to legislation or judgments as a basis for that position.<sup>53</sup>

Essentially, those institutions that cited a legal problem, and were then unable to provide the OAG the specifics, failed because the legal justification that denies data exchange is non-existent. What they appear to be citing instead was departmental "opinion" according to one legal analyst.<sup>54</sup> The *Privacy Act* itself unambiguously authorizes transfers between Canadian government agencies under four situations. Its para 8(2)(a) permits so if the institution receiving data will use it for the same "purpose." Para 8(2)(b) authorizes transfer if another act, say the *Customs Act*, authorizes information release to other government bodies. The *Custom Act* does so, authorizing other institutions "access" to customs data if, for example, it "is reasonably regarded by the official to be information relating to the national security or defence of Canada."<sup>55</sup> Para 8(2)(e) authorizes transfer if the data request is from an investigative body, in writing and "specifies the purpose and the information to be disclosed." Para 8(2)(f) authorizes transfer if the two institutions engaged have an "agreement or arrangement" and the purpose of the transfer is tied to "administering or enforcing" a law. A final catch-all provision, 8(2)(m), authorizes transfer for "any purpose" if "the public interest in disclosure outweighs any invasion of privacy that could result from the disclosure."

All of this is laid out simply, clearly and without further data transfer restriction save one - the agency that first collected the data that was then shared can only collect data that pertains to its mandate. For example, Customs Canada (now CBSA) can collect customs data and share it with the Canadian Employment Insurance Commission. This Commission, in turn, can then legally use the customs data to track down and prosecute employment insurance cheats who illegally drew their benefits while living outside Canada; however, CBSA cannot launch its own independent search for employment insurance cheats.

I may have made this overly straightforward; however, in 2000 the Federal Court of Appeal upheld precisely the cross-departmental data transfer of customs data to the Employment Insurance Commission I just described. Moreover, its eight page finding is straightforward, and free of dense legalese.<sup>56</sup> That court's support for the above cited data sharing provisions of the *Privacy Act* is also clear:

The wide range of exceptions permitted under section 8(2) unquestionably attests to the intention of Parliament to allow the disclosure of personal

---

<sup>52</sup> I will not address the Charter's role in data sharing as it is accepted that Charter, in the words of the Privacy Commissioner, "omitted" the right to privacy. Protection of individual privacy is now contained in the *Privacy Act* and this is what affects data sharing. See Stoddart, Jennifer, "The Charter and Security," A Paper for the Conference *The Charter @ 25*, Montreal, Quebec (16 Feb. 2007).

<sup>53</sup> OAG, *National Security*, 2004, Chap. 3, p. 17.

<sup>54</sup> Interview, name withheld, 21 Jan 2009. Notes held by author.

<sup>55</sup> *Customs Act (1985, c. 1 (2<sup>nd</sup> Supp.))* (Act current to Dec 29<sup>th</sup> 2008) 107(4)(h). This of course, seems to contradict that earlier-cited claim that the *Customs Act* bares transfer of all data including "the name of a ship."

<sup>56</sup> [Privacy Act \(Can.\) \(Re\) \[2000\] 3 F.C. 82 \(F.C.A.\)](#)

information to persons who have no connection whatsoever with the disclosing institution and for purposes other than those for which the information was collected.<sup>57</sup>

The following year the Supreme Court upheld that decision in a unanimous ruling.<sup>58</sup>

If there are specific provisions in law for transferring information between federal agencies what, then, is the problem? Here one must acknowledge the influence of the Arar rendition as privacy advocates, like the Canadian Bar Association, have been vocal in arguing. It signals a need for greater controls before any move is made to improve data sharing within the Canadian government.<sup>59</sup>

Unsurprisingly, the Arar Commission's report correctly attacks the wholesale transfer of databases to the United States without caveat or context, leaving the FBI to sort the wheat from the chaff in an issue of deadly concern for one vulnerable Canadian citizen. As a result, Justice O'Connor recommended a better screening of transferred material, central RCMP control of its own transfer procedures, and greater care in applying caveats. He also asked for improved oversight and that these specific recommendations govern both internal Canadian and international transfers; however, he also noted the same 'connecting the dot' lessons from the Air India disaster and the 9-11 Commission that appeared at the start of this paper.<sup>60</sup> As a result he recommended the RCMP "maintain its policy of sharing information obtained in the course of national security investigations with other agencies and police departments" as long as the just-cited recommendations he offered are followed.<sup>61</sup>

The Arar case and its aftermath are not the cause or even particularly relevant factors in current Canadian data sharing failures. A more likely assessment of the cause comes from a combined Canadian-American team that studied the need to better manage North American maritime surveillance data. Their report also provided one of the rare official acknowledgements of the sharing problem and a confident assessment of its cause:

Although national laws and policies permit the sharing of information, this direction is not *routinely* being followed at the mid-level management and analyst level.<sup>62</sup>

---

<sup>57</sup> *Ibid*, para [14].

<sup>58</sup> See [Privacy Act \(Can.\) \(Re\). 2001 SCC 89. \[2001\] 3 S.C.R. 905](#). In addition Supreme Court Justice Binnie, while acknowledging the need to set a fair balance between privacy and enhanced protection, noted "the greatest threat to the rule of law is terrorism" and that in matters of security it is "absolutely necessary" for courts to show deference to state agencies because they will have better information on the case than the judges. See Schmitz, Cristin, "Courts must defer to state : leading judge," *National Post*, 21 Mar. 2005.

<sup>59</sup> Cited in Canada, Privacy Commissioner, "Submission to the Standing Senate Committee on Banking, Trade and Commerce Bill C-25" 13 Dec 2006, p. 2 of 4. Yet evidence of serious problems with data sharing among Canadian government agencies is slight. For example, the Finance Canada, *Year Five Evaluation* on its FINTRAC programme only reported one privacy complaint dealing with government data sharing, and it concerned a CBSA currency seizure. See page 43 of that evaluation.

<sup>60</sup> Canada, *Report of the Events Relating to Maher Arar – Analysis and Recommendations*, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 2006, p. 331-343.

<sup>61</sup> *Ibid*, p. 331.

<sup>62</sup> \_\_\_\_\_, Bi-National Planning Group Final Report on Canada – United States (CAN U.S.) Enhanced Military Cooperation, (Peterson A.F.B, Colorado: Bi-National Planning Group, 13 Mar. 2006), p. C-7.

The reasons for this are many. In that legal issues are involved, front line law and security officers are easily dissuaded from tackling what initially appears complex. According to one intimately engaged insider, many officials also sense that sharing information with other departments presents “high legal risks.”<sup>63</sup> A review of the near-mandatory “privacy guidelines” and “privacy impact assessments” on most government websites underline this; however, there are no postings that outline a ‘duty to share’ when national security is at stake.<sup>64</sup>

The broad image that is left on this issue is one of a government that claims that “we cannot allow organizational silos to inhibit our ability to identify and respond to threats” while simultaneously advertising it is vigorously protecting the privacy rights of Canadians.<sup>65</sup> The result of the pursuit of these conflicting goals has usually been weakening data sharing, as there has been no government direction setting the balance between security and privacy.

### **Government Direction**

Inconsistent direction has been a part of the post-2001 pattern of our management of the federal anti-terrorist response. The Auditor General made a strong case that immediately after the 9-11 attacks Cabinet, the PCO, the Treasury Board Secretariat and the Finance Department were directly engaged in crafting the national counter-terrorist response, rigorously scrutinizing the budget submissions, and reorganizing departments.<sup>66</sup> Thereafter, the attention of these central agencies seemed to diminish, and compliance monitoring ceased or was turned over to department officials and their various interagency committees.<sup>67</sup> There was, possibly, a brief resurgence from the centre of government in 2004-5 as a result of calls from both the Auditor General and Senate for an actual security policy, better coordination and data sharing, and the tasking of the Deputy Prime Minister as the leader of the national security effort. Some of these items were quickly actioned, but since that time the interest of Prime Minister or Cabinet in counter-terrorism is hard to discern in the reports of the Auditor General, the Senate Committee or the broader literature. In 2004 the Martin government issued the current national security policy, but neither his nor the Harper Cabinet ensured departments, then sent their personnel to the combined centres and enforcement teams that the policy ordered. By 2008, the position of Deputy Prime Minister had disappeared and no other Cabinet minister took up his cross-government security duties. Prime Minister and Cabinet thus continue to follow the earlier pattern in which the responsibility for coordinating departments, and ensuring their compliance, is left to the bureaucracy.

Yet this brief review shows that officials are not well suited to a pan-government coordination task like counter-terrorism that must cross and re-cross departmental borders. They are also not good at conflict management. The federal bureaucracy has certainly proven risk-averse in dealing with the problem of providing the public both privacy and security.<sup>68</sup> This conflict is accentuated as it also pits pro-privacy oriented institutions like the Justice Department and Privacy Commissioner against the departments that provide security. Moreover, inter-agency committees, the vehicle of choice in these matters, operate by consensus and are

---

<sup>63</sup> Avis, “The Importance,” p. 32. The 9-11 Commission made a similar finding “The biggest impediment to all-source analysis - to a greater likelihood of connecting the dots - is the human or systemic resistance to sharing information.” See their Chapter 13, p. 416.

<sup>64</sup> The 9-11 Commission dealt with this directly “Each agency’s incentive structure opposes sharing with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information.... There are no punishments for *not* sharing information.” See their Chapter 13, p. 417.

<sup>65</sup> Canada, , *Securing an Open Society*, p. 18 & 9. See also p. VII and 10.

<sup>66</sup> OAG, *National Security*, 2004, Chap. 3, p. 10-11.

<sup>67</sup> See also the remarks of Wesley Wark in this regard in Michelle Shephard, “Politicians, platforms barely mention security,” *the.star.com*, 5 Oct. 2008, at <http://www.thestar.com/printArticle/512022> accessed 10 Oct. 2008.

<sup>68</sup> See Finance, *Year Five Evaluation*, p. 44.

particularly ill-suited to resolving conflict. The Auditor General has also noted the need for consensus makes it difficult for them to enforce compliance.<sup>69</sup> The Senate Security Committee shared this concern and challenged the Chairman of the Interdepartmental Marine Security Working Group with “Your working group is ensuring that the regulations are developed but they are not ensuring that they are implemented.”<sup>70</sup> The Chairman of the working group then agreed, pointing out that this was the individual minister’s responsibility and it was Cabinet’s job if two ministers were involved.

This makes eminent sense. Cabinet meets above the departmental fray and should coordinate. Equally, risk taking by officials is not desirable in our Parliamentary system of government. Ministers alone have both the power and responsibility for developing policy and must, thereby, accept the risk. In addition, major decisions of public choice, like that between personal privacy or national security, are surely the responsibilities of our elected officials and not the public service. Yet, such a view necessarily returns us to the fact that Cabinet, and its support teams in the PCO, will not remain focused on any issue long. Rather, Donald Savoie has suggested that a progressive accumulation of power around the Prime Minister has created a centralized structure that can only focus on crisis response and one or two key issues. It briefly issues direction via a process he terms “governing by bolts of electricity” and then rapidly switches its attention elsewhere.<sup>71</sup> Meanwhile, the bureaucracy, denied any independence in this structure, has become timid and disinclined to provide the coherence or coordination the centre will not. In national security matters only the Auditor General and the Standing Senate Committee on Defence and Security are providing consistent high-level attention.<sup>72</sup>

## CONCLUSION

The tragedy of 9-11 and the reports of these two watchdogs have produced a steady rise in funding, manpower, and units devoted to counter terrorism; however, progress in the coordination and data sharing – the “connecting the dots” functions that will define success or failure in our terrorist response – must be assessed as weak overall and completely absent in such areas as interdepartmental secure communications.

This paper has also shown that solutions to coordination and data-sharing problems will not be found studying alleged technical or funding shortfalls. There are no such shortfalls – only a failure to set standards and correctly balance the funding already provided. Equally, claims that legislation or adverse court rulings are halting data-sharing should also be discarded. The solution lies in using the laws already available.

There will be a need for greater involvement from ministers and the PCO, but we must be realistic. One cannot expect them to shift their attention from the issue of the day and this will not always be security. Today and next month it will likely be the current financial crisis until the next crisis attracts their attention.

The very recent public involvement of the Minister of Public Safety in the unresolved 2010 Olympics security budget suggests the centre of government may now be turning its

---

<sup>69</sup> OAG, *National Security*, 2004, Chap. 3, p.14.

<sup>70</sup> Canada, (Senate) *Canada’s Coastlines*, , p 4 of 20. IMSWG was also purported to be “the centrepiece of Canada’s marine security coordination” to the obvious doubts of the Senate committee. See p. 6 of 20.

<sup>71</sup> Savoie, Donald, J. *Governing From the Center: The Concentration of Power in Canadian Politics*, (Toronto: Univ. of Toronto Press, 1999), p 303-305, 313- 317. In his follow-on work, *Court Government and the Collapse of Accountability*, (Toronto: Univ. of Toronto Press, 2008), he terms the resulting effect “government by paralysis” at p. 311.

<sup>72</sup> One does wish the OAGs’ interval between reports on security issues were shorter than four years.

attention back to security matters.<sup>73</sup> Those in and outside of government who are concerned with the current want of counter-terrorist coordination and data sharing should, therefore, view this as a rare opportunity to press for change knowing the highest levels of government will be paying attention, however briefly. Here the most obvious demand should be for the accelerated delivery of the long-promised interdepartmental secure network. Further, the Olympics should also be used to spur those departments who have been lagging in providing their personnel to the integrated enforcement teams and the integrated centres. This event also provides the opportunity to insert some of the more successful initiatives from the federal bureaucracy. Here, one of the most promising is the direct involvement of legal teams into the exercises that will surely precede the Olympics. These teams have the potential of eliminating legal barriers at the source or, failing that, ensuring they get higher level governmental review. Finally, the Olympic security effort could well copy the Finance Department's use of outside consultants to independently assess the views of all sides of a security data sharing problem and then closely examine the legal issues involved. This would have the additional benefit of recording the *ad hoc* arrangements that may be made to overcome immediate data sharing problems as a result of the pressure of Olympic deadlines. An outside evaluator is more likely to record such 'fixes' and then ensure they are assessed for their potential to become permanent policy.

Beyond that our choices are slim. Positive change on this file has been based primarily on either terrorist provocation or public outrage over Senate Committee and Auditor General reports; however, these watchdogs can only be effective if academia, the media, and the concerned public are familiar with their work and voice support. Hopefully, this paper has done just that.

---

<sup>73</sup> Curry, Bill and Jon Friesen, "Price tag for security \$1-billion, Ottawa confirms," *Globe and Mail*, (12 Feb. 2009) p. A 10.

## **Canadian Defence & Foreign Affairs Institute**

CDFAI is the only think tank focused on Canada's international engagement in all its forms: diplomacy, the military, aid and trade security. Established in 2001, CDFAI's vision is for Canada to have a respected, influential voice in the international arena based on a comprehensive foreign policy, which expresses our national interests, political and social values, military capabilities, economic strength and willingness to be engaged with action that is timely and credible.

CDFAI was created to address the ongoing discrepancy between what Canadians need to know about Canadian international activities and what they do know. Historically, Canadians tend to think of foreign policy – if they think of it at all – as a matter of trade and markets. They are unaware of the importance of Canada engaging diplomatically, militarily, and with international aid in the ongoing struggle to maintain a world that is friendly to the free flow of goods, services, people and ideas across borders and the spread of human rights. They are largely unaware of the connection between a prosperous and free Canada and a world of globalization and liberal internationalism.

In all its activities CDFAI is a charitable, nonpartisan organization, supported financially by the contributions of foundations, corporations and individuals. Conclusions or opinions expressed in CDFAI publications and programs are those of the authors and speakers and do not necessarily reflect the views of the Institute staff, fellows, directors, advisors, or any individuals or organizations that provide financial support to CDFAI.



Canadian Defence  
& Foreign Affairs  
Institute