Archived Content

Information identified as archived on the Web is for reference, research or record-keeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards.

As per the [Communications Policy of the Government of Canada](), you can request alternate formats on the "[Contact Us]()" page.

Information archivée dans le Web

Information archivée dans le Web à des fins de consultation, de recherche ou de tenue de documents. Cette dernière n'a aucunement été modifiée ni mise à jour depuis sa date de mise en archive. Les pages archivées dans le Web ne sont pas assujetties aux normes qui s'appliquent aux sites Web du gouvernement du Canada.

Conformément à la [Politique de communication du gouvernement du Canada](), vous pouvez demander de recevoir cette information dans tout autre format de rechange à la page « [Contactez-nous]() ».

CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 33 / CCEM 33

EXERCISE/EXERCICE NEW HORIZONS

THE ABILITY TO FIGHT TERRORISM EFFICIENTLY
The Linking of Information and Intelligence Among Canadian Agencies – Integrated Databases

By Maj Scott Morrison, CD

Table of contents

Key Figures

THE ABILITY TO FIGHT TERRORISM EFFICIENTLY
The Linking of Information and Intelligence Among Canadian Agencies – Integrated Databases

Abstract

The events of September 11, 2001 did not only affect the United States of America, and their Security and Intelligence (S&I) communities, they were an abrupt awakening for every other nation on earth. They demonstrated that no country was immune from, and that any country in the world, regardless of how powerful it may be, could be attacked by non-state actors, more commonly known as terrorists. In the aftermath of these events, as the United States discovered its many weaknesses in sharing intelligence between its many S&I agencies, so too did Canada assess its ability to anticipate and counter such events. Canada had similar problems with inter-agency sharing of intelligence, and made recommendations for ameliorating such integration of intelligence to provide a better threat assessment for Canada. Based on the National Security Policy of 2005, the Integrated Threat Assessment Centre (ITAC) was created.

This paper will look at the threat of terrorism that Canada faces, and it will review Canada's intelligence sharing with its recent improvements through the creation of the ITAC. The paper will then highlight the fact that the process of information and intelligence sharing could be made more efficient through integrated databases and then it will offer three models of potential database integration for a more efficient exchange of information and intelligence among the S&I communities. The paper provides basic concepts, and it does not deal at all with technological architecture of such integration nor with the various legal and jurisdictional issues regarding security levels across the different agencies.

Introduction

The events of the 11th of September, 2001 (9/11) were an eye-opener to not only

Americans, but to the world. It was evidence that any country in the world could be targeted and

attacked. The interesting thing is that the attack was imagined, planned, orchestrated and

executed by a known terrorist organization. This is significant, in that there is no country in the

world that could pull this off, yet a group of individuals somehow organized through a network

of distributed cells, and somehow funded, and trained in a failing state such as Afghanistan

could. This action was indicative of a future modus operandi of terrorism in general. Although

this author does not agree with the US terminology "war on Terror," future wars could be waged

by violent groups of individuals, not necessarily affiliated or linked to any nation (non-state

actors)[1] against ideologies different than their own – in this case the West, and democracy.

At a press briefing one week after 9/11, National Security Advisor Condoleezza Rice

stated:

> 'This isn't Pearl Harbor.' No it was worse. Sixty years ago, the United States
> (US) did not have a director of central intelligence or 13 intelligence agencies or a
> combined intelligence budget of more than $30bn to provide early warning of an
> enemy attack. And just as intelligence was divided and diffuse on the eve of Pearl
> Harbor, there was no genuine intelligence community on the eve of September 11,
> 2001.[2]

These initial remarks from Ms Rice indicated that the US had possessed intelligence leading up

to the event, but given their varied intelligence agencies, were unable and unwilling to share and

---

[1] Although it is difficult to find an accepted definition of non-state actors, in an article on National Interst Online,
Terence Chong and Joergen Oerstroem Moeller outline the ideology of non-state actors: Transnational non-state

collate information to create the right level of knowledge to provide the necessary early warning

to avert the attack. Indeed, the lack of information sharing amongst the said intelligence agencies

was emphasized in the 9/11 commission report with applicable recommendations to improve

upon.[3] Since then, they have initiated several changes within the greater bureaucratic structure by

legislation[4] for sharing of information amongst all agencies including between law enforcement

agencies with foreign intelligence and vice versa.[5]

The Government of Canada has recently released its international and foreign policy.[6] It is

clear from this policy that Canada will synergize the conduct of its foreign policy throughout the

breadth and depth of its capabilities – in all departments and ministries. It further outlines that its

biggest threat comes from failing states, which harbour non-state actors who in turn will attack as

they see fit. The policy is also clear that it is better to engage such threats as far away from home

as possible before those threats can be made to bear on Canadian soil.

> An increasingly interdependent world has tightened the links between international
> and domestic security, and developments abroad can affect the safety of Canadians in
> unprecedented ways. Today's front lines stretch from the streets of Kabul to the rail
> lines of Madrid to our own Canadian cities. The Government has made a commitment
> to respond to potential threats to Canadian security before they reach our shores.[7]

However, in order to be able to act accordingly when dealing with non-state actors, either by law

enforcement agencies domestically or by the military overseas, good intelligence is required. In a

---

[2] Twenty-First Century Intelligence, p59.

[3] The 9/11 Commission Report, pp 407-410.

[4] The USA Patriot Act was signed on 26 October 2001. It allowed law enforcement agencies to search telephone and email communications and medical, financial, and other records and it eased restrictions on foreign intelligence gathering within the United States amongst many other issues.

[5] Larry D. Thompson (Brookings Institute) speech to National Commission on Terrorist Attacks Upon the United States, December 8, 2003.

[6] Canada in the World: Canadian International Policy - Canada's International policy.

[7] Defence: A role of pride and influence in the World.

perfect world, all nations would share information and intelligence with all other nations on terrorist organizations, even those working in and out of their own countries, and all levels of law enforcement and policing would do likewise. In a Utopian world, there would be a database that would be kept up to date about key people in these organizations, and this information could be used both nationally and internationally, collectively or by individual nations to identify, track and act accordingly with these non-state actors in such a way as to mitigate the risks they pose to the world in general. While a single global database would lead to 'information overload'[8] one could certainly think that several databases could be linked within a single nation to make information and intelligence sharing more efficient.

If future conflicts with non-state actors are to be effective, they must be intelligence driven.[9] Further more, there must be a coherent, unified effort across the Canadian Security and Intelligence (S&I) communities and a system that allows efficient sharing of critical information that can be linked, analyzed and acted upon.

Although there has been much progress in Canada lately with inter-agency sharing of information and intelligence with the creation of the Integrated Threat Assessment Centre (ITAC), there is still a necessity for a more efficient way to share and disseminate information and intelligence. This paper will offer up three models of potential integration of Canadian S&I databases which would lead to better efficiency in meeting the threat of terrorism toward

---

[8] Strategic Intelligence, p397 – Information overload is an old problem in the [Intelligence] Analyst trade. While technology can assist in the management of information, and to a point with analytical methodologies, in the end, the quality of analysis depends on the intellectual capabilities of individual analysts and manager.

[9] The Royal Canadian Mounted Police definition of Intelligence-led Policing: Intelligence-led policing is a term that has only begun to gain currency in the last few years. … intelligence-led policing involves the collection and analysis of information to produce an intelligence end product designed to inform police decision-making at both the tactical and strategic levels. It is a model of policing in which intelligence serves as a guide to operations, rather than the reverse. It is innovative and, by some standards, even radical, but it is predicated on the notion that a principal task of the police is to prevent and detect crime rather than simply to react to it.

Canada. The paper concentrates on the conceptual models, and does not stray into the technical architecture or any of the legal and jurisdictional hurdles which would be required for implementation of such integration.

A review of the current Canadian security environment with the threat of non-state actors, terrorists will be followed by a short historical study of the Canadian S&I community. Canada's newest tool, the Integrated Threat Assessment Centre (ITAC) which was established as a result of 9/11 to be a better intelligence sharing mechanism for the Government of Canada will be studied in terms of how intelligence is currently shared. Finally, three models of information and intelligence sharing (integrated database) will be presented highlighting some advantages and disadvantages of each model to demonstrate that there is scope for more efficiently dealing with the myriad of information and intelligence. The paper is meant to generate some debate within the Canadian S&I community regarding the way ahead for efficient usage of intelligence information in combating terrorism.

The Terrorist Threat to Canada

There is no single definition of terrorism, but many. Walter Enders and Todd Sandler in a paper studying terrorism post 9/11 state "Terrorism is the premeditated use or threat of use of violence by individuals or sub-national groups to obtain a political or social objective through intimidation of a large audience beyond that of the immediate victims."[10] No matter what definition is used, it is clear that violence will be involved, and that there is some sort of

---

[10] Enders & Sandler, p2.

underlying purpose for the actions. In this definition, there is no mention of a state, but of a group or (an) individual.

Terrorism is not a new phenomenon. "Terrorism has been around as a major nuisance to governments as long as recorded history."[11] While this may be so, and while it may have been debated about whether or not the application of unconventional tactics used to bring about change is moral or not, terrorism has certainly come to the forefront in the past century because of mass media.[12] While in previous centuries, there was no international mechanism to address terrorism, the United Nations has now been dealing with terrorism for several decades, ensuring that countries abide by the thirteen counter-terrorist conventions currently in place today.[13]

There have also been numerous incidents in Canada over the years from the October Crisis of 1970 in Quebec, to the seizure of the Air India disaster departing from Vancouver and the fatal storming of the Turkish Embassy in Ottawa by armed men in 1985. Most recently, and although not yet resolved, were the seventeen alleged terrorists arrested in Toronto on suspicions of conspiracy to commit terrorist acts.[14] Furthermore, the Canadian government maintains an up-to-date list of those terrorist organizations that it recognizes which currently has thirty-nine.[15]

In his opening remarks at the Canadian Association for Security and Intelligence Studies (CASIS) on 27 October, 2006, the director of Canadian Security and Intelligence Service (CSIS), Mr. Jim Judd defined the current terrorist global ideology as follows:

---

[11] The criminology of terrorism: history, law, definitions, typologies, p1.

[12] The Media and Terrorism, A Reassessment, p2.

[13] UN Action to Counter Terrorism, UN Internet site.

[14] Sweitzer, Mark, Head, Partnerships Integrated Threat Assessment Centre (ITAC), personal interview with author, 12 March 2007.

[15] Public Safety Canada – Currently listed Entities, 14 Apr 2007.

Today, most organizations such as mine in the western world and elsewhere are very much focused on the challenge of terrorism. More specifically, it is the threat represented by what I would term the "ideology of al Qaeda". I mean by that ideology espoused by the original al Qaeda organization (and what remains of it today), its organizational affiliates and, increasingly, individuals and groups around the world who are inspired by it.[16]

He goes on to say that "It [This new ideology] is global in scope, unlike most other terrorist movements of the past which tended to be more nationally or regionally focused." In terms of its global reach and following, he derisively states that "it has become a veritable United Nations of the terrorist movement."[17] It is this ideology that threatens the west, especially North America and Canada. Furthermore, it is this global reach with like-minded individuals of any citizenship including Canadian that could initiate terror cells within Canada. In fact, the Canadian government is well aware of such 'home-grown' terrorists and it has stated "As in other open societies such as Britain and Spain, there is always potential for terrorist cells to emerge. No country is free from terrorist threats or infiltration, or indeed from home-grown terrorism."[18] Additionally, due to the proximity to the United States, " . . . there are more terrorist groups active in Canada today than in any other country in the world."[19] Clearly Canada is threatened by terrorism, and must take appropriate actions across government to minimize the threat while providing a secure environment for its citizens.

Canadian Interagency Sharing of Information and Intelligence

---

[16] Mr Jim Judd, Director of CSIS - Opening Remarks to the Canadian Association for Security and Intelligence Studies (CASIS), Friday 27 October 2006.

[17] *Ibid.*

[18] Government of Canada - Canadian Ally.com.

It is clear that if terrorists are to be rendered ineffective in actions against Canada, then the Canadian S&I community has to share information and intelligence, and do so as efficiently as possible. A clear understanding of the difference of information and intelligence is required even though they are used interchangeably quite often. While information is simply raw data, intelligence is a finite set of 'fused' knowledge, including some from undisclosed sources, which is used as a basis for official decisions.[20]

The Canadian Security Intelligence Service (CSIS) was created on 23 March, 1984,[21] providing a framework of democratic control and accountability for a civilian Canadian security intelligence service, following the McDonald Commission of Inquiry in the late 1970s.[22] The commission had been ordered because there had been some irregularities and illegalities within the Royal Canadian Mounted Police regarding the conduct of both intelligence and law enforcement. "The commission recommended, among other things, that police comply strictly with the law … and that a civilian security agency, divorced from the RCMP, be created."[23]

CSIS was just one year old when the Air India disaster occurred and this event caused much angst between the RCMP and CSIS, and brought about the question of the sharing of intelligence among government departments. The inquiry into the Air India disaster should answer among other questions:

> . . . if there were problems in the effective cooperation between government
> departments and agencies, including the Canadian Security Intelligence Service
> and the Royal Canadian Mounted Police, in the investigation of the bombing of
> Air India Flight 182, either before or after June 23, 1985, whether any changes in

---

[19] Canadian Security and Intelligence Service (CSIS) – Terrorism page.

[20] Strategic Intelligence, p411.

[21] CSIS Act.

[22] CSIS Backgrounder – Mandate.

[23] Inquiry Into Certain Activities of the Royal Canadian Mounted Police, Royal Commission of.

practice or legislation are required to prevent the recurrence of similar problems
of cooperation in the investigation of terrorism offences in the future.[24]

While the inquiry is now underway, the S&I communities have been making improvements on

how they share information and intelligence since 1985. However the urgency of addressing

inter-agency sharing only occurred post 9/11. It was Canada's National Security Policy April

2004 that first formally identified the creation of an 'Integrated Threat Assessment Centre.'[25]

Prior to this, Canada had numerous agencies all working and reporting to various governmental

departments over the years. Figure 1 shows intelligence sharing prior to and after the inception of

the ITAC.

The mandate from which the ITAC operates is outlined in a classified framework

agreement which is in place. This agreement outlines that all of the Canadian agencies will share

their information with all of the other agencies, and how to do so.[26] In general, the ITAC's

mandate is the production of comprehensive and integrated threat assessments with respect to

terrorist threats focusing on domestic and international special events, critical incidents, terrorist

trends, and input to travel advisories. Additionally, the ITAC contributes to Foreign Affairs and

International Trade and Commerce threat and risk assessment for Canadian missions, interests

and persons abroad. [27]

---

[24] Government of Canada – Terms of Reference - Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

[25] Securing an Open Society – Canada's National Security Policy Apr 2004, p 18.

[26] Commander Paul Grimshaw, a former DND/ CF representative at the ITAC, is a student on JCSP 33, and provided this unclassified version of the ITAC framework agreement in an interview with the author, 19 Mar 2007.

[27] Sweitzer, Mark, Head, Partnerships Integrated Threat Assessment Centre (ITAC), personal interview with author, 12 March 2007.

Threat Assessments Prior to NSP
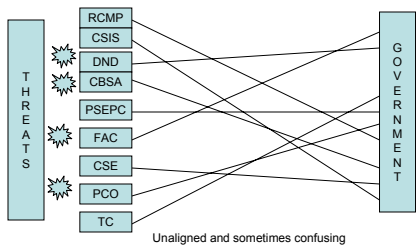
Threat Assessment Post NSP

Figure 1. Intelligence flow to Government prior and subsequent to creations of ITAC[28]
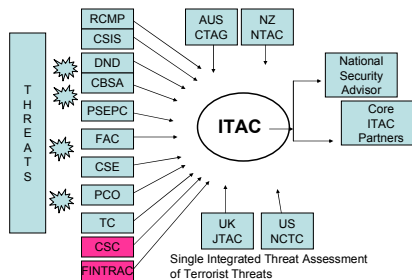
Although the consolidated reports are now of better use to the government of Canada as can be seen in figure 1, the sharing of information is still parochial[29] in that if an analyst wishes information from another agency, they have to ask the analyst affiliated with that agency, and then review hard copy print-outs of the information.

Any information that is to be used then has to be approved by the providing agency. The physical databases of all ITAC agencies less that of the Finance Department, are located in a single location, however, given existing information sharing protocols as well as the natural resistance for liberal information sharing within the S&I communities, limited integration of these databases is even doubtful.[30] If databases from the various agencies affiliated with the ITAC could as a minimum allow queries from within the ITAC, efficiencies could be made in sharing of information and intelligence within the ITAC.

---

[28] *Ibid.*

[29] *Ibid.*

[30] In terms of reluctance for S&I communities to liberally share information, this comment is made based on my personal dealings with the multinational military intelligence community, but also gleaned informally from consultations both Mark Sweitzer and Commander Grimshaw.

ITAC has approximately fifty personnel (analysts) who have been seconded for a limited and finite time from their parent agencies,[31] and are to be replaced upon completion of their tenure. In principle, based on their priorities, they draft consolidated and integrated reports on various threats to Canada. Their current focus is on terrorism, however that is the flavour of the month, and they have to continue with their other areas of analysis. [32] Even though ITAC was created to combat terrorism in an integrated manner, it is clear that several of the threat categories could be linked, and therefore, ITAC and its integrated intelligence could be useful. For example, organized crime and terrorism, although not traditionally linked, could be in a transnational operation. [33]

Proposed models for Integration of Databases for Information and Intelligence Sharing

While the thought of harnessing the ever-improvements in computing technology to share information and intelligence is a noble concept, and understanding the potential impact it will have on S&I communities,[34] it is clear that such an approach is required to combat terrorism of today and into the future. In his introductory address to the CASIS symposium in October 2006, the director of CSIS Mr Jim Judd stated:

> We need the talent to respond to a growing problem in managing the storage, retrieval, cross-referencing and analysis of the sheer volume of information. And

---

[31] ITAC Parent organizations: Canada Border Services Agency, Communications Security Establishment (CSE), Canadian Security Intelligence Service (CSIS), Department of National Defence (DND), Foreign Affairs and International Trade (DFAIT), Privy Council Office (PCO), Transport Canada, Department of Public Safety, Correctional Services Canada, FINTRAC, RCMP, OPP and SQFT.

[32] The eight Specific Threat Categories are: Critical Infrastructure, Failed/ Failing States, Foreign Espionage, Organized Crime, Natural Disasters, Pandemics, *Terrorism*, and WMD. ITAC was created specifically to address terrorism in an integrated manner.

[33] Transnational Terror and Organized Crime: Blurring the Lines, Internet, Abstract.

[34] Strategic Intelligence, p397.

we also need to strengthen our ability to take on new approaches to meta data analysis, searching for the underlying patterns and trends linked to activities.[35]

This statement is confirmation that the Canadian S&I community is aware of the need for efficiently managing, but also sharing of information and intelligence.

While it is clear that there are a myriad of both technical and legal issues which must be debated and overcome prior the realization of such integration, technological innovations are moving at such a pace, that it may not be too far away. While these issues could be the subject of another paper, it is appropriate to at least offer some general comments to indicate that both of these complex issues could be overcome. In terms of technology, there are numerous software firms which deal with such challenges on a daily basis.[36] Even the North Atlantic Treaty Organization (NATO) is studying integration of databases and there is "… ongoing effort at NC3A to provide one integrated database which contains data from a number of different sources."[37]

From a legal or jurisdictional perspective, there are many issues regarding sources of information, security classification of information and others. While agencies are lawfully allowed to share intelligence, aspects of the Privacy Act and legal statutes concerning probable cause still apply.[38] While this is an issue, the RCMP are currently conducting a trail project called National Integrated Interagency Information (N-III) which links the databases of the law

---

[35] Mr Jim Judd, Director of CSIS - Opening Remarks to the Canadian Association for Security and Intelligence Studies (CASIS), Friday 27 October 2006.

[36] Integrated Database Inc is one such company that I informally contacted to discuss conceptually integrated databases for the S&I community. While I wasn't prepared to pay the hourly rate for their consultation, such companies work in integration of databases daily.

[37] NATO NC3 Technical Architecture.

[38] Commander Paul Grimshaw, interview with the author, 4 February 2007.

enforcement communities across Canada and selected agencies.[39] N-III is an intelligence querying tool which allows various federal public agencies to have 'filtered access' to the integrated database based on levels of security consistent with current legislation, and the RCMP work with these selected agencies to establish the requisite security access.[40] It can be seen then, that the many hurdles which would have to be overcome, could be overcome, and indeed prototype projects for integration are already underway.

Before getting into the models themselves, a sample scenario using an arbitrary person 'X'[41] will be provided to amplify the need for efficient cross referencing of databases. Information or intelligence on person "X" may be found on any number of the S&I databases. He may or may not be a Canadian citizen and he may have spent some time in either a foreign or Canadian prison or he may have caused an altercation at an port of entry into Canada (airport, US border, sea port). Person 'X' may have large sums of money either in banks or various investments, and he may have a cell phone number linked to a known terrorist cell operating in a Canadian cities or elsewhere. Knowing how cumbersome the present system of information and intelligence sharing is even within ITAC, and the requirement to establish linkages of information to create intelligence, there should be a way to handle it electronically thus speeding up the process of fusion of intelligence, and getting crucial terrorist related intelligence in the hands of law enforcement or other first responders who have the authority to enforce the law. This sample scenario should be kept in mind while considering the proposed models for database integration.

---

[39] RCMP - National Integrated Interagency Information (*N-III*) System.

[40] Chief Superintendent Ray Lamb, head of N-III project, telephone conversation with author, 29 March 2007.

[41] Although the gender of person 'X' could be either male of female, the male gender will be used.

While three different models will be presented here, they only skim the surface in terms of theoretic database architecture. Any or all characteristics of each of these models could be incorporated any number of ways, thus there are really an inordinate number of ways that databases could be integrated. However each of the options presented range from the most simple to the most complex with the idea that model one keeps the existing S&I databases pure while linking them electronically for query only. Option two is a step up but allows intelligence in the form of ITAC reports to be accessed by multiple agencies and first responders across a national pipeline while option three introduces the sharing of raw information as well as intelligence, and similar to option two, allows multiple agency and first responder access.

Model 1 'Limited Pure Database'

The concept for this model would be to allow ITAC analysts the opportunity to electronically query all ITAC agency databases located at CSIS. While there would be some physical connectivity within the one building, and some software created to implement this, it is the intent of this model to keep the various databases pure and unaltered by the queries, and that it remain essentially a closed database for ITAC analysts. The responses to queries would not be specific information, but a symbolic response indicating that information is available in that database such as by a coloured flag. In other words, no raw data would be accessible by the analyst, only the fact that another agency's database had information on person X. Individual agency databases would retain an appropriate firewall to verify the classification authorization of the analyst as well as the integrity of the database. It would still require the analyst to verify through human interface with the analyst from the other agency the actual information and the links to it. Figure 2 is a pictorial representation of this simple closed database.

In this model, the efficiencies generated would be internal to the ITAC in the production of their reports. Generally, the analyst developing the report would only have to speak to those analysts whose databases showed a positive response to the query. The analyst doing the report could then conduct business as normal.
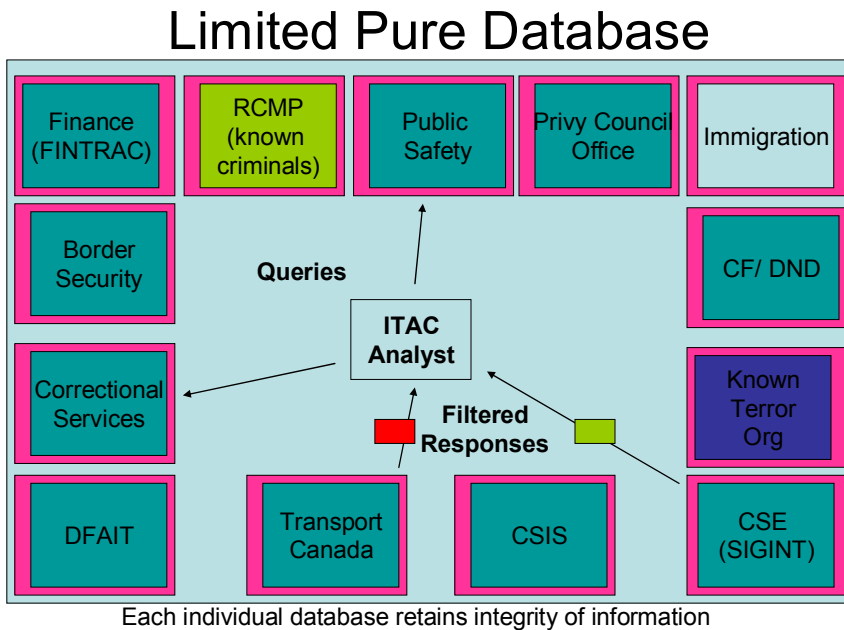
Limited Pure Database

Each individual database retains integrity of information

Figure 2.   Model One - 'Limited Pure Databases'

This option only skims the surface of integration of intelligence, and it does so within the physicality of the ITAC. While this may not appear to go far enough, it would be considered a step in the right direction in terms of the S&I communities overcoming their fear of sharing intelligence or intelligence somehow being misused. This keeps the agencies' databases pure and the current system of checks and balances of authority for dissemination of information in tact. It would only slightly increase the efficiency of the overall ITAC due to less people having to query databases for each report. The application of this model focuses the analyst within the ITAC to only those agencies that need to support the analysis of person 'X'.

However this option does not address the efficient distribution of intelligence needed beyond the ITAC for use by law enforcement agencies and other first responders. The current system of distribution of classified intelligence reports to law enforcement agencies is still cumbersome and hierarchical.[42] Critical intelligence on potential terrorist activities in specific municipal jurisdictions needs be generated or flow to the right level of first responder. Additionally, this simplistic model does not address information, but only intelligence reports, and therefore is less likely to be of immediate benefit to first responders. While intelligence reports are critical to the Government of Canada at the strategic level, they may not be as useful at the tactical level where law enforcement officials and other first responders are required to act.

Model Two – 'Secure National Pipeline'

This model addresses the more efficient distribution of integrated intelligence reports created at the ITAC only, and not the actual production of those reports. The intent would be to create a common nation-wide database, or pipeline that could be partitioned into various classification levels. ITAC would place its integrated intelligence reports into applicable security classified locations on this database. Anyone working across the country in law enforcement and other agencies with appropriate classification levels would then be able to drill into the database to the level that they require the information. Figure three highlights the multi-agency ability to drill down to their appropriate classification to benefit from the intelligence reports. While this option would make the intelligence dissemination beyond the ITAC more efficient, and therefore

---

[42] Sweitzer, Mark, Head, Partnerships Integrated Threat Assessment Centre (ITAC), personal interview with author, 12 March 2007

more immediately accessible to the first responders, this model does not assist in addressing the efficiency of the production of intelligence reports.
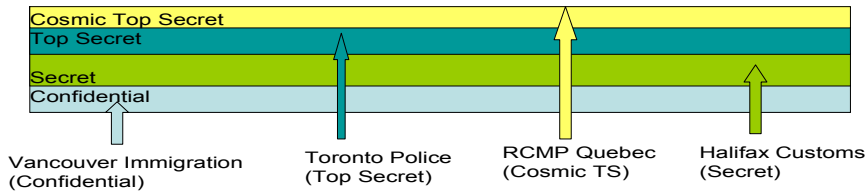
Secure National Pipeline

Figure 3 'Secure National Pipeline'

Clearly, first responders would have intelligence more quickly than the current system, and also the intelligence that is accessible will already have been sanitized, filtered and authorized by the various agencies. However, if a certain first responder searched the database (based on his/ her classification), and did not get any intelligence, yet it existed, either because it was at a higher classification or for whatever reason did not get articulated correctly in the integrated report, there may still be a requirement for a backup way to check for higher classified intelligence. Such a back up system would likely resemble the current cumbersome method of distribution which is counter-intuitive to the creation of such a national pipeline in the first place.

Model Three – 'Complex information and Intelligence Integration'

As indicated earlier, a prototype similar to this type of model is currently under development integrating the Canadian law enforcement communities and other selected agencies. It is being run as a project out of the RCMP and is called the National Integrated

Interagency Information (N-III).[43] More will be explained shortly, however the intent of this model is to not only make the distribution of intelligence more efficient, but also open up the integration to raw data as well. Similar to model 2, personnel across the country could drill only to the level of their classification. All data must also be accompanied by appropriate 'qualifiers' of the information (classification, reliability, agency that placed the information onto the system, how current is the information etc). Those personnel with the highest of classification could access the entire data base, and therefore link and compare and collate data into intelligence from across the entire data base. This could lead to interesting links and it could shed light more quickly on potential threats that could be addressed by any number of law enforcement agencies etc.

This option seeks to broaden the information sharing to the maximum extent possible (in terms of accompanying each piece of info with a 'fingerprint'). This would allow the analyst or first responder to check with the appropriate agency if there were any doubts. Figure four represents the type of partitioning by security classification as well as the required information to accompany each entry into the database.

Chief Superintendent Ray Lamb of the RCMP who is heading the project indicates that it is a useful tool for the law enforcement agencies. The system is based on the Police Information Portal (PIP) which allows police personnel to query the shared database. This data base has real-time record management of raw data and that the information on it should be current. He did indicate however, that there are caveats so that users are instructed to confirm the information

---

[43] RCMP - National Integrated Interagency Information (N-III) System.

with the originating agency for accuracy and currency. They are able to drill down for additional information, and if the originator of the information agrees, then it can be released to him.[44]

The N-III is well underway, and it seems to work for the law enforcement community because they are essentially governed by similar mandates, but different jurisdictions, however, all in all similar cultures. If one takes a leap of faith, and with some challenges to overcome, then one could see that a similar approach could be taken to link all the S&I communities to meet the proposed requirements of intelligence sharing across cultures.

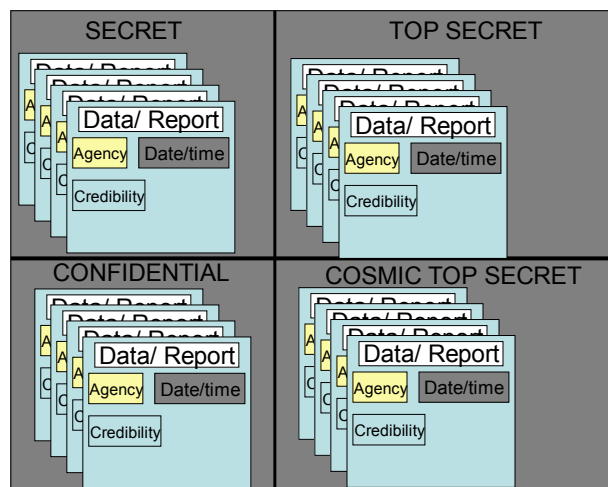**Complex information and**

Intelligence Integration

Figure 4 'Complex Information and Intelligence Integration'

Clearly this type of system will speed up the process of linking valuable information and intelligence, while simultaneously speeding up the validation of such linkages through discussions with the owners of that intelligence. While the benefits are easy to see with this type of model, there would also be some concerns about its implementation. Many agencies may try

---

[44] Chief Superintendent Ray Lamb, RCMP Ottawa, telephone conversation with author, 29 March 2007.

to do analysis rather than their current function, and there might be much duplication of efforts

that occur. Certainly the maintenance and security of such a complex database would require a

there would no doubt be opposition from within and outside the intelligence community to this type of electronic sharing, it is felt that there should be some serious thought and debate on this issue. It is clear that the information and intelligence that would be shared is extremely sensitive and there are numerous legal constraints which have been noted, yet the law enforcement community has been able to manage these within their own sphere of operations. However, given that currently most of the S&I community databases are located in one building, it seems that even a simple closed database would be a step in the right direction, and one in which limited experimentation could occur.

While there are hurdles to overcome, and security concerns for any of the models provided in this paper, it is clear that the overall improvements in efficiency in the collation of information and intelligence into useful linkages with which Canadian and international law enforcement agencies can work in order to combat terrorism is worth considering. Understandably the security and intelligence communities will have some anxieties and opposition to change, however, as non-state actors modernize and explore new techniques of remaining hidden and anonymous to the West's ability to identify, detect, track and deal with terrorists, it is incumbent on the West to similarly explore the realm of information and intelligence sharing within the overall S&I communities in Canada and around the world in order to effectively deal with this ongoing threat.

While this paper only scratched the surface of this idea, it has been shown that with a little imagination and technological experimentation conducted within the broader current legal constraints, the challenge of integrating databases is not insurmountable, and at the same time it could produce exponential dividends in efficiency.

Bibliography

Books and Research Papers

Barr Colonel David. Implications of the War on Terrorism for Canadian Defence Policy and
    Force Structure. Toronto: Canadian Forces College, National Security Studies Course Paper,
    2003.

Borys Major W.J. "Need to Know" To "Need to Share": How Terrorism is Changing the Intelligence Community's Culture. Toronto: Canadian Forces College New Horizon's paper, 2006.

Canada. A Role of Pride and Influence in The World. Department Of Foreign Affairs and International Trade, 2005.

Canada. Department of National Defence. Strategic Assessment 2005 Edited by Directorate of Strategic Analysis Policy Planning Division Policy Group, Ottawa: DND, 2005.

Canada. Securing and Open Society: Canada's National Security Policy. Privy Council Office, 2004.

Charters David A., Farson Stuart, Hastedt Glen P. Intelligence Analysis and Assessment. London, Frank Cass, 1996.

Dearth Douglas H. and Goodden R. Thomas. Strategic Intelligence: Theory and Approach Second Edition. Carlisle Barracks, PA, United States Army War College, 1995.

Hesi Carmel. Intelligence for Peace: The Role of Intelligence in Times of Peace. Portland Oregon, 1999.

Paul Todd & Jonathan Bloch. Global Intelligence: The world's Secret Services Today. Black Point, NS Canada: Fernwood, 2003.

Salisbury Colonel David. Asymmetric Warfare and the Geneva Conventions: Do we need a new Law of Armed Conflict in the Age of Terrorism? Toronto: Canadian Forces College National Security Studies Course Paper, 2002.

Santarpia LCdr BW. Taking the fight to the enemy: Terrorism and the Case for a Canadian Forces Expeditionary Orientation. Toronto: Canadian Forces College Command and Staff College 30 Masters of Defence Studies Thesis, 29 Apr 2004.

Scott, L.V., Jackson, Peter. Understanding Intelligence in the Twenty-First Century: Journeys in Shadows. New York: Routledge, 2004.

Wesley K Wark. Twenty-First Century Intelligence. New York: Routledge Taylor & Francis Group – Frank Cass, 2005.

Internet Sources

After 9/11 is it all different now? Enders Walter (U of Alabama) Sandler Todd (U of Southern California), April 2004. http://www.prism.gatech.edu/~rk114/seminarpapers/after_911_ms.pdf; Internet, accessed 7 Mar 2007.

Air India Inquiry terms of reference. http://www.majorcomm.ca/en/termsofreference/; Internet, accessed 14 Apr 2007.

Air India Report. http://www.ps-sp.gc.ca/prg/ns/airs/rep1-4-en.asp; Internet, accessed 29 Mar 2007.

Article Special forces transformation. http://www.journal.forces.gc.ca/engraph/Vol6/no4/PDF/09-Ops_e.pdf; Internet, accessed 7 March 2007.

Assessing Violent Conflicts Between States and Non-State Actors. Mark Crecenzi, Robert Jenkins and Charles Kurzman. http://gi.unc.edu/research/pdf/latane_proposal_submitted.pdf; Internet, accessed 7 March and 14 Apr 2007.

Canada's missing Foreign intelligence agency. http://cv.jmellon.com/cfis_2.pdf; Internet, accessed 5 Mar 2007.

Canadian Ally.com http://www.canadianally.com/ca/canadasimmpolicy20060607-en.asp; Internet, accessed 14 Apr 2007.

Canadian Encyclopedia. Inquiry Into Certain Activities of the Royal Canadian Mounted Police, Royal Commission of (McDonald Commission) http://www.thecanadianencyclopedia.com/index.cfm?PgNm=TCE&Params=A1ARTA0004009; Internet, accessed 14 Apr 2007.

Canadian Intelligence. http://www.journal.forces.gc.ca/engraph/Vol2/no4/pdf/41-46_e.pdf; Internet, accessed 7 March 2007.

Canadian Intelligence accountability. http://www.oag-bvg.gc.ca/domino/reports.nsf/a1b15d892a1f761a852565c40068a492/4f626474cefb11f58525 65d90072f17e?OpenDocument; Internet, accessed 5 Mar 2007.

Canadian Security Intelligence Service Act (R.S., 1985, c. C-23). http://laws.justice.gc.ca/en/C-23/index.html; Internet, accessed 7 March 2007.

CCIRC (cyber reporting). http://www.psepc-sppcc.gc.ca/prg/em/ccirc/abo-en.asp; Internet, accessed February 2007.

CSIS Backgrounder Information. http://www.csis-scrs.gc.ca/en/newsroom/backgrounders.asp; Internet, Accessed February 2007.

CSIS Commentary No 85. http://www.csis-scrs.gc.ca/en/publications/commentary/com85.asp; Internet, Accessed February 2007.

CSIS Mandate backgrounder. http://www.csis-scrs.gc.ca/en/newsroom/backgrounders/backgrounder01.asp; Internet, accessed 5 Mar 2007.

CSIS – Terrorism. http://www.csis-scrs.gc.ca/en/priorities/terrorism.asp; Internet, accessed 14 Apr 2007.

C4I. http://wps.cfc.forces.gc.ca/papers/otherpublications/80_yankowich.pdf; Internet, accessed 7 March 2007.

Database woes. http://proquest.umi.com/pqdweb?index=6&did=248738521&SrchMode=1&sid=1&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1172840559&clientId=1711; Internet, accessed 7 Mar 2007.

Defence statement 2005. http://www.forces.gc.ca/site/reports/dps/main/02_e.asp#5; Internet, accessed 7 Mar 2007.

Designing a new dimension http://proquest.umi.com/pqdweb?index=9&did=804792&SrchMode=1&sid=3&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1172840947&clientId=1711; Internet, accessed 7 Mar 2007.

Global War on Terrorism and Democratic Rights**. Tapan Kumar Bose (Revised on December 3, 2004). http://www.sacw.net/hrights/TBose27Jan2005.html; Internet, accessed 3 April 2007.

Government response. http://www.forces.gc.ca/site/Newsroom/files/KennyE.pdf; Internet, accessed 7 March 2007.

Hizbullah intelligence. http://www4.janes.com/subscribe/jtsm/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jtsm/history/jtsm2006/jtsm5013.htm@current&Prod_Name=JTSM&QueryText=%3CAND%3E%28

Intelligence-led policing. http://www.rcmp-grc.gc.ca/crimint/intelligence_e.htm; Internet, Accessed February 2007.

Interagency Intelligence. Major Tim Lannon. http://www.journal.forces.gc.ca/engraph/Vol5/no3/PDF/CMJ-Interagency_e.pdf; Internet, accessed 7 March 2007.

ISR Experiment. http://www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1432; Internet, accessed 7 March 2007.

Larry D. Thompson, Senior Fellow Brookings Institute, Governance Studies and Economic Studies speech to National Commission on Terrorist Attacks Upon the United States, December 8, 2003 http://www.brookings.edu/views/testimony/thompson/20031208.htm ; Internet, accessed 14 Apr 2007.

Mackenzie Institute – Canada Terrorism history. http://www.mackenzieinstitute.com/2003/other_peoples_wars2.htm#terrorism; Internet, accessed 5 Mar 2007

National Security and Human Rights Concerns in Canada: A Survey of Eight Critical Issues in the Post-9/11 Environment. http://www.chrc-ccdp.ca/research_program_recherche/ns_sn/toc_tdm-en.asp; Internet, accessed 7 March 2007.

NATO NC3 Technical Architecture. http://194.7.80.153/website/page.asp?menuid=18; Internet Accessed Mar 07, 16 Apr 07.

News paper Article on creation CSIS – Canada not safer. http://www.canada.com/components/print.aspx?id=688df2e6-891e-44f7-9dc6-ce42bde00dbb&k=19693; Internet, accessed 8 Mar 2007.

News paper Article on creation CSIS – Canada not safer. http://thechronicleherald.ca/Canada/563384.html; Internet, accessed 8 Mar 2007.

News paper Article on Military involvement training 'mock terrorist attack'. http://www.rbcinvest.theglobeandmail.com//servlet/ArticleNews/PEstory/LAC/20070403/TERRORGTA03/national/national/nationalTheNationHeadline/7/7/25/; Internet, accessed 3 April 2007.

No video game (Janes). http://www4.janes.com/subscribe/jtsm/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jtsm/history/jtsm2006/jtsm5032.htm@current&Prod_Name=JTSM&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5Dterrorism+%3CIN%3E+body%29%2C+%28%5B

[100%5D+%28%5B100%5Dterrorism+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5Dterrorism+%3CIN%3E+body%29%29%29%29](); Internet, accessed 7 Mar 2007.

Power in Today's World: A Nationalist United States of America: Part 1. Terence Chong and Joergen Oerstroem Moeller, 4 October, 2007 [http://www.nationalinterest.org/Article.aspx?id=14000](); Internet, accessed 14 Apr 2007.

PSEPC - Canadian List of Terrorist Organizations. [http://www.psepc-sppcc.gc.ca/prg/ns/le/cle-en.asp](); Internet, accessed 5 Mar 2007.

Public Safety Canada – List of recognized Terrorist organizations [http://www.publicsafety.gc.ca/prg/ns/le/cle-en.asp](); Internet, accessed 14 Apr 2007.

Putting pieces together. [http://ww2.psepc.gc.ca/publications/iji-iij/summer-ete04/pieces_e.asp](); Internet, accessed 7 Mar 2007.

RCMP Intelligence led policing. [http://www.rcmp-grc.gc.ca/crimint/intelligence_e.htm](); Internet, accessed 14 Apr 2007.

RCMP- N-III. [http://www.rcmp-grc.gc.ca/niii/pdf/NIIIBrochure.pdf](); Internet, multiple access – latest 18 Apr 2007.

Sanderson, Thomas M. Transnational Terror and Organized Crime: Blurring the Lines SAIS Review - Volume 24, Number 1, Winter-Spring 2004, pp. 49-61 [http://muse.jhu.edu/login?uri=/journals/sais_review/v024/24.1sanderson.html](); internet accessed 18 April 2007.

Smart Border (Northern Exposure). [http://www.govtech.net/magazine/story.php?id=3030000000018377](); Internet, accessed February 2007.

Speaking notes, Mr Jum Judd. [http://ww2.psepc.gc.ca/publications/speeches/20040426_e.asp](); Internet, accessed February 2007.

Stepped up intelligence. [http://proquest.umi.com/pqdweb?index=2&did=637764571&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1172840559&clientId=1711](); Internet, accessed 7 Mar 2007.

Stockholm International Peace Research Institute: Holmqvist, C.,"Engaging non-state actors in post conflicts settings," (eds.) Bryden, A. and Hänggi, H., Security Governance and Post-conflict Peacebuilding, Geneva Centre for the Democratic Control of Armed Forces, DCAF (Berlin: Lit Verlag, 2005). [http://www.sipri.org/contents/conflict/nonstateactors.html](); Internet, accessed 14 Apr 2007.

Strategy 2020. http://www.cds.forces.gc.ca/pubs/strategy2k/s2k07_e.asp; Internet, accessed 7
    Mar 2007

The Canada Institute of the Woodrow Wilson International Center for Scholars and the Canadian
    Centre of Intelligence and Security Studies (CCISS) at Carleton University co-hosted a
    publication launch and panel on the topic of Canada-U.S. bilateral security and intelligence
    relations. Intelligence Sharing Between the United States and Canada Event Location:
    Ottawa, Canada, January 29 2007, 8:30 a.m. - 12:30 p.m.
    http://www.wilsoncenter.org/index.cfm/topics/topics/index.cfm?topic_id=1420&fuseaction=t
    opics.event_summary&event_id=214721; Internet; accessed 14 Apr 2007.

The Criminology of Terrorism: History, Law, Definitions, Typologies.
     http://faculty.ncwc.edu/TOConnor/429/429lect01.htm; Internet, accessed 14 Apr 2007.

The Media and Terrorism: A Reassessment. Paul Wilkinson.Terrorism and Political Violence.
    Vol9 No2 (Summer 1997)published by Frank Cass London.
    http://www.st-
    andrews.ac.uk/academic/intrel/research/cstpv/pdffiles/The%20Media%20and%20Terrorism.
    pdf; Internet, accessed 14 Apr 2007.

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks
    Upon the United States: Official Government edition, Washington DC
    http://www.gpoaccess.gov/911/index.html; Internet, accessed 14 Apr 2007.

UAV Trial. http://www.forces.gc.ca/site/Newsroom/view_news_e.asp?id=1433; Internet,
    accessed 7 March 2007.

United Nations Counter terrorism. http://www.un.org/terrorism/; Internet, accessed 14 Apr 2007.

United Nations Report on Terrorism dated 2006, http://www.unodc.org/images/A60288.pdf;
    Internet, accessed 10 Apr 2007.

US State department list of Terrorist organizations. http://www.state.gov/s/ct/rls/fs/37191.htm;
Internet, accessed 5,18 Mar 2007.

United States of America: US PATRIOT Act October 24 2001
    http://www.epic.org/privacy/terrorism/hr3162.html; Internet, accessed 14 Apr 2007.

Wilkes, Jon. The Integrated Data Environment: A new tool for Interoperability and effective data
    Integration for Command and Control.
    http://www.il.wroc.pl/czasopisma/JTIT/2003/4/32.pdf; Internet accessed 16 Apr 07.