National Defence / Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Intelligence Policy: Finding a Balance for Sharing

Major D.J. Carson

JCSP 40

Exercise *Solo Flight*

Disclaimer

PCEMI 40

Exercice *Solo Flight*

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 40 – PCEMI 40
2013 – 2014

SOLO FLIGHT

Intelligence Policy: Finding a Balance for Sharing

By Major D.J. Carson
Par le major D.J. Carson

Word Count: 5027

Compte de mots :

The Canadian Challenge

> *Security and rights are not in opposition, but are intertwined like DNA strands. Together they form part of the genetic code of modern citizenship. People around the world yearn for both civil liberties and security, and have a right to both. People come to Canada to enjoy a high level of political, economic and religious freedom. They also come to Canada to avoid the impunity and arbitrary limits on those freedoms that are, sadly, commonplace in many parts of the globe. Security and human rights are not matter and anti-matter. They are compatible, and inseparable.*
>
> - Richard B. Fadden, Director of CSIS, 2009

Canada's policies on intelligence sharing have received a great deal of attention throughout the last decade. This attention largely focused on human rights aspects surrounding the case of Maher Arar, the political sensitivity and damage to Canada's reputation from the trial of Sub-Lieutenant Delisle for supplying Top Secret Allied intelligence to Russia, and allegations stemming from reporting on Edward Snowden regarding the potential infringement by the government on privacy rights of Canadians. Canadian intelligence cooperation with the US and other key allies was criticized, and media began to question the need for such close collaboration. However, Canada has a long history of cooperating with select partners regarding intelligence collection and sharing. This tradition is a cornerstone of both past and present Canadian foreign and security policies. Through examination of Canadian policies pertaining to the sharing of intelligence it becomes clear that despite recent controversies and challenges, intelligence sharing relationships are as essential today as they were when they were first established during the Second World War. Not only must Canada maintain the ability to support its allies, these partnerships themselves must remain a policy priority for the government.

Through exploring the requirement to share, the intelligence sharing structure, and by looking at how and with whom sharing takes place it will become clear that Canada's

domestic whole of government and international intelligence sharing relationships are essential to maintaining Canadian sovereignty and security. It will also become clear that human rights and privacy for Canadian citizens, as well as the maintenance of mutual trust between allies, are factors that require continuous attention. Policies promoting and facilitating intelligence sharing not only provide Canada access to the essential information it requires to ensure the safety of Canadians, but also allow Canada to make informed foreign policy decisions. As a member of these partnerships Canada sees significant gain for a relatively low cost. Privacy and human rights concerns must be overcome in order to ensure Canada maintains access to the wealth of allied intelligence available.

The Need to Share

Intelligence sharing plays a large role in national security policy. Many Canadians believe that as part of an isolated and peaceful nation they are buffered from the effects of the increasingly global nature of terrorism. Following the 2006 terrorist attacks in London Martin Rudner, a national security professor and director of the Canadian Centre of Intelligence and Security Studies at Carleton University in Ottawa explained that most Canadians consider that they "belong to a just, highly decent society. Therefore, they simply don't understand why someone would want to attack them." [1] He indicated that "there is a very profound feeling among Canadians of, `why would anyone want to do us

[1] Canwest News Service, "Canadians Apathetic About Terrorist Threat," *Canwest News*, 4 June 2013. Last Accessed 5 May 2014. http://www.canada.com/story html?id=24981e24-4a11-40a7-9bfc-52e465b06922

harm?'"[2] However, at that same time the Government of Canada (GoC) and the Public Safety Minister were telling Canadians that they were not only unprepared for a terrorist attack, but were not immune from the scale of attacks seen in London, Madrid, and New York.[3] Canada's perceived geographic isolation from the world's crisis, and proximity to the US had led to "passivity towards national security in general, and intelligence in particular."[4] Given the changing international security environment this was a dangerous viewpoint that the GoC has been working to correct.

Not only is Canada a target, but it has felt the effects of international terrorism through events such as the Air India bombing, the 1985 attack on the Turkish embassy in Ottawa, through Canadians killed in 9/11, and due to individuals such as Ahmed Ressam, who used Canada as a point of entry to the US while attempting to commit a terrorist act. As of 2013 Public Safety believed that the threat not only remained, but had increased for Canada, and towards Canadian interests globally.[5] The 2006 arrest of the 'Toronto 18' while training to carry out a series of coordinated attacks in Canada; the 2010 'Project Samosa' arrest of three men in Ontario for activities related to the production of IEDs; and most recently the 2013 arrest of two men planning to attack a VIA train bound for Toronto are all key examples of the increased threat to Canadians.[6][7][8] A key factor in each

---

2 Canwest News. *Canadians Apathetic*…

3 Ibid.

4 Andrew D. Brunatti, "The Architecture of Community: Intelligence Community Management in Australia, Canada, and New Zealand." *Public Policy and Administration 2013,* vol 28:119. Sage Publications (26 November 2012). 135. http://ppa.sagepub.com/content/28/2/119

5 Public Safety Canada, "Building Resistance Against Terrorism: Canada's Counter-Terrorism Strategy." (Ottawa). 4. Last accessed 1 May 2014. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/rslnc-gnst-trrrsm-eng.pdf

6 Michelle Shephard, "Man convicted in Toronto 18 plot, Ali Mohamed Dirie, dies fighting in Syria," *Toronto Star*, 25 September 2013. Last accessed 21 April 2014.

of these instances was a link to international terrorist groups for assistance or influence. Not only have terrorist related threats been discovered in Canada during this period, but Canadians have also become global players in terrorism. Canadians were involved in the 2013 gas plant attack in Algeria, have potential links to a 2012 bombing in Burgas, and Canadians have travelled to Syria, Somalia, and other countries to participate in terrorist activities.[9] Terrorism has globalized. The 2013 Public Report on the Terrorist Threat to Canada states that "the threats Canadians face at home are most often connected with and inspired by developments in the terrorist threat abroad."[10] The increasingly global nature of the security threat means that the Canadian intelligence apparatus must monitor not only domestic threats, but must increasingly be linked with intelligence networks worldwide. It has become clear since 9/11 that the global threat environment requires states to have extensive knowledge of (intelligence on) activities outside of their areas of expertise. For this environment Canada requires a global intelligence network.

Global coverage is not possible in isolation. Despite significant investment in the Canadian intelligence community since 9/11, capacity remains vastly outweighed by demand and necessity for timely, relevant intelligence. Even the US, with massive

---

http://www.thestar.com/news/gta/2013/09/25/toronto_18_ali_mohamed_dirie_convicted_in_plot_dies_in_syria.html

[7] Ottawa Citizen, "RCMP Say Project Samosa Suspects were preparing to build IEDs," *The Ottawa Citizen*, 30 August 2010. Last accessed 15 April 2014. http://www.ottawacitizen.com/news/RCMP+Project+Samossa+suspects+were+preparing+build+IEDs/3441574/story.html

[8] CBC, "Alleged al-Qaeda Plot Against VIA Train Thwarted," *CBC News*, 22 April 2013. Last accessed 7 May 2014. http://www.cbc.ca/news/politics/alleged-al-qaeda-supported-plot-against-via-train-thwarted-1.1377031

[9] Public Safety Canada. "2013 Public Report on the Terrorist Threat to Canada." (Ottawa). Last accessed 7 May 2014. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/trrrst-thrt-cnd/index-eng.aspx; 16, 18.

[10] Public Safety Canada. *Building Resistance*…3.

collection and processing capacities, requires allies for global coverage. Further, unlike many of its allies, Canada does not have a dedicated international intelligence collection organization. Defence Intelligence (DI) and the Communications Security Establishment Canada (CSEC) cover most of this jurisdiction, with recently increased assistance from the Canadian Security Intelligence Service (CSIS).[11] According to CSIS the "sharing of intelligence and cooperation, both at the national and international levels, is essential to effectively gauge current and future threats to the security of Canada and to analyze terrorist trends."[12] The Canadian intelligence community as a whole lacks the capacity to collect, process, or analyze its own intelligence to cover the global threat spectrum.

Capacity is not the only driving force for intelligence sharing. In addition to a shifting security threat, technology has increasingly enabled global networks and has largely made national borders obsolete in threat prevention. Technology has increased the pace of information transmission and allowed cooperative security networks to warn and act almost instantaneously. Although there is likely room for further investment in Canada's intelligence community, any level of investment would not eliminate the requirement for intelligence sharing. However, a different perspective on the need for intelligence policy reform was put forward by Patrick Lennox who indicated that the shifting threat towards terrorism was neither "the lone nor the ultimate cause of the transformation" of the Canadian security apparatus post 9/11.[13] He argued that the changes in Canada were necessary due to "the country's subordinate position in relation

---

[11] Stuart Farson and Reg Whitaker. "Canada" in *PSI Handbook of Global Security and Intelligence*. Volume 1 (Westport, CT: Praeger Security International, 2008), 43.

[12] Canadian Security Intelligence Service. "Intelligence Sharing." Last accessed 15 April 2014. https://www.csis-scrs.gc.ca/bts/shrng-eng.asp

[13] Patrick Lennox, "From Golden Straightjacket to Kevlar Vest: Canada's Transformation to a Security State," *Canadian Journal of Political Science*. 40:4 (December 2007), 1022.

to the US power," or that Canada had no choice but to follow the US policy lead.[14] However, whether this factor holds as a key push for Canada's security reform or not, globalization of terrorism has made international intelligence sharing crucial for the Government of Canada (GoC) and for all of our key allies.

In addition to keeping Canada safe from well-publicized terrorist threats Canada has other requirements for intelligence. For DND timely and relevant intelligence is required to plan and support all international and domestic operations, from training and preparedness, security awareness for small peacekeeping missions, to intelligence-led operations for large-scale deployments such as Afghanistan.[15] While the Chief of Defence Intelligence carries the mandate to provide military intelligence, this cannot be achieved without a heavy reliance on both raw information and processed intelligence from key defence allies and non-traditional partners. Further, the Department of Foreign Affairs and International Trade, as well as other departments within the GoC require global SIGINT to provide intelligence to assist with strategic policy decisions.[16] Across the government various demands necessitate a robust program of international intelligence sharing.

---

[14] Ibid. 1022.

[15] The requirement for allied intelligence for DND can be seen given the potential for rapid change in security for Cdn personnel with small UN missions in areas such as South Sudan. Canadian peacekeepers operate in remote areas and intelligence regarding the situation and intention of the population and insurgents on the ground is essential for all security, especially given a lack of intelligence integrated into UM missions. See article on rapid change in Sudan situation. http://www.aljazeera.com/video/africa/2014/04/survivors-recount-horrors-s-sudan-attack-201442011955498901.html

[16] Communications Security Establishment Canada. *What We Do.* (Ottawa). Last accessed 5 May 2014. http://www.cse-cst.gc.ca/home-accueil/inside-interieur/what-nos-eng html

The Canadian Intelligence Sharing Network

Intelligence within Canada comes from a number of distinct players who have worked increasing efficiently throughout the last decade due to changes in policy, and the demands of a changing environment. While policy reform in Canada has not been as comprehensive as that seen in the US structure post 9/11, the domestic intelligence community in Canada has progressed considerably. The Macdonald Commission of 1981 resulted in the first push towards increased control of the Canadian intelligence community by recommending a civilian intelligence agency separate from policing.[17] This was achieved in 1984 when the CSIS Act created CSIS and two review bodies, the Security Intelligence Review Committee (SIRC) and the Inspector General (IG) for review and compliance. Although the pace of change in the community slowed throughout the 1990's, like most Western governments Canada reacted to 9/11 by reviewing and adapting its existing intelligence legislation. For Canada this meant adopting robust new legislation and increased funding to the intelligence community. Change was quick and encompassing through Bill C-36, which saw the approval of a number of reforms which had been languishing. At the very senior level the reaction included establishment of a Cabinet Security Committee, something which had been lacking throughout the 1990s. Although this later faded to a standing Deputy Minister level Interdepartmental Committee on Security and Intelligence, the period of senior level

[17] Justice D.C. McDonald, "Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police," (Ottawa 1981). Last Accessed 7 May 2014. http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm

focus allowed for significant progress.[18] Legislation was backed financially by over $8 billion in new security spending, over $1.6 billion of which was on intelligence and policing, something particularly significant given the lack of previous political planning or budget forecasting for this initiative.[19] Bill C-36 created the Security of Information Act, brought key changes to the Communications Security Establishment including recognition of its mandate, and most importantly for intelligence sharing included provisions on the disclosure of information.[20] Although titled the Canadian Counter-Terrorism Act, due to its scope Bill C-36 constituted the basis for a Canadian National Security Act and brought Canada into the 21st century for security legislation.[21] However, although Canadian national security policy changes since 9/11 appear as direct responses to the attacks themselves and to a changing security environment following the debut of the Global war on Terror, some authors believe that Canada's policies were more of an evolution then a revolution, and that 9/11 was merely used as a catalyst to approve a number of already planned changes.[22] The fact that Bill C-36 was an omnibus bill supports this theory. These authors believe that the changes caused by the post-Cold War environment, accelerated by the events of 9/11, were what ultimately led to growth of the intelligence community in Canada, and to Canada's expanded international intelligence sharing partnerships.[23]

---

18 Farson and Whitaker. 27.
19 Farson and Whitaker. 28.
20 Parliament of Canada, Bill C-36 (Ottawa. 2001). Last accessed 7 May 2014. http://www.parl.gc.ca/HousePublications/Publication.aspx?Pub=Bill&Doc=C-36&Language=E&Mode=1&Parl=37&Ses=1
21 Farson and Whitaker. 29.
22 Ibid. 21.
23 Ibid. 21.

Domestically, a second round of policy change came in 2004 when Canada began to work towards a much more integrated domestic security environment through Prime Minister Martin's "Securing an Open Society." Intelligence sharing and integration were primary themes of this policy: reducing "institutional boundaries within the federal government; jurisdictional boundaries within Canada, federal, provincial, and municipal; and internationally between allies and within the framework of international institutions and multinational agreements."[24] Overall, the results of this integration were seen through the development of a number of integrated threat assessment centers. The largest example of this increased domestic intelligence cooperation came through the development of the Integrated Terrorism Assessment Centre (ITAC), which includes representation from all key federal intelligence agencies, and maintains linkages into provincial partnerships. ITAC uses intelligence sharing from key partners to develop threat assessments, and to distribute threat warnings across all levels involved in Canadian security, including first responders.[25] This center brought previously inaccessible vetted security intelligence to provincial and even municipal levels, providing awareness and allowing for better preparation for potential security threats.

Although legislation has played a large role in facilitating increased intelligence sharing between the federal, provincial, and even municipal players, security for events such as Vancouver 2010 and the G8/G20 summits provided a real world push and testing for domestic intelligence sharing.[26] Intelligence sharing during these events, and through ITAC is not flawless, but as steps toward enabling the seamless sharing of essential

---

[24] Farson and Whitaker. 36.

[25] Integrated Terrorism Assessment Centre (ITAC). Last accessed 1 May 2014. http://www.itac.gc.ca/ntrntnl_cprtn/index-eng.asp

[26] Farson and Whitaker. 40.

information for domestic security they have been hugely successful. One key component to this success is the ability of agencies to share information while still preserving departmental mandates and collection methods. This is an issue which is much more complicated in the international sharing of intelligence.

The 'Away' Team: Canadian Intelligence Sharing Partnerships

Although there have been significant improvements in Canada's domestic intelligence sharing, international intelligence sharing has also seen change. Canada is part of a number of military and security partnerships that have existed and strengthened since World War II, some of which include legal obligations for sharing. As a nation with a relatively small intelligence collection capability Canada's major sources of intelligence are foreign security and intelligence agencies. "The largest suppliers of such information are agencies of countries with whom Canada is closely allied. Even if [Canada] had its own secret intelligence service working abroad, there would still be a need for agreements with foreign agencies."[27] Canada has always been, and will always be, a net importer of intelligence. This requires strong partnerships.

The cornerstone of Canada's international intelligence cooperation is through the 'Five Eyes' Intelligence Community. This long-standing partnership with Australia, New Zealand, the United Kingdom, and the United States has been referred to as "the most exclusive intelligence sharing club in the world."[28] Canadians were generally unaware of

---

[27] Justice D.C. McDonald. *Second Report – Volume 1, Freedom and Security Under the Law*, 632.

[28] James Cox. "Canada and the Five Eyes Community," *Strategic Studies Working Group Papers*. (Canadian International Council: December 2012), 4.

the extent of Canada's dependency on the Five Eyes partnership until the recent Delisle espionage incident. However, due to media coverage awareness has grown. Media speculated that the case had done irreparable damage to Canada's position as a trusted partner in the 'Five Eyes' community.[29] Canada's role in the community has also received significant attention through the release of documents by Edward Snowden, which focused on the privacy and human rights risks of intelligence sharing partnerships. These recent cases highlight that trust between partner nations is as important for the government as balancing ensuring privacy and human rights for Canadians.

The 'Five Eyes' relationship began as a second world war signals and cryptology cooperation between the UK and US, and grew to its present state throughout the Cold War.[30] This arrangement lacks an overarching governance body, but allows each state to operate within its own domestic legal and policy framework. This potentially has a disadvantage for members in that without a formal structure there is no legal assurance of how any information provided will be ultimately used. Once information is passed to a Five Eyes partner there is no guarantee that any specific originator dissemination caveats will be enforced. However, this is a relationship built on a history of mutual trust. This relationship is not limited to a specific government sector or department. The partnership began and continues with signals intelligence via Canada's Communication Security Establishment (CSEC) but is equally strong with national assessments community through the Privy Council Office, and in the defence intelligence community through the

---

[29] Ibid. 4. See also The Canadian Press, "Navy Spy Scandal prompted US to increase oversight of Canadian Military Intelligence," *The Toronto Star*, 27 May 2013. Last accessed 5 May 2014. http://www.thestar.com/news/canada/2013/05/27/navy_spy_scandal_prompted_us_to_increase_oversight_of_canadian_military_intelligence_sources.html

[30] USA, National Security Agency, *British-US Communications Intelligence Agreement*. 5 March 1946. http://www nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf

Chief of Defence Intelligence (CDI). Each Canadian intelligence player works with their respective partner organizations across the community.[31] With the relatively recent expansion of the security field the relationship has extended to newer intelligence realms such as finance and transportation, and to the more tactical levels of law enforcement.

Sharing also takes place through partnerships such as North American Aerospace Defence Command (NORAD) and the North Atlantic Treaty Organization (NATO). NORAD was developed on the premise of joint aerospace defence - which requires intelligence sharing - and remains a legal agreement for open sharing between both governments at the strategic level, and both militaries operationally.[32] The NATO partnership is also a formal relationship based on and working towards increased intelligence sharing. Spelled out in NATO's 2010 Strategic Concept is the goal of "enhance[ing] intelligence sharing within NATO, to better predict when crises might occur, and how they can best be prevented."[33] However, while the Five Eyes community links into all intelligence players in Canada, the NATO and NORAD sharing arrangements largely partner with Defence Intelligence.

Outside of traditional partnerships the changing nature of national security - with an increased emphasis on extremism from North Africa and the Middle East - has led Canada to establish partnerships for intelligence sharing with non-traditional allies.[34] Emerging relations require Canada to be even more careful with the risk to human rights as each of these countries may balance security and individual freedoms differently than

---

[31] Cox. 8.

[32] USA. North American Aerospace Defense Command. *History*. Last Accessed 7 May 2014. http://www norad mil/AboutNORAD/NORADHistory.aspx

[33] NATO, "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization," Lisbon, 19-20 November 2010. 21. http://www nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

[34] Public Safety Canada. *Building Resistance...* 12.

Canada. Additionally, there are also advocates for intelligence collection and sharing within larger organizations such as the UN.[35] Although Canada operates under the assumption that information and awareness are essential for operations, there are a number of concerns with UN-wide intelligence sharing that make this development unlikely.[36] Given the open nature of the UN, information is only likely to be shared by the key intelligence producing countries in cases of a serious and imminent risk to the direct safety of UN personnel, or selective sharing.[37] As a net importer of intelligence Canada would be limited in its ability to share intelligence with organizations such as the UN. Smaller partnerships allow Canada to maintain more control and trust regarding the use of Canadian intelligence. When it comes to sharing relationships it is clear that more exclusive is better, and Canada is currently well placed to gain from membership in the essential clubs.

---

[35] Walter Dorn, "Intelliegnce-Led Peacekeeping: The United Nations Stabilization Mission in Haiti (MINUSTAH), 2006-07," *Intelligence and National Security*, vol 24, no 6. December 2009. Last accessed 2 May 2014, http://walterdorn.net/pdf/Intelligence-LedPkg-MINUSTAH_Dorn_INS_Dec2009.pdf

[36] Traditional intelligence sharing with the UN is unrealistic: given the size and diversity of the UN membership, classified information passed to it as a whole would become too widely distributed to trust that it would be controlled. With most UN members being net importers of intelligence, like Canada, there is little incentive for key producers of intelligence to share within the UN structure, with little hope of control over their intelligence once shared, and little return.

[37] During Colin Powell's presentation to the UN Security Council on WMDs in Iraq, he stated clearly that "I cannot tell you everything that I know." Washington Post, "A Policy of Evasion and Deception," *The Washington Post Company* (3 February 2003.) http://www.washingtonpost.com/wp-srv/nation/transcripts/powelltext_020503.html

Challenges to Intelligence Sharing Policy

Privacy

Despite the necessity for intelligence sharing there are several factors which must be overcome. In order to gain popular public support for the continued necessity of intelligence sharing partnerships, it is essential to understand the balance between security concerns and challenges to individual privacy and human rights for Canadians, and the necessity for mutual trust for partner nations.

Rapid advances in technology that enabled the globalization of security threats have complicated the privacy environment for the GoC. The technical capacity for surveillance has grown significantly for both governments and corporations, aided by a surge in social media and open-source personal information available online. This information has become an easy target for intelligence agencies, and according to the Canadian Privacy Commissioner it "has the potential to become the predominant collection channel."[38] One of the major challenges for Canada has been the balance of trying to create an effective national intelligence establishment while preserving the civil rights and freedoms of the citizens it is designed to protect. Although various organizations play a role in intelligence collection, CSEC has the largest role in the privacy debate.

---

[38] Privacy commissioner special report. 3.

CSEC has been the focus of media scrutiny related to privacy due to documents leaked to the press in the US by Edward Snowden. These reports accuse CSEC of cooperating with the US National Security Agency (NSA) in the mass collection of unwarranted data from Canadians.[39] However, former CSEC director John Adams argues that legislatively "what CSEC can and cannot do is carefully detailed and circumscribed by law, Ministerial Directives, Ministerial Authorizations, and policies."[40] Routine foreign collection is based on well-established policies covering the bulk of CSEC work. In cases where a foreign target is in contact with a Canadian, collection is governed based on special provisions in legislation provided by Bill C-36. One key provision surrounding this collection requires that "satisfactory measures [be] in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security."[41] Further, collection on Canadian targets must be reviewed and approved by the MND.

Privacy is also safeguarded by the oversight of a Commissioner for CSEC, a retired judge with clearances to monitor and a mandate to report on collection activity. The Commissioner reports annually and provides recommendations to ensure that policy keeps pace with the rapid growth in activity and technological ability of the CSEC organization. In his 2012 report to Parliament the Commissioner indicated that the privacy of Canadians is further protected by the culture within CSEC. He outlined that "CSEC's Chiefs, during [his] time as Commissioner, [had] spared no effort to instill

---

[39] Canadian Broadcasting Corporation. "CSEC Used Airport Wi-Fi to Track Canadian Travellers: Edward Snowden Documents," *CBC online*. 31 January 2014. http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

[40] John Adams, "Terrorism, The Internet, and the Security/Privacy Conundrum," *Strategic Studies Working Group Papers*. (February 2014). 7.

[41] Adams. 7.

within CSEC a culture of respect for the law and for the privacy of Canadians."[42] To counter the belief that allies could assist with domestic monitoring Adams asserts that international partners cannot be used circumvent Canadian laws to carry out activities which are not legally permitted in targeting Canadian citizens.[43] In addition to the Commissioner's annual review, the Office of the Privacy Commissioner of Canada recently provided a special report to parliament on privacy surrounding all Canadian intelligence collection activities, and agreed that "independent review mechanisms ensure […] accountability of security agencies, safeguard public trust and verify demonstrable respect for individual rights."[44] The Privacy Commissioner's main message was that transparency is the key to accountability.[45] Legally and operationally CSEC, the agency attracting the bulk of privacy concerns, appears to be well positioned to protect the privacy of Canadians.

Although government assessments indicate that CSEC works towards increasing security while protecting privacy for Canadians, Canadians need to become more aware of the changing nature of privacy. While the GoC has legislated protection of privacy rights, commercial corporations and search engines are not equally restricted, nor are foreign adversaries. The current reality is that Canadians are tracked with every search or

---

42 Robert Decary. "Communications Security Establishment Commissioner Annual Report 2012-2013," (Ottawa 2013), 4. http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/ann-rpt_e.pdf.

43 Adams. 8.

44 Office of the Privacy Commissioner of Canada. "Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance." (Ottawa: 28 January 2014). 3. Last Accessed 7 May 2014. http://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.pdf

45 Ibid. 4.

smart phone action, and that this information is difficult to stop at a border.[46] The US government has enacted strong legislation in the form of the US Patriot Act which renders "suspect personal email, telephone conversations and other forms of technological communication open to new levels of scrutiny in the name of security."[47] When there is legal authorization to do so Canadian intelligence organizations can also access the networks of service providers. While intelligence sharing agreements may lead some Canadians to fear for their privacy, legislation appears thorough. However, Canadians may need to reevaluate their expectation of privacy with regard to daily activities. Further, Canadians spend a significant amount of their time online, and demonstrate a greater willingness to publish and share their personal details then other Western countries. Adams indicates that the "potential for malicious activity is endless" and that the GoC is already working with industry to ensure privacy rights of Canadians through challenges to corporations such as Facebook.[48]

A final key factor in the privacy debate is that Canada is not alone in working for increased protection and assurance for intelligence sharing. Europe has similar reservations about the privacy of its citizens and the sharing of intelligence. Many European countries have much more stringent views on privacy protection then the US and have taken measures to safeguard their interests.[49] In Canada these safeguards are

---

[46] Adams. 9. (Also the source document Adams refers to here, a CNN special report) Schneier, Bruce. "The Internet is a Surveillance State," CNN, 16 March 2013. Last accessed 2 May 2014. http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance/

[47] Patrick Lennox, "From Golden Straightjacket to Kevlar Vest: Canada's Transformation to a Security State," *Canadian Journal of Political Science* 40:4 (December 2007), 1023.

[48] John Adams, "The Government of Canada and Cyber Security: Security begins at Home," in *Journal of Military and Strategic Studies* (volume 14, Issue 2, 2012), 2, 9, and 10.

[49] Anna Staser-McGill and David H Gray, "Challenges to International Counterterrorism Intelligence Sharing," *Global Security Studies,* Volume 3, Issue 3 (Summer 2012), 78. Last Accessed 25 April 2014.

reflected in existing Canadian legislation such as the Canadian Security Intelligence Service Act, the Security of Information Act, the Canada Evidence Act, the Access to Information Act, and the Privacy Act. [50] Although it is increasingly important for the governments to be active in the collection of information for public safety, accountability for these organizations is vital. Unless the need to release information for security reasons outweighs the invasion of privacy, Canadian intelligence agencies are legislated and monitored to ensure privacy.[51]

Human Rights

A second area of debate surrounding the sharing of intelligence pertains to human rights. While intelligence sharing is essential to national security, there is an impression in Canadian media that sees "the fight against terrorism not as defending democracy and our values, but as attacking them."[52] This view is largely based on public cases in Canada such as that of Maher Arar, where the investigating commission found that RCMP officers had exchanged inaccurate information with the United States "that likely played a role in [Arar's] rendition by the United States to Syria and his subsequent torture."[53] However, this took place in the immediate post 9/11 environment, and there has been

---

http://eds.a.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=8618563d-db15-4f4c-8ec0-ab6dc591bfdf%40sessionmgr4005&vid=1&hid=4111

[50] Privacy Commissioner. 4.

[51] Canada. Canada Privacy Act, Section 8 (2 m) - http://laws-lois.justice.gc.ca/eng/acts/P-21/page-3 html

[52] Richard B. Fadden, "Remarks at Canadian Association for Security and Intelligence Studies (CASIS) Annual International Conference," *CSIS Website*. (Ottawa: 29 October 2009), 2. Last accessed 20 April 2014. https://www.csis-scrs.gc.ca/nwsrm/spchs/spch29102009-eng.asp

[53] Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism*. (New York, NY: Cambridge University Press, 2011), 416.

change in the Canadian intelligence community since that time. There are two elements to consider when looking at human rights abuses and intelligence sharing: information Canada provides to partners, and intelligence Canada receives.

How can Canada ensure that another instance like that of Maher Arar does not occur, or that intelligence we share will not lead to human rights violations? This relates to Canada sharing intelligence with countries that don't share our same standards of human rights. Key organizations such as NATO have human rights assurances within their mandates.[54] However, Canada cannot afford to share only with countries that share our beliefs and legal assurances. Former CSIS director Fadden indicated that "just as we have diplomatic links to countries with poor human rights records, so must there be intelligence links."[55] He held that in order to track threats across the planet, there must be intelligence sharing with those countries where human rights records may be questionable. Others echo this sentiment and believe that "newly cultivated allies in the war on terrorism offer valuable insight into groups operating in their own back yard."[56] However, in addition to building intelligence sharing partnerships, Canada has taken steps to help safeguard the information it shares with these partners.

In 2009 Public Safety Canada began developing a policy to deal with cases where there was a substantial risk that sending information to — or soliciting information from — a foreign agency would result in torture. The resulting 'Framework for Addressing Risks of Mistreatment in Sharing information with Foreign Entities' is now reportedly

---

[54] NATO Website. 6. Last Accessed 5 May 2014. http://www nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

[55] Fadden. 4.

[56] McGill and Gray. 76.

followed by a number of Canadian agencies.[57] Although not officially published, media sources reporting on it indicate that in cases where there is a risk, the matter would be referred to the responsible Deputy Minister or agency head for a decision. The Deputy Minister would then need to consider five factors:

> 1. The threat to Canada's national security and the nature and imminence of the threat;
> 2. The status of Canada's relationship with — and the human rights record of — the foreign agency;
> 3. The rationale for believing that sharing the information would lead to torture;
> 4. The proposed measures to lessen the risk, and the likelihood they will be successful — for instance, the agency's track record in complying with past assurances; and
> 5. Views of Foreign Affairs and other agencies.[58]

While this is a considerable step forward for the oversight of information passed to intelligence sharing partners, critics of this document, including media, attest that the Arar Commission recommended that information never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture.[59] However, even Justice O'Connor "underscored the importance of responsible information-sharing in protecting Canada's security."[60] Regardless, this new framework demonstrates that the government is taking human rights concerns seriously when it comes to sharing information.

---

[57] Canadian Press, "Spy Agency Ok'd to Share Information that Could Lead to Torture," *CBC News website*. 29 July 2013. Last accessed 7 May 2014. http://www.cbc.ca/m/touch/canada/british-columbia/story/1.1301989

[58] Ibid.

[59] Ibid.

[60] Fadden. 5. also found in Roach. 413.

The Arar incident also demonstrated that Canada must consider the potential consequences of the information it shares with any ally, even within the trusted Five Eyes partnership. In the Arar case Canadian officials did not pay enough attention to the accuracy of the information they released, but they also failed to consider the US use of 'extraordinary rendition,' or the practice of transporting suspects to a third country for interrogation as a result of this information. One result from this in Canadian intelligence agencies has been an increase in release and disclosure training to ensure information is reviewed prior to release.[61]

The second case to consider is whether Canada should be willing to accept intelligence potentially obtained through the use of torture. While Canada's National Security policy outlines that one of the primary reasons for security and intelligence activities is to protect Canadians and our principles, which incudes the rule of law and human rights, protection of Canadians is the priority.[62] Canada cannot ignore intelligence that could safeguard or prevent injury to Canadians despite potential abuses which may have led to its discovery. Reviews of Canada's intelligence structure over the last decade attest that despite strong pressures at home and abroad Canada managed to improve its capacity and intelligence reach "in meeting the challenge of the multi faceted threats to the security of Canada […] while not losing sight of the human rights and constitutional implications of security measures."[63] The balance of freedom and security still requires considerable attention to ensure, but the Canadian government has been successful in

---

[61] Certified 'Release and Disclosure' Officer training is now provided by the Chief of Defence Intelligence Organization. This is a trend within the organization to better understand disclosure. Author has taken this training.

[62] Government of Canada, "Securing our Open Society: Canada's National Security Policy." April 2004. 19. Last accessed 7 may 2014. http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf

[63] Farson and Whitaker. 47.

implementing a number of safeguards and checks to minimize the chances of future human rights infringements from occurring. It is essential that safeguards be in place to ensure that the activities of our agencies are appropriate and in compliance with Canadian law and policy.[64] However, a significant number of safeguards are already in place to review intelligence activities, and the addition of the new Framework is another step towards ensuring checks and balances for information sharing.

Mutual Trust

Sharing intelligence exposes countries to vulnerability due to the sensitive nature of intelligence capabilities and sources, and mutual trust between partners is essential. Loss of control over shared information can lead to anything from a failed operation to a serious threat or embarrassment for a partner government.[65] For Canada, the Deslisle case potentially weakened allied trust in Canada's ability to secure classified information. DND's initial assessment from the compromise was potential risk to its access to allied intelligence.[66] Additionally, Canada needed to improve its security practices following this incident in order to assure its partners that it was taking vulnerabilities seriously.[67] Similarly, Edward Snowden has potentially marred the US reputation for safeguarding

---

64 Government of Canada, "Securing...". 19.

65 McGill and Gray. 83.

66 Colin Freeze and Jane Taber, "Russian Mole Had Access to Wealth of CSIS, RCMP, and Privy Council Files," *The Globe and Mail*, 22 October 2012. Last Accessed 5 May 2014. http://www.theglobeandmail.com/news/politics/russian-mole-had-access-to-wealth-of-csis-rcmp-privy-council-files/article4627659/?page=all

67 Press, "Navy Spy Scandal Prompted US to Increase Oversight of Canadian Military Intelligence: Source," *The Toronto Star*. 27 May 2013. Last Accessed 2 May 2014. http://www.thestar.com/news/canada/2013/05/27/navy_spy_scandal_prompted_us_to_increase_oversight_of_canadian_military_intelligence_sources.html

Canadian secrets as Canada was forced to defend the practices of CSEC following the release of stolen documents. Although as a key producer of intelligence the US has less to lose through breaches of mutual trust, for a net importer of intelligence such as Canada protection of allied intelligence must be assured at almost any cost.[68]

Conclusion

Privacy, human rights, and mutual trust are all challenges within the intelligence sharing community that are part of a larger struggle for intelligence agencies as they adjust to the shift to digital information, and the increased vulnerability of digital files. However, longstanding relationships such as the 'Five Eyes' and NATO have proven capable weathering these challenges and have grown stronger since 9/11. The last decade has seen a significant shift in the reach and quantity of threats any nation must monitor. Terrorists now use the internet and social networking as force multiplier, allowing them to recruit, plan and execute plans globally. The National Security Policy released in 2004 highlighted three core national security interests: protecting Canada and Canadians at home and abroad; ensuring Canada is not a base for threats to our allies; and contributing to international security.[69] Two of these three represent needs for Canada to contribute internationally, and represent obligations we as Canadians have to share with our Allies. Despite significant policy challenges and progress over the last decade regarding the sharing of intelligence, the key concern for Canadians is knowing that their government

---

[68] This was clearly seen in the Charaoui security certificate case where CSIS decided to withdraw its case at potential risk to Canadians rather then reveal information to the courts which could damage the trust allied intelligence partners had placed in the organization. As seen in Fadden. 6.

[69] http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf

will maintain a balance between protecting the privacy of citizens and ensuring national security.[70]

[70] Canada, Office of the Auditor General of Canada, "2009 March Report of the Auditor General of Canada – Chapter 1 – National Security: Intelligence and Information Sharing," 2.

BIBLIOGRAPHY

Adams, John. "Terrorism, The Internet, and the Security/Privacy Conundrum," *Strategic Studies Working Group Papers*. (Canadian International Council): February 2014.

Adams, John. "The Government of Canada and Cyber Security: Security Begins at Home," *Journal of Military and Strategic Studies*, Volume 14, Issue 2. (2012).

Bronskill, Jim. "RCMP Memo Says CSEC Helped Shape Directive on Torture," The Canadian Press. 16 July 2013. http://www.thestar.com/news/canada/2013/07/16/rcmp_memo_says_csec_helped_shape_directive_on_torture.html

Bronskill, Jim. "Harper Government Approved Military Information Sharing Despite Torture Risk," The Canadian Press. 13 April 2014. http://www.thestar.com/news/canada/2014/04/13/harper_government_approved_military_information_sharing_despite_torture_risks_memo_shows html

Brunatti, Andrew D. "The Architecture of Community: Intelligence Community Management in Australia, Canada, and New Zealand." *Public Policy and Administration 2013,* vol 28:119. Sage Publications (26 November 2012). http://ppa.sagepub.com/content/28/2/119

Canada. Canadian Security Intelligence Service. *Public Report 2011-2013*. Ottawa: 2013. https://www.csis-scrs.gc.ca/pblctns/nnlrprt/2011-2013/PublicReport_ENG_2011_2013.pdf

Canada. Communications Security Establishment Canada. *What We Do*. http://www.cse-cst.gc.ca/home-accueil/inside-interieur/what-nos-eng html Last accessed 5 May 2014.

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.

Canada. Office of the Auditor General of Canada. *2013 Spring Report of the Auditor General of Canada*. Ottawa: Spring 2013.

Canada. Office of the Privacy Commissioner of Canada. "Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance." (Ottawa: 28 January 2014). Last Accessed 7 May 2014. http://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.pdf

Canada. Parliament of Canada. *Bill C-36*. Ottawa: 18 December 2001: http://www.parl.gc.ca/content/hoc/Bills/371/Government/C-36/c-36_4/c-36_4.pdf

Canada. Privacy Act. http://laws-lois.justice.gc.ca/eng/acts/P-21/page-3 html Last accessed 5 May 2014.

Canada. Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. Ottawa: Canada Communication Group, April 2004. http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf

Canada. Public Safety Canada. *2013 Public Report on the Terrorist Threat to Canada*. Ottawa: 2013. Last Accessed 16 April 2014. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/trrrst-thrt-cnd/index-eng.aspx

Canada. Public Safety Canada. *Building Resistance Against Terrorism: Canada's Counter-Terrorism Strategy*. Ottawa: 2013. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/rslnc-gnst-trrrsm-eng.pdf

Canadian Press, "Spy Agency Ok'd to Share Information that Could Lead to Torture," *CBC News website*. 29 July 2013. Last accessed 7 May 2014. http://www.cbc.ca/m/touch/canada/british-columbia/story/1.1301989

Canadian Press, "Navy Spy Scandal Prompted US to Increase Oversight of Canadian Military Intelligence: Source," *The Toronto Star*. 27 May 2013. Last Accessed 2 May 2014. http://www.thestar.com/news/canada/2013/05/27/navy_spy_scandal_prompted_us_to_increase_oversight_of_canadian_military_intelligence_sources.html

Canwest News Service. "Canadians Apathetic About Terror Threat," *Ottawa Citizen*, 4 June 2006. Last Accessed 29 April 2014: http://www.canada.com/story.html?id=24981e24-4a11-40a7-9bfc-52e465b06922

Cox, James. "Canada and the Five Eyes Community," *Strategic Studies Working Group Papers*. (Canadian International Council: December 2012).

Decary, Robert. *Communications Security Establishment Commissioner Annual Report 2012-2013*. http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/ann-rpt_e.pdf

Dorn, Walter A. "Intelliegnce-Led Peacekeeping: The United Nations Stabilization Mission in Haiti (MINUSTAH), 2006-07," *Intelligence and National Security*, vol 24, no 6. December 2009. Last accessed 2 May 2014, http://walterdorn.net/pdf/Intelligence-LedPkg-MINUSTAH_Dorn_INS_Dec2009.pdf

Elcock, Ward. Speech, Canadian Association for Security and Intelligence Studies (CASIS) Annual Conference, Vancouver, BC, October 16-18, 2003. Canadian Security Intelligence Service website, Last accessed 10 April 2014, https://www.csis.gc.ca/nwsrm/spchs/spch17102003-eng.asp

Fadden, Richard B. "Remarks at Canadian Association for Security and Intelligence Studies (CASIS) Annual International Conference," *CSIS Website*. Ottawa: 29 October 2009. Last accessed 20 April 2014. https://www.csis-scrs.gc.ca/nwsrm/spchs/spch29102009-eng.asp

Farson, Stuart and Whitaker, Reg. "Canada" in *PSI Handbook of Global Security and Intelligence*. Volume 1, Westport, CT: Praeger Security International, 2008.

Freeze, Colin. "Canada's Little-Known Spy Agency Comes Out Into the Open," *The Globe and Mail*, 22 December 2010. Last Accessed 7 May 2014. http://www.theglobeandmail.com/news/national/canadas-little-known-spy-agency-comes-out-into-the-open/article4260580/?page=all

Freeze, Colin. "Five-Eyes Intelligence Sharing Program Threatens Canadians Abroad, Watchdog Warns," The Globe and Mail, 31 October 2013. http://www.theglobeandmail.com/news/politics/five-eyes-intelligence-sharing-program-threatens-canadians-abroad-watchdog-warns/article15199925/

Freeze, Colin. "Tip from US was needed to kick start Delisle Probe," *The Globe and Mail,* 29 November 2013. Last Accessed 15 April 2014. http://www.theglobeandmail.com/news/national/tip-from-us-was-needed-to-kick-start-delisle-probe/article5831230/;

Lennox, Patrick. "From Golden Straightjacket to Kevlar Vest: Canada's Transformation to a Security State," *Canadian Journal of Political Science* 40:4 (December 2007).

Roach, Kent. *The 9/11 Effect: Comparative Counter-Terrorism*. New York, NY: Cambridge University Press, 2011.

Schneier, Bruce. "The Internet is a Surveillance State," CNN, 16 March 2013. Last accessed 2 May 2014. http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance/

Staser McGill, Anna-Katherine and Gray, David H. "Challenges to International Counterterrorism Intelligence Sharing," *Global Security Studies,* Volume 3, Issue 3 (Summer 2012). Last Accessed 25 April 2014: http://eds.a.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=8618563d-db15-4f4c-8ec0-ab6dc591bfdf%40sessionmgr4005&vid=1&hid=4111

United States of America, National Security Agency, *British-U.S. Communication Intelligence Agreement*. (March 1946). Last Accessed 7 May 2014. http://www nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf

Washington Post, "A Policy of Evasion and Deception," *The Washington Post Company* (3 February 2003). Last accessed 5 May 2014. http://www.washingtonpost.com/wp-srv/nation/transcripts/powelltext_020503 html