CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 32 / CCEM 32

EXERCISE NEW HORIZONS

"NEED TO KNOW" TO "NEED TO SHARE": HOW TERRORISM IS CHANGING THE INTELLIGENCE COMMUNITY'S CULTURE

By /par
Major W.J. Borys

This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.

La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.

Table of Contents

Introduction

The terrorist events in the United States (US) of September 11, 2001,[1] alerted the most powerful nation on earth that it was vulnerable to a threat that had been emerging against its citizens for some time. Despite the shock that the attacks created, US intelligence officials knew the threat of such an attack. The 9/11 Commission conducted a thorough investigation into the events of 9/11 and linked them primarily to systemic weaknesses within the US intelligence community. The 9/11 Commission found that the intelligence community had knowledge about plots regarding aircraft, the CIA knew that two of the hijackers were in the US but did not inform the FBI in time, and if the FBI had worked with the National Security Agency, these two hijackers could probably have been found.[2]

The intelligence agency within the US that was responsible for protecting America against terrorism was, and still is, the Federal Bureau of Investigation (FBI). The FBI was not well known for its terrorism responsibilities for main two reasons. First of all, the FBI has primarily a domestic focus, and since most terrorist attacks against American citizens were perpetrated outside of the US, the FBI played a minor role in dealing with these incidents.[3] Second, the FBI has become a law enforcement organization, with the inherent mindset of collecting evidence to solve crimes that have happened in the past, rather than collecting intelligence to prevent atrocities from happening in the future. This mindset was acceptable when hijackers saw aircraft as targets, and hijackers could be negotiated into agreements that did not kill innocent

[1] Referred to as "9/11" throughout the rest of this paper.
[2] M.E. Bowman, "Information at Risk," *American Intelligence Journal* (Autumn/Winter 2005): 47.
[3] Arthur S. Hulnick, "U.S. Intelligence Reform: Problems and Prospects," *International Journal of Intelligence and CounterIntelligence,* vol. 19, no. 2 (Summer 2006): 313.

civilians. However, this mindset was no longer appropriate in a post-9/11 world where hijackers can turn aircraft into weapons and render post-hijacking negotiations useless.[4]

The US intelligence community consists of fifteen different agencies working in various government departments. These fifteen agencies can be generally grouped into the two categories of national security and law enforcement. The 9/11 Commission stressed that these organizations needed to effectively work together to prevent future terrorist attacks. The fact that the 9/11 hijackers immigrated into the country (US Immigration responsibility), learned to fly within the regulated aviation community (FAA responsibility), were affiliated with terrorists (CIA and FBI responsibility) and were funded from outside sources (US Treasury responsibility) shows how multidimensional the threat is to the national security agencies of not only the US, but any country dealing with transnational terrorism. Coupled with the fact that the Islamic culture and language are only understood by a small group of individuals within these agencies, Islamic terrorism is essentially an alien threat faced by the US intelligence apparatus.

The Bush administration has acted upon many of the recommendations of the 9/11 Commission. Since the 9/11 Commission identified terrorism as the single most important threat facing the US, the US government has begun to reorient its intelligence community by passing the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[5] Despite being criticized as placing too much attention upon a single threat, the vast scope of the US intelligence community reorganization has caused a member of the CIA's Senior Executive Service to state,

[4] Sergio Koc-Menard, "Australia's Intelligence and Passenger Assessment Programs," *International Journal of Intelligence and CounterIntelligence,* vol. 19, no. 2, (Summer 2006): 218.
[5] Robert D. Vickers, "The Intelligence Reform," *International Journal of Intelligence and CounterIntelligence,* vol. 19, no. 2, (Summer 2006): 357.

> …terrorism is clearly the most compelling immediate threat to U.S. security, and will require considerable additional resources. It requires sifting through a massive volume of often dubious information, looking for links, patterns, and clues of specific attacks. The collection and analysis challenges are enormous, as is the counterintelligence problem. Counterintelligence is particularly frustrating in an environment where it is almost impossible to check the credibility of sources and information, and the process is both expensive and time consuming. It takes skills not in the mainstream of intelligence priorities for decades….[6]

Given the breadth of government resources required to combat Islamic based terrorism, some of which are extremely scarce, this paper will demonstrate why the US government must shift from its "need to know" intelligence culture to one of "need to share." This is the most expedient way that the US can exploit its limited Islamic terrorism intelligence resources and its established relationships with allies. The paper will start by addressing the reasons that have prevented the sharing of information within the US intelligence community in the past. Then to prove the assertion that the US intelligence community must shift from a "need to know" to "need to share" paradigm, the discussion will move to the needs and benefits of information sharing between government agencies, and with industry. The paper will also examine some information technology tools that improve information sharing, and it will close by considering the need for information sharing between the nations in North America.

The "Need to Know" Intelligence Culture

Although governments have maintained secrets for a very long time, the current US government areas of interest that necessitate secrecy are those that effect national security: the military, foreign policy, vulnerabilities, and weapons of mass destruction.[7]

[6] Vickers, "The Intelligence…," 363.
[7] Bowman, "Information…," 46-47.

The reason why secrecy is an important tool within national security circles is the nature of geopolitics.

> In theory, intelligence systems collect, analyze, and disseminate information on behalf of decisionmakers engaged in protecting and advancing a state's interests in the international system. This process is inherently competitive and secretive, even among allies, because the international system is essentially one of self-help and anarchy. Particularly when the international system is multipolar and fluid, "friendships" between governments do not endure and coinciding interests at one moment easily diverge at the next.[8]

In an attempt to reduce the disclosure of sensitive material, President Eisenhower established the concept of the "need to know" principle in Executive Order 10501.[9] The "need to know" principle minimizes the number of people within an already trusted group – those successfully screened to be sufficiently trustworthy – to have access to national security information. Another impediment to information sharing between intelligence agencies is the varying methodologies used by each agency to conduct their personnel security screening process. As a result of these variances, each intelligence agency does not necessarily respect the security levels of the others.[10] The CIA in particular is the only agency to use a polygraph in its screening process.[11] As a result, individuals in other agencies may have a "need to know," but are not cleared to know. Both of these impediments to information sharing build upon a culture within the intelligence community that emphasizes the protection of information, not people.

[8] Jennifer E. Sims, "Foreign Intelligence Liaisons: Devils, Deals, and Details," *International Journal of Intelligence and CounterIntelligence* vol. 19, no. 2 (Summer 2006) 196.

[9] Bowman, "Information…," 46.

[10] Vickers, "The Intelligence…," 362.

[11] Douglas Hart and Steven Simon, "Thinking Straight and Talking Straight: Problems of Intelligence Analysis," *Survival* vol. 48, no.1 (Spring 2006): 42.

As a result of the inherent information protection mindset of the intelligence community in the US, the events of 9/11 were not the only time the US has been attacked when its intelligence community knew an attack was imminent. Just like the time period before 9/11, US intelligence (Navy in this particular case) had in 1941 intercepted signals intelligence (SIGINT) indicating that the Japanese were about to attack the US. However, the information was insufficient to discern the attack location, preventing the conversion of the information into actionable intelligence. Because the US Navy intelligence agency wanted to keep its ability to intercept and read Japanese military messages secret, and the intelligence alerting of a Japanese attack was considered inactionable, the US Navy intelligence deemed that the US President did not have a "need to know" and therefore he was never made aware of the potential threat.[12]

Harry S. Truman was aware of the many lives lost due to the lack of proper exploitation of intelligence information during World War II and was very dissatisfied with the general lack of coordination within the US intelligence community. This lack of coordination resulted in intelligence information from various US intelligence agencies being directly delivered to the President for synthesis. In 1946, Truman created the Central Intelligence Group (which became the Central Intelligence Agency (CIA), "to avoid 'having to look through a bunch of papers two feet high' and instead receive information that was 'coordinated so that the President could arrive at the facts.'"[13] In effect, President Truman was attempting to force information fusion within the US intelligence community. Immediately upon creation of the CIG, security units from the various US government departments refused to hand over 'their' information to the CIG

[12] Loch K. Johnson, "A Centralized Intelligence System: Truman's Dream Deferred," *American Intelligence Journal* (Autumn/Winter 2005): 6.
[13] Johnson, "A Centralized…," 6-7.

for the creation of the *Daily Summary* (later to become the CIA's *President's Daily Brief*).[14] As a result, until the IRTPA of 2004, the *President's Daily Brief* was not a synthesis of intelligence from the entire US intelligence community, but "was mostly drawn from [CIG/] CIA sources and analysis."[15]

Although there have been many attempts to centralize the US intelligence community, the new IRTPA has been criticized for failing to consolidate the community under the new Director of National Intelligence (DNI). The main complaint is that the current US intelligence community structure isolates the independent intelligence capability within the Department of Defence, resulting in a major impediment to information sharing between US intelligence agencies.[16]

Shifting Towards a "Need to Share" Culture

IMPACT OF THE THREAT

Terrorist activities are criminal acts that are characterized by military-like effects. They simply fall somewhere between national security and law enforcement and therefore are addressed by both these parts of a modern society's security apparatus, or neglected by both as they simply "falls between the cracks."

The collection and analysis of information regarding threats to a country or its citizens is the purview of the intelligence community. As eloquently stated by a past Director of the FBI, Louis Freeh, when commenting about the 1993 World Trade Center bombing, "merely solving this type of crime is not enough: It is equally important that the

[14] *Ibid*., 6-7.
[15] Hulnick, "U.S. Intelligence…," 305.
[16] Johnson, "A Centralized…," 11-12.

FBI thwart terrorism before such acts can be perpetrated."[17] Performance assessment within the FBI had a law enforcement bias – numbers of arrests, indictments, prosecutions and convictions. These metrics where easy to define and served the purposes of the local FBI field offices. Success against national priorities like counterterrorism and counterintelligence were very difficult to quantify and "often involved lengthy intelligence investigations that might never have positive … results."[18] Despite attempts to reinvigorate the FBI's counterterrorism efforts since 1976, a report to the Director of the FBI in September 2001, Robert Mueller, stated that,

> …the goal to "prevent terrorism" requires a dramatic shift in emphasis from a reactive capability to highly functioning intelligence capability which provides not only leads and operational support, but clear strategic analysis and direction.[19]

US GOVERNMENT DIRECTION

Due in part to the findings of the 9/11 Commission, President Bush has formally directed the intelligence community to share information through Executive Order 13356. This order states,

> give the highest priority to (i) the detection, prevention, disruption, pre-emption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (2) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information; [20]

[17] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report,* (Washington, D.C.: U.S. Government Printing Office, September 20, 2004), 76 [publication on-line]; available from http://www.9-11commission.gov/report/index.htm; Internet; accessed 30 March 2006.
[18] *The 9/11 Commission Report,* 74.
[19] *Ibid*., 75-78.
[20] Bowman, "Information…," 47.

The order goes on to direct agencies to "write to release" their intelligence analysis. The "write to release" concept is motivated by the desire to share information by creating records in such a way so that the information can be distributed in both unclassified and versions of varying classifications. The goal of this direction is to protect intelligence gathering sources and methods, yet improve the dissemination of collected intelligence to all agencies that require access to this information. The agencies that the President has identified as those who should have access to terrorist information are those that,

> support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.[21]

This broad access suggests that the US government realizes that dealing with the terrorist threat, whether resident or attempting to gain entry, must engage a wide range of government, public and international organizations to prevent terrorists from perpetrating their crimes. Through the 2002 National Security Strategy (NSS), President Bush stated that, "[t]o defeat this threat we must make use of every tool in our arsenal – military power, better homeland defences, law enforcement, intelligence, and vigorous efforts to cut off terrorist financing."[22] It is police, immigration officials, banks and motor vehicle departments that have a "need to know" which individuals pose a risk. Therefore there is "need to share" the names of potential terrorists with the millions of people who come into contact with potential terrorists daily. It is this focus upon use rather than intelligence

[21] *Ibid.,* 48.

[22] George W. Bush, *The National Security Strategy of the United States,* (Washington, DC: The White House, 17 September 2002): i.

information protection that stresses the need for the intelligence community to move to a "need to share" environment.[23]

Furthermore, the IRTPA has mandated the complete reciprocity of security clearances between intelligence agencies to assure access to sensitive information. If successful, this "may do more than any other single section of the reform act to improve the unity and performance of the entire intelligence community."[24]

RE-ORGANIZATION: FOSTERING INTERAGENCY TRUST THROUGH "JOINTNESS"

The 9/11 Commission suggested that the law enforcement and intelligence communities could benefit from the types of reforms that the 1986 Goldwater-Nichols Act mandated upon the US military.[25] Amongst other initiatives, the Goldwater-Nichols Act mandated that before reaching high-ranking positions, senior officers must have spent some period of duty with a different service or in a joint command. Although this initiative has the potential of narrowing the type of advice provided by these officers to executive officials, the result of broadening the experience of senior staff to reduce competition and increase cooperation was seen as a very beneficial outcome that outweighs this risk.

In an attempt to benefit from the US military's style of jointness, the IRTPA established a hierarchy amongst the US intelligence community.[26] The current

[23] Bowman, "Information…," 48-49.
[24] Vickers, "The Intelligence…," 368.
[25] *The 9/11 Commission Report,* 96 & 426.
[26] Vickers, "The Intelligence…," 360.

organization of the Director of National Intelligence (DNI)[27] is similar to that of the US Department of Defense Joint Chiefs of Staff. One benefit of this structure is that the Associate Deputy DNIs, who are functional heads of the various aspects of intelligence, staff their organizations with individuals from all fifteen US intelligence agencies.[28] Besides fostering an improvement to cooperation and a reduction to competitiveness, this initiative has already created a better representation of the US intelligence community within the *President's Daily Brief*- hopefully an early indication that the joint staffing initiative is working.[29]

One of the Associate DNI's mentioned above heads the National Counter-Terrorist Center (NCTC) and several intelligence agencies have consolidated their intelligence arms to improve the internal flow of information and to better integrate themselves into the NCTC. The Department of Homeland Security (DHS) has consolidated its intelligence gathering and analysis groups from various DHS components under the Office of Intelligence and Analysis.[30] Despite demands to create a separate security service outside of the FBI, the Bureau remains the chief domestic antiterrorism organization and has consolidated intelligence, counterterrorism and counterintelligence under the new National Security Service (NSS).[31] The head of the NSS reports directly to both the head of the FBI and the DNI. Since the CIA remains the chief international antiterrorism organization, this makes both the CIA and the FBI peers

[27] The top US intelligence official, replacing the Director of Central Intelligence who is still the head of the CIA.
[28] Vickers, "The Intelligence…," 360.
[29] Hulnick, "U.S. Intelligence…," 306-307.
[30] *Ibid*., 314.
[31] *Ibid*., 313.

in the fight against terrorism.[32] The hope is that cooperation will improve between the two organizations, and that the "old boundaries between domestic and foreign intelligence are eroding."[33] Currently, the FBI, CIA, DHS and any other intelligence agency report their antiterrorism activities to the DNI through the joint NCTC.

A "NEED TO SHARE" FRAMEWORK

The IRTPA and various Presidential directives have reorganized the US intelligence community in an effort to facilitate information sharing. This reorganization has stressed a conversion from a "need to know" culture to one of "need to share" between the various US intelligence agencies. Domestically, the US government has put in place legislation to foster a better antiterrorism intelligence system. Since the vast majority of critical infrastructure (a potential terrorist target) in the US is privately owned and operated, the US reforms have included the private sector in their new intelligence-sharing regime. Only time will tell whether these initiatives will result in the effects desired. The paper will now shift to the benefits of using information technology (IT) to facilitate a "need to share" culture.

IT as an Enabler

GENERAL

The fact that the upcoming generation of intelligence community workers are the most computer savvy generation ever makes those contemplating the potential impact of IT upon the intelligence community very optimistic. Due to a childhood and adolescence full of IT, new recruits into the intelligence community,

[32] Vickers, "The Intelligence…," 361.
[33] Hulnick, "U.S. Intelligence…," 314.

> …are fearless in their adoption of new ideas, patient when software does not perform as expected, and accustomed to relying on software tools to perform a variety of tasks, from participating in the collective environment for massive multi-user games to compiling sophisticated music videos…New intelligence recruits, educated through web research in a universe of hypertextuality, are not afraid of using advanced software solutions in their professional environments.[34]

In 1946, the main goal of President Truman's efforts to centralize US intelligence under the CIG/CIA was to fuse US intelligence sources into information the President could effectively use.[35] With technology, this goal is proving to be less elusive. Although attempts discussed above to reorganize the intelligence community are in their early stages and therefore have yet to be proven, there are many technological capabilities that can improve collecting, analyzing and exploiting available intelligence.

DATA MINING

Once given access to intelligence data, either on the Internet or intranet, the ability to mine the data can be done by tools as simple as the MicroSoft Windows search function or more powerful but still widely available search engines like Google or Yahoo.[36] The CIA and NSA are turning to commercial companies to improve the capabilities of software tools to data mine.[37]

With the vast amount of data collected by governments and industry in the areas of fingerprinting, healthcare and at border crossings, data mining of this vast source of data can very quickly increase the amount of intelligence available.[38] However, the

[34] Hart and Simon, "Thinking Straight…," 48.
[35] Johnson, "A Centralized…," 7.
[36] T. Higgins, P.A. Shakarian, and R.E. Ferguson, "No Stone Unturned: A Thorough Search for Tactical Intelligence Analysis," *American Intelligence Journal* (Autumn/Winter 2005): 62.
[37] Hulnick, "U.S. Intelligence…," 308.
[38] Heiko Borchert, "A Transatlantic Agenda for Homeland Security Co-operation," *Jane's Homeland Security & Resilience Monitor* vol. 5, no. 3 (April 2006): 14.

utilization of extensive databases collected for other purposes creates serious civil rights and personal privacy concerns. In the US, the government has acknowledged its duty, as do most democracies, to protect the privacy of their citizens. Although the President has directed the creation of an information-sharing environment with the intelligence community, Congress has mandated that the environment be created "in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[39]

INTERNET AND OSINT

The borderless characteristic of the Internet has made it the communications method of choice for many terrorist organizations. "The [I]nternet enables terrorist groups to exploit liberal Western laws ensuring freedom of speech to disseminate their propaganda without effective supervision and with little or no censorship."[40] Therefore, the various Internet communication methods from chat rooms to blogs, web pages to online news distribution, all form a relatively high quality source of open source intelligence (OSINT). However, as discussed above, one problem that exists within the US intelligence community that limits the exploitation of OSINT is the lack of linguists and those that have studied Islamic culture. With the severe shortage of intelligence experts within the US trained in Muslim languages and culture, the 9/11 Commission saw information sharing as a more efficient use of this scarce resource.[41]

Since OSINT is open to everyone, OSINT is inherently suited for the private sector to act as intelligence collectors and analysts. One of the benefits of private sector

[39] Bowman, "Information…," 47-48.
[40] Joe Charlaff, "Israeli Centre Tracks Jihadists in Cyberspace," *Jane's Homeland Security & Resilience Monitor* vol. 5, no. 3 (April 2006): 10.
[41] *The 9/11 Commission Report*, 401.

involvement is that it provides an “alternative analysis” or “multiple approach analysis” which is publicly available to any interested party. Without access to more active forms of intelligence collection, the private analysis of OSINT is not seen as a probable source of actionable intelligence, but rather a source for background information on various national security related topics that would include terrorism. James Arnold Miller proposes to create such a OSINT-based global threat monitoring network.[42] Dr Reuven Erlich has already established a ten person, Intelligence and Terrorism Information Center, funded by private contributions “to monitor and report on the activities of terrorist organizations and the countries that sponsor them.”[43] In the case of Dr. Erlich, his work is reported to provide him with,

> …a very nuanced understanding of how jihadists think. He said, ‘Anyone who is able to grasp the language and underlying messages of some of the Saudi sheikhs can understand the background that fanned the flames of hate which played a major role in bringing about the catastrophic attack on 11 September 2001. The West did not understand the undercurrents of hate in the messages coming over the Internet and Arabic TV networks, and missed the signals. It is an information war for control over public opinion and the battlefield is the media.[44]

SHARING AND ANALYSIS TOOLS AND TECHNIQUES

During the Cold War, analysis of the threat posed by the Soviet Union varied slowly over time. In contrast, terrorists and insurgents form dissimilar groups that are constantly changing. The ability to analyse these quickly evolving threats requires new analysis tools.[45] Further motivation for obtaining new analysis tools is the inexperience of those that are currently being recruited in large numbers into the intelligence community.

[42] James Arnold Miller, “Turning Open Source Data into Knowledge about Global Threats,” *American Intelligence Journal* (Autumn/Winter 2005): 76-77.

[43] Joe Charlaff, “Israeli Centre …,” 10.

[44] *Ibid*., 11.

[45] Hulnick, “U.S. Intelligence…,” 308.

These junior analysts are being used primarily for compiling current reports, which "…are essentially running summaries of what has happened, with very little emphasis upon plausible future extrapolations concerning threat behaviour, strengths and weaknesses."[46]

The concern is that there is actually a "newsroom" mentality developing in some intelligence agencies.

> In-depth speculative research is impossible due to the tempo of current reporting and discouraged because incentives are structured by results that are easy to quantify, such as the number of reports that analysts produce…As long as analysts are trained and rewarded for collecting and reporting rather than probing and predicting, the probability of catastrophic strategic asymmetric surprise will remain high.[47]

A further complication is the movement of intelligence analysis into the world of the policymaker. Paul R. Pillar, formerly of the CIA,[48] suggests that the ideal model for the relationship between the intelligence and policymaking communities is a sharp separation. The separation permits the intelligence officer to be somewhat isolated from the influence of the policymaker to permit objective analysis based upon the data collected. Certainly the policymaker has a role to suggest topics of analysis that are important to national security, but the intelligence officer must have the freedom to analyse the collected information and objectively discern what is happening or suggest what might happen. After the policymaker obtains the analysis from the intelligence officer, the policymaker must remain free to decide how best to react to the analysis. In cases where the policymaker becomes too involved in the intelligence analysis process,

[46] Hart and Simon, "Thinking Straight…," 44.

[47] *Ibid*., 45.

[48] Amongst other duties, Mr Pillar served as the National Intelligence Officer for the Near East and South Asia from 20000 to 2005.

there is a risk that the analysis will simply focus upon what the policymaker needs to justify a particular position. In the extreme, the intelligence community may be so strongly influenced by the policy community that there is a fear to share an alternative or dissenting.[49] Therefore there is a need to create an information-sharing environment that will provide the policymakers visibility into how the analysis was conducted without providing them too much power in influencing the analysts' conclusions. Technology can help create this environment.[50]

There are software tools that can expose the logic of one person's arguments to others. By capturing the structure of the ideas that led to a particular conclusion, others can assess the conclusion in detail if desired. This assessment could result in greater confidence in the conclusion, propose a dissenting view or suggest that other information is still required to complete the analysis. If further assessment is required, the reviewer can suggest where the assessment is considered weak and direct the assessors to information or share their own information. The communication engendered by this process functions as a means to create micro-societies that are interested in particular fields of analysis. These micro-societies facilitated by structured arguments and dialogues perform the roles of information sharing, peer review and mentoring, all at the same time.[51]

Another technique to share information within a micro-society is social bookmarking. This is a practice were information found on the Internet or intranet is posted to a specific webpage and described using the terminology of that specialty. This

[49] Paul R. Pillar, "Intelligence, Policy and the War in Iraq," *Foreign Affairs* vol. 85, no.2 (March/April 2006): 16-24.
[50] Hart and Simon, "Thinking Straight…," 47.
[51] *Ibid*., 49-50.

process supports information sharing by converting information from one micro-society into another. Junior analysts and outside experts benefit from knowing the type of information that is available in a particular topic area, and with the embedded e-mail information of the one who posted the information, are able to communicate with the individual thereby enlarging the collaboration effort between organizations and disciplines.[52]

Finally, blogging is a technique that shares the opinions of analysts with a wider community. Blogs facilitate peer review without the interference of official censorship. Although potentially sensational, used responsibly, blogs help avoid the pitfalls of analytical bias or groupthink by providing an avenue for expressing dissenting views. In a threat environment where the consequences of error pose a significant danger to the public at large, the expression of dissenting views plays an important role in understanding the entire situation.[53]

DISSEMINATION THROUGH INTEGRATED IT

An example of the power of intelligence dissemination is the effort to control the entry of potentially threatening individuals through a nation's ports of entry via passenger matching programs like the Advanced Passenger Information System (APIS)[54] or the Advanced Passenger Processing (APP) System. The US Transportation Security Administration program Secure Flight[55] endeavours to provide the same degree of security for domestic flights. The basic technique of passenger matching programs is to

[52] *Ibid*., 51-54.
[53] *Ibid*., 54-56.
[54] GlobalSecurity.org, "Advanced Passenger Information System (APIS)," http://www.globalsecurity.org/security/systems/apis.htm; Internet; accessed 21 April 2006.
[55] Transportation Security Administration, "Secure Flight Program," http://www.tsa.gov/public/interapp/editorial/editorial_1716.xml; Internet; accessed 21 April 2006.

compare those attempting to enter a country against a watch list. The watch list can consist of individuals who pose a particular national security threat, or the watch list can consist of suspect documentation. If the documentation is suspect, there may be a situation where the individual identified on the documentation is not the individual using it to gain entry. The fraudulent use of identification may be a sign of identity theft, which can be mitigated by the use of biometrics like fingerprinting and linking the passenger fingerprints to the Integrated Automated Fingerprint Identification System (IAFIS).[56]

In the case of the APP System used in Australia and New Zealand, passenger privacy is protected through the use of a 24/7 operations centre. When a passenger has registered to board an aircraft or disembark a ship to enter Australia or New Zealand, that person's identity documentation is scanned and the information is sent to the operations centre. Within 15 minutes, the operations centre returns a reply indicating whether immigration officials will accept the individual into the country. No reason is given, simply a decision regarding the individual's suitability for entry. As a result, no personal information is exchanged with the air carrier or ship line, who now knows that if they deliver the person to Australian or New Zealander immigration officials, the person will be denied entry into the respective country.[57]

Intelligence plays a pivotal role in creating accurate watch lists of potential terrorists. Given that any one particular nation does not have access to all the potential individuals who may try to enter their country, cooperation and information sharing

[56] Wikipedia, "Integrated Automated Fingerprint Identification System," http://en.wikipedia.org/wiki/Integrated_Automated_Fingerprint_Identification_System; Internet; accessed 21 April 2006.

[57] Koc-Menard, "Australia's Intelligence…," 218-222.

between governments is important to maximize the potential for identifying dangerous individuals.[58]

A North American Information Fusion Centre

IMPEDIMENTS TO INTERNATIONAL INFORMATION SHARING

When a nation shares any of its intelligence, the inherent belief amongst intelligence professionals is that the country has lost some of its edge over the other countries competing within the "international system…of self-help and anarchy."[59] Furthermore, the countries involved in the intelligence exchange will need to establish a counterintelligence operation in the other country to ensure that their intelligence is not used against them or their citizens.[60] The lost advantages coupled with the additional counterintelligence activity are costs that need to be considered against the gain obtained from information sharing. As a result, international information sharing tends to be more extensively used in situations where the international situation is changing rapidly, as it is in the case of transnational terrorism.[61] The complexity of sharing with groups of countries forces these exchanges preferentially along bilateral rather than multilateral lines.[62]

For similar reasons to preferring bilateral rather than multilateral information exchange agreements, countries that have engaged in large-scale internal information sharing arrangements make themselves less attractive for cooperation other countries. The country that will potentially share information with the more information integrated

[58] *Ibid*., 224-226.
[59] Sims, "Foreign Intelligence…," 196.
[60] *Ibid*., 205.
[61] *Ibid*., 197.
[62] *Ibid*., 202-203.

country is less likely to understand the consequences of how their information is going to be used, and therefore avoids the risk through non-participation.[63]

NEED FOR NORTH AMERICAN INFORMATION SHARING

Michael Tucker identified the paradox of a "lesser power neighbor to a superpower."[64] If a lesser power reduces its ability to deal with threats within its borders, then its superpower neighbour will threaten its territorial sovereignty as the superpower attempts to provide for its own security.[65] When the lesser power does make a serious effort to control threats within its borders, those threats are due primarily because of its superpower neighbor's strategic posture, rather than the inherent security needs of the lesser power. Either way, its superpower neighbor threatens the lesser power's sovereignty directly or indirectly. The security of both powers is inextricably linked and it is in the best interest of both to influence each other's policies towards their own interest. This inevitability is best achieved in a cooperative manner.

Whether is an "international system…of self-help and anarchy"[66] or it is transnational terrorism, there are forces currently discouraging and encouraging international information sharing between the countries within North America. The overall solution rests in establishing the right balance for each country. Although some encourage international information sharing,[67] others are more cautious. For example, the

[63] *Ibid*., 211.
[64] Joseph T. Jockel, *Security to the North: Canada-U.S. Defense Relations in the 1990s,* (Michigan State University Press: East Lansing, 1991), 67.
[65] United States of America, *The National Security Strategy of the United States of America,* (March 2006): 37.
[66] Sims, "Foreign Intelligence…," 196.
[67] Tim Harper, "'Fortress America' Sparks New Fears," *Toronto Star*, (March 15, 2005) [journal online]; available from http://web11.epnet.com/citation.asp?tb=1&_ug=sid+B591FC1F%2D983B%2D407E%2D80CA%2D334A6C0AB7C5%40sessionmgr3+dbs+nfh+cp+1+19B7&_us=sel+False+frn+1+sl+%2D1+hd+False+hs+True+

former Canadian Public Safety Minister[68], Anne McLellan said, "Where it makes sense for us to share systems, share information, and work together in identifying those high-risk goods… [and] high-risk people, we will continue to do so...."[69] but it would be "irresponsible" for Ottawa to turn over information to Washington on a wholesale basis.[70]

BENEFIT OF AN EXPANDED NORAD ARRANGEMENT

In a similar process to exchanging information regarding potential terrorists attempting to immigrate into a country, countries need to be aware of potential weapon launches from outside their borders. Besides the normal array of threats already tracked by NORAD,[71] crude air-or-sea-launched cruise missiles have recently been added to the list.[72] Given the short warning period NORAD would be given to deal with this threat, the inclusion of the maritime operating picture into the overall operating picture seems inevitable. The Bi-national Planning Group (BPG) has arranged to improve the exchange of information regarding vessels of interest (VOI) by placing a CF maritime intelligence analyst inside the NORAD-USNORTHCOM Combined Intelligence and Fusion Center (CIFC) who works closely with an American maritime intelligence analyst. Information

or+Date+fh+False+ss+SO+sm+ES+mdbs+nfh+dstb+ES+mh+1+ri+KAAACBTB00011269+4565&_usd=0000&_uso=tg%5B2+%2D+tg%5B1+%2D+tg%5B0+%2D+db%5B0+%2Dnfh+hd+False+op%5B2+%2DAnd+op%5B1+%2DAnd+op%5B0+%2D+st%5B2+%2D+st%5B1+%2DHarper+st%5B0+%2DFortress++America+ex%5B0+%2Dthesaurus+mdb%5B0+%2Dimh+B4F0&fn=1&rn=1; Internet; accessed 27 March 2006.

[68] The head of Public Security and Emergency Preparedness Canada (PSEPC).

[69] Harper, "'Fortress America…'"

[70] *Ibid*.

[71] In many ways, a long-standing information sharing initiative between DoD and DND.

[72] Lieutenant-General Rick Findley and Lieutenant General Joe Inge, "North American Defence and Security in the Aftermath of 9/11," *Canadian Military Journal* vol. 6, no. 1 (Spring, 2005): 11 [journal on-line]; available from http://www.journal.forces.gc.ca/engraph/Vol6/no1/05-Inter_e.asp; Internet; accessed on 24 April 2006.

from CIFC regarding the VOI is then passed to both countries' domestic operation centers. [73]

Although a cliché, geography has forced Canada, the US and Mexico to become allies and this condition will persist as long as threats to each other's security can potentially be launched from each other's territory or territorial waters. Given the complexity of the terrorist threat, these three countries will continue to be driven to greater levels of cooperation. Although it seems natural that this would be accomplished under existing mechanisms like NORAD, this is not necessarily the case. Other mechanisms may be created to strike the balance required to share information, keep necessary information secret and manage the relationship so that it provides benefits to all. This reality makes it difficult to contemplate a secure North American continent without the participation of Mexico in some form or another.

Conclusion

The intelligence process consists of collection, analysis, and dissemination functions. In the government context, the purpose of the intelligence process is to provide organizations information that will guide their actions to improve or maintain national security. In the area of antiterrorism, information sharing can be used in all of these functions. It can increase the volume of data collected, improving the characterization of the terrorist situation. With more intelligence data available, a more complete analysis can be distilled. Information sharing can also facilitate the creation of analyst groups that share insight into each other's analysis and guide each other to useful sources of information. The dissemination function of the intelligence process is by definition

[73] Findley and Inge, "North American Defence…," 14.

information sharing, however the traditional “need to know” concept has been replaced. The “need to share” concept pushes intelligence to the very large number of antiterrorist stakeholders that have the ability to act upon the information. This is the biggest change in the overall intelligence process: the realization that to be able to act upon the intelligence available to identify potential terrorists, it needs to be widely disseminated to those who can do something about it.

Terrorism is a transnational threat. Countries need to explore cooperative ventures to quickly fill the gaps that exist within their own intelligence and national security forces. Within North America, this will lead to a greater degree of cooperation between Canada, the US and Mexico. Although the form and degree of this cooperation is constantly changing, geography dictates that each country is dependent upon the other for its own security. Unfortunately, the degree of success each country achieves in improving its national security will remain unknown. For in the area of national security, “[n]o real yardstick for success is available, only failure.”[74]

[74] Vickers, “The Intelligence…,” 363.

Bibliography

Borchert, Heiko. "A Transatlantic Agenda for Homeland Security Co-operation." *Jane's Homeland Security & Resilience Monitor* vol. 5, no. 3 (April 2006): 12-14.

Bowman, M.E. "Information at Risk." *American Intelligence Journal* (Autumn/Winter 2005): 44-49.

Bush, George W. *The National Security Strategy of the United States*. Washington, DC: The White House, 17 September 2002.

Charlaff, Joe. "Israeli Centre Tracks Jihadists in Cyberspace." *Jane's Homeland Security & Resilience Monitor* vol. 5, no. 3 (April 2006): vol. 5, no. 3 (April 2006): 10-11.

Findley, Lieutenant-General Rick and Lieutenant General Joe Inge. "North American Defence and Security in the Aftermath of 9/11." *Canadian Military Journal* vol. 6, no. 1 (Spring, 2005): 9-16. Journal on-line; available from http://www.journal.forces.gc.ca/engraph/Vol6/no1/05-Inter_e.asp; Internet accessed on 24 April 2006.

GlobalSecurity.org. "Advanced Passenger Information System (APIS)." http://www.globalsecurity.org/security/systems/apis.htm; Internet; accessed 21 April 2006.

Hart, Douglas and Steven Simon. "Thinking Straight and Talking Straight: Problems of Intelligence Analysis." *Survival* vol. 48, no.1 (Spring 2006): 35-60.

Higgins, T., P.A. Shakarian, and R.E. Ferguson. "No Stone Unturned: A Thorough Search for Tactical Intelligence Analysis" *American Intelligence Journal* (Autumn/Winter 2005): 60-66.

Hulnick, Arthur S. "U.S. Intelligence Reform: Problems and Prospects." *International Journal of Intelligence and CounterIntelligence,* vol. 19, no. 2, (Summer 2006); 302-315.

Jockel, Joseph T. *Security to the North: Canada-U.S. Defense Relations in the 1990s*. Michigan State University Press: East Lansing, 1991.

Johnson, Loch K. "A Centralized Intelligence System: Truman's Dream Deferred." *American Intelligence Journal* (Autumn/Winter 2005): 6-15.

Koc-Menard, Sergio. "Australia's Intelligence and Passenger Assessment Programs." *International Journal of Intelligence and CounterIntelligence,* vol. 19, no. 2 (Summer 2006): 218-236.

Miller, James Arnold. "Turning Open Source Data into Knowledge about Global Threats." *American Intelligence Journal* (Autumn/Winter 2005): 74-77.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. (Washington, D.C.: U.S. Government Printing Office, September 20, 2004). Publication on-line; available from http://www.9-11commission.gov/report/index.htm; Internet; accessed 30 March 2006.

Pillar, Paul R. “Intelligence, Policy and the War in Iraq.” *Foreign Affairs* vol. 85, no.2 (March/April 2006): 15-27.

Sims, Jennifer E. “Foreign Intelligence Liaisons: Devils, Deals, and Details.” *International Journal of Intelligence and CounterIntelligence* vol. 19, no. 2 (Summer 2006): 195-217.

Transportation Security Administration. “Secure Flight Program.” http://www.tsa.gov/public/interapp/editorial/editorial_1716.xml; Internet; accessed 21 April 2006.

United States of America. *The National Security Strategy of the United States of America,* March 2006.

Vickers, Robert D. “The Intelligence Reform.” *International Journal of Intelligence and CounterIntelligence* vol. 19, no. 2, (Summer 2006): 356-364.

Wikipedia. “Integrated Automated Fingerprint Identification System.” http://en.wikipedia.org/wiki/Integrated_Automated_Fingerprint_Identification_System; Internet; accessed 21 April 2006.