Information-Sharing for Counter-Terrorism in Canada after 9/11: Issues in the Administrative Coordination of Multi-Agency Intelligence

---

A Comparative Study between Canada, the UK and Australia

Fall/Winter 2014

Richard Mah, MPA Candidate
University of Victoria, School of Public Administration
For Client Insp. Kenneth Burton, OIC Support Services, Pacific Region Training Centre, RCMP
Supervised by Dr. Emmanuel Brunet-Jailly, Associate Professor, University of Victoria

"The [counter-terrorism] agencies are like a set of specialists in a hospital, each ordering tests, looking for symptoms, and prescribing medications. What is missing is the attending physician who makes sure they work as a team"

- The 9/11 Commission Report (2004)

"…government is not a machine, but a living thing. It falls, not under the theory of the universe, but under the theory of organic life. It is accountable to Darwin, not to Newton… … Government is not a body of blind forces; it is a body of men, with highly differentiated functions, no doubt, in our modern day of specialization, but with a common task and purpose. Their cooperation is indispensable, their war-fare fatal. There can be no successful government without leadership or without the intimate, almost instinctive, coordination of the organs of life and action.

-Woodrow Wilson in Constitutional Government in the United States (1908)

EXECUTIVE SUMMARY

Objectives

This paper will analyze key problems in the public administration of security information-sharing policy objectives introduced in Canada following the 9/11 terrorist attacks in the United States. This paper will also present a possible solution to the problems identified.

Background

The tragedies of Air India Flight 182 and September 11, 2001 (9/11) painfully demonstrate what can go wrong when information is not shared in the field of public safety and counter-terrorism. Analysis of the 9/11 terrorist attacks revealed that, in the days leading up to the attacks, the U.S. government failed to share and integrate key pieces of information on the terrorist group al-Qaeda. As a result of these information-sharing failures, critical opportunities to capitalize on investigative leads and intervene in the terrorist plot were missed. In Canada, there was a similar inability within government to share and integrate information before the 1985 terrorist bombing of Air India Flight 182. A subsequent inquiry into the attack concluded that the Canadian government was also collectively in possession of sufficient information warning of the attack. In both cases, the failure to share information between the agencies collectively responsible for public safety resulted in a failure to appreciate the nature and extent of the terrorist threat until too late.

After 9/11, public demands for greater security and safety, driven primarily by fears of another terrorist attack, brought about sweeping changes to national security and public safety policies. These changes reflect the aspiration to design an intelligence-led, pre-emptive, and whole-of-government approach to counter-terrorism. While governments wanted to avoid repeating the same mistakes and avoid another intelligence failure, the Air India and 9/11 terrorist attacks also underscored a deeper shift with respect to public security and safety. Contemporary terrorist groups, such as al-Qaeda, for example, exemplify a new and dangerous terrorist threat environment. Today's terrorist groups are described as being increasingly dangerous, networked, transnational and elusive, driven by absolutist and distorted religious ideology. Information-sharing after 9/11, as such, has also come to underpin new security strategies to cope with greater uncertainty with respect to threats to public safety as well as to support strategies of pre-emptive defense against future terrorist attacks.

Summary of Methods

The following methods were used to achieve the project objectives; a literature review, a comparative analysis, and a best practice scan. A review of the literature was conducted using the University of Victoria library as well as the Royal Canadian Mounted Police (RCMP) Canadian Police College Library. Results from the search were used to conduct the best practice scan and comparative analysis. A best practice scan was conducted to summarize the best practices,

methods of implementation, the participants involved, as well as the reasons for and the challenges with information-sharing in other organizations. A comparative analysis was used to compare post 9/11 information-sharing systems between Canada, the UK and Australia. Similarities and dissimilarities between the information-sharing systems were then summarized. A best practice scan was conducted to summarize the reasons for and the challenges with information-sharing in other organizations, including the methods of implementation and the participants involved. A comparative analysis was used to compare and contrast the post 9/11 information-sharing systems found in Canada, the UK and Australia. Similarities and dissimilarities between the information-sharing systems were then summarized.

Findings

A review and comparison of the changes to institutional reforms relating to post-9/11 counter-terrorism initiatives indicate that Canada, the UK, and Australia have all responded to the demands for post-9/11 information-sharing in a similar fashion. Information-sharing mandates were commonly operationalized by way of “Integrated Teams” and “Integrated Threat Assessment Centres.” Integrated Teams involve the creation of new inter-agency security institutions designed to overcome information-sharing failures and problems of fragmentation. Integrated Teams attempt to achieve these objectives by bringing together, or "co-locating" representatives from various security-related agencies, such as policing and intelligence officers, but also border enforcement, military and immigration officers. Within the Integrated Team environment, participants work closely together at the operational and investigative level. In this respect, integrated teams are similar to a “task force” in that they serve as a mechanism for inter-departmental coordination and integration. Integrated Teams differ, however, in that they are a more permanent operational program that possesses their own operating and management structure.

Integrated Threat Assessment Centres (ITAC), on the other hand, illustrates efforts to share information at the strategic and government advisory levels by combining and centralizing high-level intelligence products and assessments. ITACs were introduced after 9/11 and represent a significant organizational restructuring of public-safety and counter-terrorism resources. Similar to integrated teams, ITACs bring together or “co-locate” representatives from among the various intelligence, policing and security agencies within governments. ITACs were commonly found to be located centrally within the intelligence community and function as the state’s so-called “nerve center” for intelligence analysis and dissemination. In this central position, ITACs also typically provide strategic and operational planning advice to both the executive branch, on threats to its security, as well to individual departments with respect to providing direction for intelligence planning and priorities. In all three countries, desires to integrate separate computer databases, often referred to as networked interoperability, were also noted. We found that computer inter-operability was not yet fully realized in Canada, the UK or Australia.

By situating information-sharing policy within their international context, we also found that information-sharing practices in the Canadian context are uniquely influenced by US concerns over

their domestic security vis-à-vis the Canadian-US border. Unlike the UK and Australia, information-sharing in Canada also occurs within the context of securing its southern border from terrorist incursions, while at the same time ensuring the borders remain open for trade.

In order to assess the performance of the post-9/11 integration model generalized above, we examined recent counter-terrorism experiences in the UK and Canada. These are the 2005 London Bombing attacks in London, UK, as well as the 2004 and 2008 Auditor General Reports on national security initiatives in Canada. Together, these events suggest that the information-sharing initiatives outlined above have not been effective in achieving their policy objectives of greater information-sharing.

The enduring nature of information-sharing problems suggests a deeper and more systemic coordination problem. An analysis of classical administrative theory suggests that there are limits to the traditional bureaucratic model's ability to unify contemporary counter-terrorism work. Information-sharing initiatives appear to confront a longstanding tension in the contrariety between organizational differentiation and integration. In other words, there appears to be conflicting demands between the requirement for more integrated forms of organization on one hand and the requirements for organizational specialization and differentiation on the other. A greater demand for horizontality is mainly a consequence of counter-terrorism work that seeks to employ innovative conceptions of intelligence analysis in response to a new and evolving threat environment. These tensions are manifest in organizational problems such as increasing fragmentation, jurisdictional and functional overlap, as well as principle-agent problems and information hoarding.

Recommendations

In reality, coordination and integration problems have been around for some time, representing an inherent and permanent problem of governance. Administrative coordination problems, moreover, arise in most spheres of socio-economic and political life (Deputy Minister Task Forces, 1996, p. i). With respect to information-sharing and the post-9/11 counter-terrorism mission, the coordination problem is especially pronounced. If the enduring failures to share information are rooted in structural coordination and integration failures, however, then one possible way forward would be to consider alternative models of organizational coordination. Recent horizontal approaches to management are one such alternative.

A brief analysis on the horizontal management literature suggests that innovative and non-traditional modes of coordination may offer a potential solution to the problem of information-sharing. A horizontal model may provide a more effective means for operationalizing information-sharing policy objectives. The collaborative, networking and enhanced decision-making benefits of the horizontal design, however, appear to be based on a fundamentally different view and understanding of organizations. In particular, the horizontal design’s emphasis on non-traditional, networked and participative forms of decision-making represents a significant departure from the traditional bureaucratic model. Further study in the use of more horizontal management models,

in the field of counter-terrorism and public safety, are therefore suggested, namely: (i) whether the necessary accountability mechanisms within a horizontal management model are sufficient for ensuring good governance consistent with the values of a liberal democracy, and; (ii) potential implications of the rapidly evolving Digital Age on information-sharing regimes.

Table of Contents

1. INTRODUCTION

Project Objective

This paper will analyze key problems in the public administration of security information-sharing policy objectives introduced in Canada following the 9/11 terrorist attacks in the United States. By way of solution, this paper reviews the potential application of the horizontal management approach to the administrative problems found in information-sharing.

Project Rationale

The RCMP, together with its partners, plays a crucial role in ensuring public safety having responsibility for the primary investigation of criminal offences related to terrorism and espionage. The RCMP, moreover, recognizes that no individual agency or department holds all the relevant information or clues necessary to combat today's terrorist enemies. As a result, any failure to share information on the RCMP's part, which could have reasonably been expected to prevent or disrupt a terrorist attack, would likely result in significant damages. These damages can include the diminishment of the RCMP's reputation, increased costs to civil society, and damages to Canada's relations with its international allies. As such, senior managers and security practitioners in the RCMP wish for this project to build upon its research and policy capacity in order to support its role in achieving the goals of effective information sharing.

The RCMP's Regional Departmental Security Section (DSS) will be the primary client and is responsible for ensuring the operational integrity and readiness of the RCMP. As part of this responsibility, DSS works to ensure that the Government of Canada's Departmental Security Management and Operational Security Standards are met, and, in particular, that information is protected throughout its life cycle. DSS, therefore, plays a crucial role in ensuring the confidentiality, integrity and availability of RCMP information. This responsibility includes the mandate to safeguard information from improper disclosure, use, disposition or destruction. DSS works to ensure the effective security of information through a systematic approach that identifies and categorizes information and associated assets, assesses risks to them, and implements appropriate personnel, physical, and IT safeguards.

Project Scope

Several significant changes were made to Canada's counter-terrorism capabilities after 9/11, such as the strengthening of police powers in order to investigate and prevent terrorist acts. The scope of this paper's analysis, however, was limited to the institutional structures, activities and context related to the implementation and public administration of information-sharing policy objectives introduced after 9/11. In addition, the paper was limited to information gathered and analyzed through open sources only. No confidential information was accessed or used for this paper.

The Key Questions or Issues Addressed in the Project

The following key questions were raised in the project:

1. What is information-sharing?
2. Why is information-sharing an important policy problem?
3. What is specific or unique about security or intelligence information gathering?
4. How is information-sharing accomplished in the UK and Australia?
5. How is information-sharing accomplished in other organizations or sectors?
6. Is there an enduring failure to share information, and if so, why?
7. What are some possible solutions to the problems identified?

Project Methods

The following methods were used to achieve the project objectives, namely: a literature review, a comparative analysis, and a best practice scan. First, a review of the literature was conducted using the University of Victoria library, the RCMP's INFOWEB, and the Canadian Police College Library.

We simultaneously searched the following databases: The EbscoHost databases, Academic Search Complete, PsycInfo, Military and Government Collections, Google Scholar, Google Canadian Government Document Search using the following search parameters.

> ("information sharing" or "information integration" or "intelligence sharing" or "knowledge sharing") and (governmental or organizational or intergovermental or interorganizational or "cross boundary" or "inter-agency") and (challenge* or problem* or obstacle* or impediment* or difficult*).
>
> ("information sharing" or "information integration" or "intelligence sharing" or "knowledge sharing") and (counter-terrorism or anti-terror* or terror* or 9-/11 or security or safety or intelligence) and (UK or United K* or Canada or Australia)

Results were limited to between 2002 to 2014, and peer reviewed articles were selected.

Results from the search were used to conduct the best practice scan and comparative analysis. A best practice scan was conducted to summarize the reasons for and the challenges with information-sharing in other organizations, including the methods of implementation and the participants involved. A comparative analysis was used to compare and contrast the post 9/11 information-sharing systems found in Canada, the UK and Australia. Similarities and dissimilarities between the information-sharing systems were then summarized.

2. INFORMATION SHARING FOR PUBLIC SAFETY: AN IMPORTANT POLICY PROBLEM?

There has been a change in the management of public safety in Canada since the September 11, 2001 (9/11) terrorist attacks. This change was precipitated by a failure to produce actionable intelligence that could have prevented the Air India Flight 182 and the 9/11 terrorist attacks. As a result, governments sought to reform intelligence institutions in order to deliver a coordinated and "government-wide" approach to counter-terrorism. In particular, reformers argued for closer inter-agency information-sharing and collaboration, especially between policing, intelligence, immigration and border security agencies. Post-9/11 reforms also reflect an ambition to design a more pre-emptive and preventive approach to counter-terrorism.

Information-Sharing Failures: Air India Flight 182 and September 11, 2001

On 23 June 1985, the Sikh extremist group Babbar Khalsa destroyed Air India Flight 182, killing 329 people on board. The subsequent investigations into the terrorist attacks revealed a lack of information-sharing between the Canadian Security Intelligence Service (CSIS), the RCMP, Transport Canada, and the Communications Security Establishment (CSE). As a result, opportunities to investigate and interdict the lead planner of the attack, Talwinder Singh Parmar, were lost. The inquiry, led by Justice John Major, concluded that the Canadian government, on the whole, held sufficient information warning of the bombings but key pieces of information were not shared or considered together. As a result, nobody knew or learned of the full extent of the terrorist plot that year (Major, Volume 1 Overview, 2010, p. 98). While Canadians were deeply concerned over these intelligence failures, the problem of inadequate information-sharing did not move to the forefront of public consciousness until after 9/11 (Roach, 2010, p. 179).

On 11 September 2001, Islamist terrorist group al-Qaeda hijacked four commercial airline jets and crashed two of them into the World Trade Centre. The third aircraft crashed into the Pentagon while the fourth jet ran into the ground. 2973 US civilians were killed (National Commission on Terrorist Attacks upon the United States, 2004, p. 311). The subsequent inquiry into the attacks, later known as the 9/11 Commission Report, concluded that there was a failure to share information between government departments. The Commission argued that there were several opportunities to capitalize on investigative leads and uncover the terrorist plot, but these were lost due to poor information-sharing (Jones, 2007, p. 388). For example, critical pieces of information were never exchanged between the FBI and the CIA on the 9/11 terrorists Khalid al Mihdahr and Hazmi “Khallad”. Mr. Mihdhar’s suspicious travel history and connections with Mr. Khallad were never connected with the FBI’s ongoing investigation into Mr. Khallad's involvement in the USS Cole Bombing (National Commission on Terrorist Attacks upon the United States, 2004, p. 272). In their explanation of these failures, the Commission was especially critical of the missed opportunity to connect two separate investigations done independently by the FBI and the CIA. In particular, the *Foreign Intelligence Surveillance Act* (FISA) was singled out as responsible for

creating the so-called "wall" that separated criminal investigations from intelligence investigations. This division of investigations thus served to block the flow of information between the FBI and CIA, as well as between internal sub-units within the FBI (National Commission on Terrorist Attacks upon the United States, 2004,p. 78).

A New Reality of Networked, Diffuse and Dangerous Terrorist Threats?

The 9/11 and Air India Flight 182 terrorist attacks focused attention on the problem of inadequate information-sharing. However, the attacks also substantiated growing concerns that radical Islamist terrorist groups such as al-Qaeda signaled the arrival of a new threat environment (Swire, 2006, p. 955). U.S. president George W. Bush, for example, argued that "... [the] new realities and dangers posed by modern terrorists … represented a threat like no other …". Bush added that "[t]he changing nature of the threats facing America requires a new government structure to protect against invisible enemies that can strike with a wide variety of weapons" (Bush, 2002, DHS). UK Prime Minister Tony Blair similarly spoke of "... a new global terrorism driven, not by a set of negotiable political demands, but by religious fanaticism". In Australia, Gordon Brown similarly remarked that "[t]he new terrorist threat… multi-dimensional in its operation – has changed the rules of the game – and so changed how we need to protect ourselves against it" (Field, 2009, p. 196). In summary, government officials and political leaders pointed to a sea-change in the nature of contemporary terrorist threats and so correspondingly called for a new counter-terrorism strategy. What follows is a brief outline of the key differences often made between today's terrorist groups and past terrorist groups.

First, there has been a noted increase in the use of violence inspired by religion since the mid-1990's. In contrast to terrorist events between 1960-1980, terrorist motives were predominantly described as concerned with the right to self-governance or national separatist aspirations (Commission of Inquiry, Research Studies, Vol. 1, 2010, p. 20). Another significant distinction between "old" and "new terrorism", therefore, lies in the apparent increase in the use and distortion of religious texts to motivate and inspire acts of terrorism.

The terrorist group al-Qaeda and other Islamist terrorist leaders, for example, draw their motivation from a long tradition of extreme intolerance within factions of radical Islamism. Such camps include the Ibn Taimiyyah, Wahhabism, the Muslim brotherhood, and Sayyid Qutb. These factions are galvanized by the U.S. military presence in the Middle East, U.S. support for Israel in the Arab-Israel War, and over the perception that U.S. policies are inherently anti-Arab. Osama Bin Ladin and other Islamist terrorist groups, for example, identify America as the "font of all evil" and the "head of the snake" that must be converted or destroyed (National Commission on Terrorist Attacks upon the United States, 2004, p. 362). al-Qaeda's plans, moreover, are known to consist of seven stages that end with the ultimate goal of the implementation of Shariah Law. The years 2010-2013, for example, is "Stage Four", which targets secular regimes in Egypt, Jordan and Saudi Arabia for attacks. "Stage Five" occurs in 2013-2016, where al-Qaeda leaders predict the increase in Islamic influence in the world, with a parallel decline in U.S. and Israel power. The "sixth stage" involves an all-out war between ''believers'' and ''infidels'", and finally the seventh stage has as its

goal the implementation of Shariah Law by 2020. Other al-Qaeda objectives include the withdrawal of U.S. forces from Iraq, the creation of an Islamic state in at least part of Iraq, expanding the jihadist struggle into neighboring countries, including Egypt, Jordan, and Syria, and launching attacks against Israel (Shpiro, 2012, p. 243).

The religious dimensions of new terrorism create a new danger in that it seems to suggest to terrorists that there is a religious duty or imperative to eliminate one's enemies. The absolutist and religious nature of terrorist goals is dangerous because it could lower the psychological constraints to mass murder or genocide, and instead present them as an acceptable or desirable necessity in achieving a new religious order. Religious texts can also be distorted to portray violence as the ultimate expression of a terrorist's "religious" faith. The potential to lift the psychological and political constraints to mass and indiscriminate killings is, therefore, another distinguishing characteristic of new terrorism (Field, 2009, p. 197). Former terrorist groups feared that mass indiscriminate killings would alienate their political base of support. Today's terrorist, however, can distort religious texts to regard violence as morally justified and necessary (Commission of Inquiry, Research Studies, Vol. 1, 2010, p. 29). For this reason, some government officials warn that the threat posed by contemporary terrorism should cause grave concern. The threat is exponentially more dangerous should terrorists gain the capacity to deploy Weapons of Mass Destruction (Ackleson, 2005, p. 139).

The rise of transnational and non-state actors as a potent threat to public safety is another defining characteristic of new terrorism (9/11 Commission Report, 2004, p. 47). There are several implications of such a new threat. First, threats to national security now can emerge quickly and unpredictably. During the Cold War, threats emerged gradually and relatively visibly as enemies had to mobilize considerable military resources (9/11 Commission Report, 2004, p. 362). The predominant concern, moreover, was the threat of a large-scale missile attack from the Soviet Union and its allies. Tools were developed such as satellite imagery and high-altitude airplanes in order to track enemy tanks and missile sites (Swire, 2006, p. 957). Cold War adversaries also used familiar methods of command-and-control methods, with the result that their movements were relatively predictable. Due to these features, governments could study enemy movements with some visibility and predictability, with security efforts focused largely on trying to determine the intentions and capabilities of the Soviet Union and its allies (9/11 Commission Report, 2004, p. 88).

Today's terrorist groups, on the other hand, tend to organize through flexible and network-based affiliations rather than through traditional command-and-control structures. al-Qaeda, for example, does not operate with clear or unified lines of communication. Their activities and operations, as such, have little central control or oversight. Rather, al-Qaeda's organizational structure is characterized by their networked yet loosely affiliated "cells" that can operate independently of another. This operating structure makes today's terrorists more difficult to identify and track (Jones, 2007, p. 397). al-Qaeda also recruits members through local radicalization and recruitment campaigns as well as internet propaganda. Recruits are often encouraged to form covert terrorist cells of their own and propagate jihadist ideologies (Shpiro, 2012, p. 241). In addition, terrorist cells also employ asymmetrical tactics of terrorism to launch

surprise attacks on civilian population (Air India, Research Studies, Volume 1: Threat Assessment RCMP/CSIS Co-operation,p. 73).

As such, governments were no longer in a position to assume that threats would unfold incrementally or gradually among state-based opponents as they did in earlier large-scale conflicts. (9/11 Commission, 2004, p. 362). The lack of an external territory or asset that could be easily destroyed also meant that conventional warfare tactics were less effective in ensuring security than before (9/11 Commission, p. 348). Large powerful states had more to lose in a war, and therefore were more easily deterred than modern terrorist groups (9/11 Commission, 2004, p. 362). The imperative to stop another potential terrorist attack placed tremendous pressure on officials to identify and disrupt potential terrorist plots. One consequence of new terrorism, as such, was the need for new, innovative and cutting-edge intelligence.

Thus, it is in this context of new terrorism that the existing bureaucratic mechanisms for intelligence and information-sharing were increasingly seen as inadequate. In the face of a new and emerging, diffuse yet networked terrorist threat, the traditional bureaucratic model appeared ill-equipped, slow and inadequate. This sentiment was articulated by the Commission when it argued that the 9/11 terrorist attacks demonstrated that:

> … doing business rooted in a different era are just not good enough. Americans should not settle for incremental, ad hoc adjustments to a system designed generations ago for a world that no longer exists. We recommend significant changes in the organization of the government (National Commission on Terrorist Attacks upon the United States, 2004, p. 399).

Thus, the call for a new way of organizing intelligence in the U.S. rested on the argument that the current intelligence community was founded largely on outdated assumptions. In particular, the security institutions that failed to prevent the 9/11 attacks were seen as built on experiences and assumptions from past conflicts such as the Cold War.

3. NEW INTELLIGENCE FOR NEW TERRORISM: INFORMATION-SHARING'S INTELLECTUAL FRAMEWORK

The demands for intelligence reforms reflect aspirations to implement innovative conceptions of intelligence analysis in response to past intelligence failures, but as well to cope with the new and evolving threat environment. What would emerge after 9/11, in other words, was a new framework for intelligence underpinned by information-sharing systems. What follows is a brief discussion on the underlying logic of information-sharing, as well as an outline of the process of information collection in the context of counter-terrorism and the international intelligence community.

The Logic of Information-Sharing

In their concluding chapters "A Different Way of Organizing the Government", the 9/11 Commission called on the US government to reforms its intelligence and security institutions in order to become a "smart" government that was capable of integrating "all-sources" of information in order to "see the enemy as a whole" (9/11 Commission Report, 2004, p. 400). These recommendations were advanced in the *Intelligence Reform Act* (2004), which instructed the President to implement an "Information Sharing Environment" (ISE) to serve as the new framework for intelligence (Jones, 2007, p. 385). As well as in Canada, information-sharing was emphasized in their first national security policy "Securing an Open Society". While not codified to the extent of the U.S., the policy does provide a high-level framework for a more integrated approach to counter-terrorism that aims to "…reduce the risk that information held by one part of Government will fail to be provided in a timely fashion to those who can utilize it" (Securing an Open Society, 2004, Ch. 2, p. 18). Moreover, several high-profile inquiries into intelligence failures in Canada have also led to similar conclusions on the need for information-sharing.

For example, the Auditor General, in his analysis on the state of national security and anti-terrorism initiatives following 9/11, commented that intelligence after 9/11 is increasingly conceived of as "the collection, evaluation, analysis, integration, and interpretation of all available information". The AG went on to point out that "… information on known or suspected terrorist and potential threats, vulnerabilities, and previous events exists in many forms and in many places" (Office of the Auditor General, 2004, Ch. 3, p.15). In his inquiry into the Air India Flight 182 bombings, Justice John Major similarly argued for all-source analysis. Major argued that the essence of good intelligence is when disparate facts from diverse sources are pulled together in order to assemble a larger pattern. Major added that it is only when enough information is pooled together can seemingly insignificant new additions of information lead to new or deeper understandings (Major, 2010 Vol 1, p. 97). In the UK, it was similarly argued that effective counter-terrorism must be ensured by providing the capabilities to "… bring to bear all sources of intelligence in a co-ordinated way" and that successes are achieved "… through close collaboration

between all involved piecing the intelligence picture together, with teams able to have shared access to all available intelligence" (UK Butler, 2004, p. 142).

The underlying logic of information-sharing is that by considering seemingly disparate or inconsequential pieces of information together, new insights or connections can be gained that are not otherwise apparent when viewed in isolation. This method is also known as "all-source analysis" or the "mosaic-effect" within the intelligence community. Specifically, by increasing the flow of information from "all available sources" governments would bolster their ability to detect a terrorist enemy that was increasingly elusive, diffuse and de-centralized. As well, if today's terrorist enemies could be hiding anywhere, then it would follow that information warning of an attack could also be hiding anywhere (Jones, 2007, p. 397). The goal of all-source analysis has thus expanded the range of actors that now contribute to the overall counter-terrorism efforts. The general duty police officer, for example, now occupies a crucial role in counter-terrorism as intelligence agencies seek to leverage their established and extensive contacts within the communities they serve. Local police knowledge can be a crucial source of information with respect to discovering terrorist activities (Bayley, 2009, p. 82).

The notion of information-sharing is not an entirely new concept, however. In 1949, Sherman Kent advocated the vast accumulation of information in order to predict and thus prevent an enemy attack. Kent considered intelligence as a form of knowledge that could be divided into three general categories, namely: "basic descriptive" knowledge or descriptions of the world as it is; the "current reportorial" knowledge, or descriptions of the day-to-day changes in the world; and "speculative-evaluative" knowledge, or predictions about how the world will change. Thus, to produce predictions about how the world will change, Kent called for the collection of vast quantities of information, in what were later referred to as "encyclopedias of information". Such encyclopedias would serve the purpose of creating basic descriptive knowledge, which, in turn, provides the foundation for producing speculative-evaluative knowledge. In this model, information would become somewhat synonymous with intelligence. Critics of Kent's model, however, were sceptical with respect to the question of how well analysts could be expected to predict future events, as well as exactly how much information was needed to accomplish this. In either case, Kent's idea about the role of intelligence and the intelligence analyst in particular to provide predictive analysis proved influential. Indeed, Kent's model was later embraced with the creation of the Central Intelligence Agency (CIA) in 1947, which followed the intelligence failures to predict the Pearl Harbour surprise attacks. The CIA was subsequently created to act as a central coordination hub for the integration of "all sources of information" (Jones, 2007, p. 386).

In summary, the logic of information-sharing were advanced in Canada, the UK and Australia as well as in the US. These countries were concerned with a more integrated and preventive approach to counter-terrorism in order to avoid past intelligence failures but as well to combat new terrorism (Jones, 2007, p. 388).

Information-sharing for Public Safety and Counter-Terrorism

The gathering and collection of information for the purposes of counter-terrorism occur within a secretive, extraordinary and international context. States such as the US, Canada, Australia and the UK, for instance, have established an extensive and global network of intelligence capabilities. These capabilities range from human agents or "assets" on the ground to computers capable of surveilling their targets from "land, sea, or air" (Mutton, 2013, p. 671). These capabilities are commonly referred to as the intelligence tradecraft and have a specific nomenclature. Human source intelligence (HUMINT), for example, is information that comes from a human source and is often targeted for disrupting terrorist recruitment, training, resourcing, incitement and planning. Signals Intelligence (SIGINT) refers to signals intelligence and usually means information gathered from intercepted communications. SIGINT is mostly targeted for intervening in terrorist propaganda and tactical planning. Financial intelligence (FININT) is collected for the purposes of thwarting terrorist resourcing. Imagery Intelligence (IMINT) typically comes from satellites and other aerial reconnaissance vehicles for the purposes of reconnaissance on prospective targets (Rudner, 2010, p. 132).

To organize and provide a framework for these methods, policy-makers typically guide intelligence efforts according to the "intelligence lifecycle". The intelligence lifecycle organizes the flow of intelligence activities into distinct phases, specifically the: planning and direction, collection, processing, production and analysis, and dissemination phases. In practice, these steps are not sequential. The model nonetheless remains useful for conceiving of intelligence activities as a flow of activities between their collection and interpretation or analysis (Johnson, 2010, p. 2). The goal of intelligence collection is to provide decision-makers and policy-makers with "a blend of secret and public" information to inform decision-makers on how best to respond to a terrorist threat. Another way to characterize the work of an intelligence agency is to see them as the "producers" of information assessments and the policy-makers as the end "consumers" (Johnson, 2011, p. 649).

Intelligence collection also follows a complex identification and prioritization process known as a strategic "threat assessment." What information to collect and how frequently, in other words, is determined by a study of what threats or forces are capable and probable of inflicting harm to the state. The typical threat assessment is composed of three areas: the actors targeted, such as a terrorist individual or group; the type of information sought, such as military, economic or political; and the level of geographic focus, such as global or regional (Johnson, 2011, p. 642). The scope of intelligence collection activities, as such, is influenced by policy officials who "task" intelligence agencies with areas of interests or defined priorities. Intelligence collection, however, can also occur without formal assessments or tasking. For example, the National Reconnaissance Office (NRO) in the U.S. is estimated to process 400 hundred satellite photos a day. The NRO also processes a steady inflow of SIGINT and HUMINT reports from the NSA and the CIA. The collection and processing of this information, however, is not necessarily specific to any particular case, but rather the information is stored for later "mining" should its subject matter become of importance later. Indeed, analysts and their computers at the NRO cannot keep up with the analysis of such a

large volume of data (Johnson, 2010, p. 8). Today's information collection, as such, can also operate under the assumption that one should gather as much information as possible for the sake of future analysis (Berman, 2014, p. 31).

Despite these impressive capabilities, intelligence agencies face limits to what they can collect in terms of scarcity of resources and opportunities given that the world is so vast. Even the most resourceful states cannot collect information on all threats across the globe, or as U.S. intelligence officials sometimes call it, achieve “global transparency” (Johnson, 2010, p. 5). One way states address these natural limitations is to develop liaison relationships with other foreign intelligence agencies. Thus, an additional dynamic of intelligence collection is that it occurs within the particular context of international cooperation and relations with respect to state security and military strategy. Indeed, international intelligence sharing is an integral part of Canada’s intelligence activities.

For instance, the intelligence agreement between the UK, U.S., Canada, New Zealand and Australia under the UK-USA agreement, also known as the “Five Eyes," involves a high level of information-sharing. The agreement involves the daily routine sharing of a vast amount of information, with each member state contributing and drawing from an integrated communications monitoring and processing system. The agreement, moreover, allocates collection responsibilities, such as which country covers which subjects at which locations. The UK, for example, benefits from U.S. imagery intelligence, while the U.S., in return, receives UK HUMINT as well as SIGINT and code breaking analysis. Such an agreement overcomes the burden of having to collect intelligence, or cover a particular region, by themselves (Mutton, 2013, p. 671). Moreover, in the international context of military strategy and warfare, intelligence agencies also play a role in advancing the interests of their country, usually through clandestine and manipulative means. Other activities, as such, can also include counter-intelligence operations in order to safeguard state secrets from adversaries (Johnson, 2010, p. 1).

4. INFORMATION-SHARING PRACTICES AND CHALLENGES IN OTHER ORGANIZATIONS

The goals of information-sharing and the benefits they promise are not unique to the field of counter-terrorism. Similar efforts to share and integrate information can be found in other sectors and industries. A review of the literature on information-sharing found the following fields to have information-sharing as an organizational objective, namely: healthcare, social work and child welfare, business and manufacturing, construction and project management, and local government and city administration. What follows is a definition of information-sharing at the organizational level, then a survey of how information-sharing is being pursued, as well as the particular challenges noted in each of the above-noted industries.

Information-Sharing across Organizations

In its most basic form, information-sharing refers simply to the voluntary act of making information available to others. Information-sharing as an organizational process, however, is more complex. A more useful definition, therefore, is one that includes information-sharing to be a process that involves:

> the transfer of information from a holder entity that is willing, able, and entitled to provide the information to a receiver entity that is able to demonstrate the need for the information, is able to receive it, and agrees to abide by usage rules set by the holder" (Pardo, 2008, p. 9).

Information-sharing is about creating "… an organizational mechanism from which to create communication channels that can give participants access to other information and knowledge with the expectation that more complete information will be available to those who need it, when they need it" (Dawes, 2009, p. 393).

The concept of information-sharing, moreover, is closely related with the concepts of process integration and information systems inter-operation. The relation is based on the notion that system inter-operation and information integration are pre-requisites to effective information-sharing. In other words, whenever information is to be shared between organizations, some interoperation of systems and integration of information or process have to be established (Scholl, 2012, p. 313). Information integration can be conceptualized as, "the forming of a larger unit of organizational entities, temporary or permanent, for the purpose of merging processes and/or sharing information" (Bigdeli, 2013, p. 817). Such conceptions see information integration as concerning aspects of high-level governance. Inter-operability, on the other hand, is sometimes presented as a concept concerning lower-level technical aspects of information-sharing. Such technical means typically refer to Information Technology systems (IT) and their ability to exchange information across system borders, whereas notions of cooperation, a common cross-

organizational strategy and implementation properly being issues of institutional governance (Pardo, 2008, p. 10).

Other researchers minimize the distinction between the two concepts, preferring to present them along a continuum of interconnected factors ranging from the social to the technical, thus emphasizing both the social and technical elements of information-sharing. This approach serves to highlight information-sharing's inherent complexities. The factors along this continuum are: a "trusted social network," "shared knowledge and information," "integrated data", and "interoperable technical infrastructure" (Bigdeli, 2013, p. 817). A trusted social network is a set of collaborations between those persons exchanging information and who trust each other at the fundamental stage of exchanging information. The flow of knowledge, whether in tacit or explicit form, refers to shared knowledge, often taking the form of formal documents, emails, messages and information relationships. Integrated data, on the other hand, refers to the integration of data at various levels in an organization, which usually requires an agreement on information standards in a networked organization. Lastly, the definition of an interoperable technical infrastructure refers to the ability of separate and different information systems to "communicate with each other," transfer information, and use the information that has been transferred (Pardo, 2008, p. 10).

Healthcare

In the field of health care, improved information-sharing is increasingly becoming an organizational objective for several reasons. First, information-sharing and coordination between medical specialists is being presented as a way to treat diseases in a more cohesive and holistic way. Second, information-sharing is also seen as a way to improve continuity of care and "real-time" decision-making by bedside clinicians and emergency room staff. Information-sharing is also a key objective in the international efforts to mitigate communicable diseases and prepare for pandemics. Last, the literature also shows that some rural hospitals look to information-sharing as a means to increase efficiency and performance in the face of increasing demands and fewer resources.

Information-sharing was studied extensively in the field of cancer patient care. It was argued that a more "systems-minded" cancer care organization was needed in order to promote a holistic approach to care and intervene when necessary to improve care coordination and continuity of care. The goal of information-sharing, as such, was to address some of the organizational problems relating to the coordination of multiple medical specialties involved in cancer care and the fragmentation of information that resulted. In particular, the lack of information-sharing between the primary and specialty care-givers was often cited as a key reason for why patients "fell through the cracks." Continuity of care was thus a common objective, which is defined as the "…systematic assurance of uninterrupted, integrated medical and psychosocial care of the patient" (Clauser, 2011, p. 202).

To achieve these goals, an agenda was put forward to "…aggregate all available data to enable meaningful use at the point-of-care and population level such that every consumer, doctor, researcher and institution has appropriate access to the information they need". This vision was operationalized through the Health Information Technology (HIT) knowledge management system. At the heart of the HIT is a centrally accessible database, designed to provide information to the multiple medical staff responsible for caring for patients with head and neck cancer (Clauser, 2011, p. 202). Complementing the new central database was the emergence of multi-disciplinary care centers. These centers emphasized "care coordination as a specialty challenge" and sought to enhance teamwork and communication involving treatment planning and execution among various specialties, namely cancer surgeons, radiation oncologists, and medical oncologists (Clauser, 2011, p. 205).

Studies of these initiatives have revealed that several challenges remain with respect to realizing a holistic approach to cancer care. One area that proved particularly challenging was overcoming staff concern regarding the accuracy of the information that was being shared. Some staff members were concerned that an error or misstatement made in one chart may be inadvertently propagated when shared electronically with another provider or system. In the medical field, the accuracy of the information is paramount as inaccurate information can lead to fatal errors (Clauser, 2011, p. 202). Another point of contention relates to the uneven benefits that arose from information-sharing. The financial benefits that were found in terms of improved quality, for example, did not flow to important members even though they had made important changes and contributions to information-sharing efforts. Some participants, as such, were questioning their incentive to participate (Clauser, 2011, p. 206).

The lack of coordination between different specializations is also evident in the work of mental health addiction. Information-sharing initiatives were noted in new joint collaborations between community addiction and mental health professionals in order to improve upon day-to-day problem solving. This included outreach and education services to parents with children coping with mental health and addiction issues, including Attention Deficit Hyperactivity Disorder (ADHD) (McLaren, 2013, p. 5). Efforts were mainly aimed at bringing the work of nurses and psychologists in the Adult Mental Health Services (AMHS) and psychiatrists in the Community Addiction and Mental Health (CAMHS) field together through co-location of staff and secondments (Mclaren, 2013, p. 5).

A review of the experience revealed several challenges to effective collaboration and information-sharing in the co-location approach to improving care in the community mental health and addiction field. First, the different cultural approaches to service delivery between CAMHS psychiatrists and AMHS psychologists were noted as key barriers to effective collaboration. For example, the psychiatrists that were focused on CAMHS work were said to be more family-oriented, inclusive and holistic than the psychologists concerned primarily with AMHS, who were perceived as crisis and medication intervention focused. CAMHS services were, therefore, seen as offering a more proactive approach to care, which raised concerns about the level of involvement and communication required of AMHS psychologists during post-transitions. These differences

also resulted in confusion between nursing and support staff with respect to different administrative methods such as record keeping and care planning between the two groups (Mclaren, 2013, p. 5).

Another area where information-sharing is increasingly used as a means of coordinating the work of different medical specialties can be found in the Emergency Medical Services (EMS) field. Here gaps were identified between the work of paramedics that arrive on scene and hospital staff, a gap commonly referred as the pre-hospital vs. hospital gap. Separate information systems were linked to address this gap to include the pre-hospital units, specifically with respect to capturing and analyzing time stamp data. It was hoped that this would specifically provide "end-to-end" data from the pre-hospital to hospital and trauma centre and ultimately improve service performance, reduce disability consequences and save lives. As a result of the newly integrated information system, paramedics were provided access to view limited demographic and medical emergency data prior to arriving on the scene. This information allowed them to improve their service by making important medical preparations in advanced, such as bringing the right equipment to the scene (Schooley, 2007, p. 780). The time-critical and life-saving dynamics of emergency response work have raised some significant challenges to information integration, however. The need for timely information that could be trusted was the biggest concern raised by the pre-hospital team. It was found that emergency professionals tend to take a cautious approach to new information technologies overall, with the adoption being somewhat slow given the fact that inputting data was typically the last thing on a responder's mind during life and death situations (Schooley, 2007, p. 756).

The obesity epidemic has also urged organizations to share information and seek greater collaboration. The Health and Physical Activity Network (HPN) in Canada, for example, brings together government and 34 community-based organizations that have a role in promoting positive lifestyles, such as health eating, physical activity and living smoke-free. While the majority of the participants in the network include schools and education boards, other partners also include local restaurants, grocery stores and workplaces. The network reflects the idea that in order to encourage and support healthy weights governments will have to urge cooperative action across all sectors and levels of government (Barnes, 2010, p. 238). One challenge noted with respect to the HPN network was power asymmetries between the participating agencies. Educational organizations and the school boards in particular were seen as holding the most power by virtue of their central position in the network and multiple links to health and social services organizations. The higher status of school boards was also attributed to some level of recognition by health promotion agencies that the most efficient and effective means to reach children and facilities was likely through the school boards. The power differences with other participating agencies meant, however, that other participating organizations such as community recreation organizations were relegated to minor roles in the network (Barnes, 2010, p. 246).

In Australia, a recent report by the National Health and Hospital Reform Commission argued that Australia's health system should make better use of their data. In particular, the report argued that data should enhance decision making, drive improvements in clinical practice, guide how

resources are marshalled and deployed and provide the basis for feedback loops to promote improvement in access to, and quality and efficiency of, care. In response, hospitals in Australia have taken on the task of integrating previously separate information-management systems with the goal of providing access of clinical performance data, especially with respect to hospital mortality data, to the clinician. Information-sharing as such was employed to improve the clinician's practice at the bedside, as well as the hospital's responsiveness to safety and quality issues in terms of triggering early preventative investigations (Lloyd, 2011, p. 30).

The sharing of information to clinicians revealed several challenges. A key concern was the timeliness and the usefulness of the information that was shared to the clinician. The data that was shared included mostly broad performance indicators, such as the number of admitted patients, infection rates, and waiting list times. These data proved to be of limited use to the clinician, who often required deeper knowledge. Clinicians also voiced their concern over the possibility of sharing erroneous or ambiguous information. There was a lack of confidence that the current information system provided the necessary context for understanding how the data was collected and defined, as well as the sources of the health data that were being circulated. To the clinician, the credibility of reported data is paramount and many were wary of drawing erroneous conclusions from information that was not yet validated or that showed inconsistencies (Lloyd, 2011, p. 28).

In the US, information-sharing is also increasingly used as a key strategy for improving the overall safety, effectiveness, and quality of health services provided. The US Health Information Exchange Initiative (HIE), for example, attempts to leverage Personal Health Information (PHI) in order to improve patient care. The pre-existing databases for PHI were typically isolated and fragmented within various hospitals, physical practices, laboratories and pharmacies. The integration of personal health information, however, is seen as growing in important in an increasingly mobile population. Several retired Americans, for example, receive treatment in very different locations, depending on the season. As well, increasingly prevalent chronic conditions, such as diabetes, can only be managed if information is shared to manage the patient's care. The sharing of PHI is also important in terms of patient safety and qualities issues in instances of handoff of patients between different medical specialists, and are complicated by changes in insurance coverage and reliance on multiple providers. As a result of these concerns, the sharing of patient-level electronic health records is now mandated under the *Health Information Technology for Economic & Clinical Health Act* (HITECH). The Act now requires that electronic health records be 'connected in a manner that provides for the electronic exchange of health information to improve the quality of healthcare" (Vest, 2010, p. 288).

The goal of integrating patient records has not yet been realized, however, with several challenges to information-sharing noted. Key among these challenges was the apparent lack of a sustainable business model. For example, the cost of implementation and administration of the new database approached $12 million US dollars for its development and approximately $3 million in annual operations and maintenance. Participants voiced concerned over the high cost, especially as it was difficult to show concrete returns on their investment costs. While federal, state, and private

grants helped to overcome implementation and ongoing costs, they were not seen as ".. a viable alternative to self-sustaining revenue streams". Another significant barrier to success was a lack of trust between the health service providers. It became evident that organizations did not fully trust one another with their proprietary information. Competitive dynamics was noted between participants as information was withheld in the interests of gaining a competitive advantage. In addition, some organizations cited fear of legal liability from unlawful disclosures as reasons for not sharing information. While privacy laws did allow for the sharing of information for the purpose of patient care, some organizations perceived the weight of the risk of liability as outweighing any potential for reward (Vest, 2010, p. 290).

Social Work and Child Welfare

Information-sharing was also evident in the field of social work and child welfare. Recent high profile failures in the child protection system have highlighted the need for a more comprehensive approach to social and youth work. Consequently, it was suggested that the expertise, resources and information from social, youth, education, police and nursing disciplines be pooled together. In doing so, it was argued that the integration of these resources, would enable social and child welfare professionals to paint a fuller picture of a child's life and thus support enhanced decision-making and actions with respect to young persons at risk (Thompson, 2013, p. 190).

In the UK, for example, the *Children Act* (2004) imposes on all professionals who, during their duties, come into contact with children, the responsibility to protect and promote their wellbeing (Chudleigh, 2005, p. 41). At the core of the *Children Act* is a statutory duty to develop information-sharing databases in order to better understand the lives of children so that they can be effectively protected. The aim, in other words, is to overcome previous problems of fragmentation by establishing a fuller picture of a child's life in order to assess the risk of maltreatment or abuse. In particular, information-sharing practices focused on early intervention strategies to child welfare and safety, with the majority of information-sharing occurring at the "stage of referral" by different medical professionals dealing with children (Thompson, 2013, p. 191).

Some professionals were skeptical of the full picture analogy as applied to child welfare, however. Some argued that the creation of a full picture in the everyday life of a child involves greater complexity and subjectivity than the information-sharing project assumes. In practice, some professional's described a process that requires "back and forth translation and revision" and that such processes are "a complex activity involving a process of sense-making and connection" (Thompson, 2013, p. 192). These persons point out to the moral and social judgments that need to be made with respect to safeguarding children, arguing that the "full picture" approach takes on "…objectivist assumptions about the stability of meaning." Rather, information is not fixed and does not have the same meaning for all childcare professionals involved in the same case, but involves sense-making and translation with the context of organizational and social relevance. Thus, deciding what information is a signifier of concern, or what information should be shared or further assessed, with respect to ensuring child welfare, requires difficult and complex judgments

and interpretations that many felt were not made sufficiently visible in the existing information-sharing approach (Thompson, 2013, p. 191).

The need for greater information-sharing was also noted in the work relating to criminal offenders with mental health problems in the UK. The inter-relations between criminality and health is an enduring challenge for the UK's Criminal Justice system and National Health Services. For example, several high profile inquiries into violence and homicide involving people with mental illness and deaths in police custody have highlighted the risk of not sharing health related information. It has been estimated that between 1998 and 2003 in the UK, of the 153 deaths in police custody, over half had indications of mental health problems. The transition between health and criminal services, in particular, was identified as a time of high-risk. The immediate post-discharge period from mental health inpatient care was also associated with a significant increase in the risk of suicide. The issue of continuity of care and information-sharing between the health and criminal fields is, therefore, an important one. In response, health and risk information about recently released prisoners with severe and enduring mental illness are now being shared between mental health and criminal justice agencies using an internet-based network called the Multi-Agency Information Sharing Network (MAIS) (Lennox, 2012, p 132).

Challenges to effective information-sharing in the MAIS experience quickly became apparent, however. First, it was found that the criminal justice agencies did not always receive the information they felt they needed, whereas the health care agencies reported that they routinely received the information they felt they needed. In particular, criminal justice agencies typically asked for primary health and risk-related information from their health care counterparts. However, the perception was that the criminal justice agencies may have lacked awareness or understanding of how to use this information to contribute to a person's safer detention in custody. From a policing perspective, detention in police custody is for a short period and for the purpose of gathering evidence and rendering decisions about criminal charges. In this context, health-related information is valued so far as it can ensure "medical fitness" for detention and interviews, and not as a nurse or clinician may view the situation as an opportunity to conduct a comprehensive health assessment, improve an individual's health, or provide referrals to further health or social services. Moreover, a clinician or nurse have different professional codes of conduct to abide by, which may not be conducive to a police officer's investigative process. Thus, it quickly became evident that health and criminal justice agencies have competing organizational aims which can lead to clashes of priorities and competing tensions, which challenge information-sharing objectives (Lennox, 2012, p. 132).

Multinational Corporations, business and manufacturing

Information sharing was also increasingly being used in the business sector. The majority of information-sharing initiatives in the business sector were aimed at gaining a competitive advantage in the marketplace, especially with respect to joint-collaboration projects involving research and development, product innovation and manufacturing. In addition, information-sharing was also noted as a way for large Multinational Corporations (MNCs) to coordinate the

activities of their regional offices in order to overcome problems associated with geographic and cultural distances.

In China and India's manufacturing and technology services sectors, the sharing of information was noted as a key strategy for developing emerging market opportunities. For example, several western-based Multi-National Corporations (MNCs) use information-sharing to transfer low-cost product models to India and China. The result is cost-savings for the MNCs due to the relatively inexpensive human resources and talent pool from which to draw in these markets. The information shared includes formal business processes such as project management, quality and inventory management, as well as human resources practices. What began as low-cost production or low-end services, however, is beginning to progress into greater product and service sophistication, thus creating new opportunities for MNCs in the Indian and Chinese markets. As a result, information-sharing between firms are becoming increasingly sophisticated, with more complex knowledge being transferred from the West into Indian and Chinese manufacturing firms. In short, information-sharing is a central part of firms in China and India's strategy to gain competitive advantages in the manufacturing and technology services markets (Teagarden, 2008, p. 194).

As this evolution towards more sophisticated and complex manufacturing and service models develops, however, several challenges to information-sharing between China and India have been identified. First, culture, language and geographic distance differences between the knowledge producers and the knowledge recipients continue to present barriers to information-sharing. These barriers become increasingly problematic as the information transferred becomes increasingly complex. What began as low-cost manufacturing has evolved into more complex operations. This greater complexity has also increased the extent to which participants must interact with one another in order to engage in the transfer, as well as a greater emphasis on tacit and knowledge such as software development (Teagarden, 2008, p. 195). Second, distrust between China and India remains. The different cultures and national identities were less a problem when the information shared was straightforward and well understood. These included business processes and procedures such as scripts, training protocols and back-office support that could be easily explained and followed. The transfer of more complex knowledge into more sophisticated operations than before has exasperated feelings of distrust, particularly with respect to the perception of China as being a "technology thief" and lacking enforcement with respect to intellectual property rights (Teagarden, 2008, p. 195).

MNCs also employ information-sharing strategies to enhance their capacities for innovation, especially with respect to supporting Research and Development activities (R&D). R&D collaborations between firms, even among direct rivals, are increasingly becoming commonplace. Past successful joint R&D collaborations include the development of the 45-nm microchip between NEC, Sony and Toshiba, and the hybrid power trains for Sport-utility vehicles between GM and Daimler Chrysler. Such collaborations are desired for their ability to share resources and risks, minimize redundant expenditures, and increase a firm's knowledge base. Joint-collaborations can also improve a firm's reputation and gain them access to new networks

(Husted, 2010, p. 37). Analyses of past R&D collaborations show that information-sharing mainly takes place at the individual level within an integrated team environment. The majority of the company's research and development activity takes place in R&D teams. However, it is with the individual employee that much of the knowledge actually resides. Thus, the individual employee decides whether to share information, as well as judges the value of the information that is shared with them. In the R&D sector, therefore, the effectiveness of information-sharing is largely dependent on personal information-sharing efforts and behavior (Husted, 2010, p. 38).

The individualistic nature of information-sharing can present challenges for joint-collaborations. Past projects have revealed that individuals employees involved in information-sharing can often find themselves experiencing dual allegiances. That is, employees can find themselves caught between the pressures to remain loyal and committed to their home organization and the collaboration at the same time. The participating organizations ultimately remain as separate entities, however, and thus have competing expectations, objectives and interests. Thus, the individual employee must decide what information to share, while remaining loyal to their home organization but at the same time demonstrating commitment to the collaboration by adding value to it (Husted, 2010, p. 38). Such decisions involve difficult questions of balance, especially considering the inherent uncertainties in R&D work. For instance, the value of R&D work is often ambiguous, with no clear benefit of collaborative efforts realized until the final product is realized. From the organization's perspective, a key challenge is to ensure that their information-sharing employees engage in collaborations in such a way that they protect the company's strategically important knowledge while simultaneously contributing to the R&D effort as a collaborating partner. Such difficult balancing acts are further complicated by the fact that information-sharing often occurs in informal networks and situations, therefore, placing greater importance on personal attributes, relationships and social norms (Husted, 2010, p. 40).

MNCs are also increasingly seeking to leverage their information holdings in order to improve organizational performance and gain competitive advantages in their respective marketplace. It has been argued that in order for MNC's to succeed they must adapt to each local context in which they operate, as well as leverage the knowledge and competencies gained in each context by integrating them. The challenge, in other words, is to combine geographically distant knowledge with local knowledge in order to develop new competencies. Such efforts are increasingly seen as the "source of value creation" and "sustainable competitive advantage" (Mudambi, 2011, p. 186). The task of managing and integrating dispersed experience remains a significant challenge for MNCs, however, especially as many contexts cross national boundaries, industries, and cultures. Moreover, the most valuable competencies often involved highly tacit knowledge, making the capture and integration of this knowledge in disparate contexts equally as challenging (Mudambi, 2011, p. 187).

One approach to meeting these challenges has been the use of so-called "virtual teams," as has been the practice for Finland based Vaisala Instruments (VI), manufacturer and distributor of industrial measurement applications. Vaisala made it a goal to enhance their knowledge sharing across their sales and service network of 24 offices in 12 countries through the creation of virtual

teams supported by social networking technologies (Kaupilla, 2011, p. 401). The company believed that by leveraging social networking technologies, they could combine the individual strengths and experiences from their employees to "boost organization-wide management of fine-grained knowledge" (Kaupilla, 2011, p. 395). The case of a virtual team approach demonstrated some success for VI, particularly with respect to improving communications and shared understanding between the sales and marketing teams. Before the virtual team project, sales persons complained that they were not always receiving the necessary product-specific information they need for customer service. Conversely, the marketing team was not provided with customer information and product feedback from the sales team (Kaupilla, 2011, p. 405).

However, challenges remain with respect to managing and integrating tacit knowledge. It was noted, for example, that the discussions that took place in the virtual knowledge sharing space were overly task-oriented, with few "social" elements such as stories or small talk. The formalized adoption of the network was seen as at odds with the objective to share tacit knowledge and to create interactive knowledge processes (Kaupilla, 2011, p. 410). When participants were asked about this, it became evident that not all employees were comfortable sharing their personal experiences such as customer encounters, especially if they were negative. As a result, the majority of the knowledge shared referred to explicit products and technologies, while little knowledge was shared with respect to markets or customers, which involved more context specific and interpretive information (Kaupilla, 2011, p. 409).

Construction and Project Management

Several benefits are felt to be gained by information-sharing in the construction industry, including improved problem-solving, as well as reducing the repetition of past mistakes made in previous projects. Construction companies are also interested in reducing their costs by avoiding critical errors or mistakes and by improving the efficiency and effectiveness of their problem solving capabilities in order to enhance their engineering methodologies (Lin, 2006, p. 693). Information-sharing was also seen as a way to retain professional skills and experience as it is common practice for engineers and construction experts to take domain knowledge with them when finishing a project or leaving a company.

Information-sharing to this end has proven challenging in this field, however. Construction projects are highly fragmented, with each project bringing a number of stakeholders that collaborate at different stages during the project lifecycle. Construction projects, as such, can be information intensive, with each stakeholder in a project communicating a significant volume of information across the different phases of a project. Each project, moreover, is temporary in nature and each project has different circumstances (Dave, 2009, p. 897). The fragmented and ad-hoc nature of construction projects have challenged companies to find ways to capture and reuse valuable knowledge. In the UK construction management experience, for example, it was found that the management and sharing of tacit knowledge was a key challenge. Information management of explicit knowledge, such as procedure manuals, organization maps, and work breakdown structures were relatively straightforward and capable (Dave, 2009, p. 894). Explicit

knowledge, however, remained a challenge to manage as it became evident that this knowledge remained largely stored in the minds of project team members. Capturing and transferring this knowledge across organisations for use in future projects therefore remained a significant challenge (Dave, 2009, p. 901).

In Taiwan, some construction companies have experimented with internet and social networking technologies to share information. In one case, a construction firm implemented a “construction map based knowledge management system” to organize information that were captured during the construction phase of the project into “network knowledge maps." The new information system proved useful in producing new insights into the factors affecting construction management, and was felt valuable by the engineers to share knowledge and ultimately improve the results of their construction projects. In contrast to the previous information management system, a single centralized database, the new system was felt superior in terms of its ability to retrieve and share tacit knowledge (Lin, 2006, p. 694). In one example, a junior engineer upon encountering a problem with a fire alarm system in which he had no previous experience was able to utilize the knowledge map to find an expert with the relevant knowledge. The problem was encountered previously in seven separate projects, and as such the junior engineer was able to study the “knowledge packages," which included digital videos from the map in order to solve his problem (Lin, 2006, p. 704).

Networked websites are also increasingly used by project managers at the National Aeronautics and Space Administration (NASA). Here, a networked and central database was employed to share the various flight programs and projects in order to allow others to see what has been done in past projects. The documents were linked at each stage of the project development so as to aid the project manager. Best practice documents, lessons learned, video nuggets of experts were some of the documents shared (Liebowitz, 2003, p. 195). NASA’s goal is to improve the “…sharing of documents related to best practice documents, strategic reviews and lessons learned documents, as well as project management and engineering methodologies.” However, practitioners cautioned about the need to improve upon the proposed techniques for knowledge sharing as it was felt that the proposed system was too “passive.” In particular, users asked for greater “intelligence” technology that could actively push the relevant information to users at a time when they needed it most. The development of a more “active” analysis and dissemination method of information-sharing were also presented in terms of enabling greater “organizational learning” within NASA (Liebowitz, 2003, p. 197).

City Administration and Local Governments

Cities and municipalities are also increasingly pursuing information-sharing. For one thing, some local governments have embraced information-sharing as a means to leverage their existing information resources in order to reduce operational costs. Such initiatives are in response to growing fiscal pressures and budget deficits, forcing many local governments to find ways to reduce their level of spending on public programs. These initiatives, moreover, coincide with broader “e-government” initiatives, which also aim to reduce costs but at the same time increase

government transparency and quality of service. Another key reason for the increasing use of information-sharing in cities and municipalities is due to the growing concern over local capacities to respond to increasingly complex and horizontal governance issues. For example, the “urban green” and “quality of life” agendas are two key areas that attempt to tackle environmental and social challenges faced by local governments.

In Chicago, for example, growing ecological and sustainability issues in the urban context have urged city administrators to experiment with collaboration initiatives that emphasize working across traditional boundaries, employing external networks and promoting deeper and wider technological and social change. In particular, Chicago’s Environmental Action Agenda targets a range of environmental issues, including restoring the Chicago River, reducing pollution from storm water runoff, improving energy efficiency and enhancing the City’s recycling and alternative transportation programs. To this end, the city’s administration is emphasizing the need to "direct efforts across departments, as well as encouraging participation from the private and non-profit sectors” (Young, 2010, p. 1052). In other words, there was recognition that the city’s goals required an approach that emphasized the cross-functional nature inherent in the Urban Green agenda. Such functions crossed traditional boundaries of water, land use, the city’s “built environment”, but as well as responsibilities that reached beyond the role of the executive branch or even the public sector in general. In this context, information-sharing was seen as critical in order to build new competencies by leveraging existing information, skills and resources from the different sectors. City managers, as such, looked inward within their organizations to develop “centres of expertise” in sustainability, but as well to acquire knowledge through capturing new information and sharing that information in order to enable “organisational learning” and innovation (Young, 2010, p. 1058).

The success of the City of Chicago’s sustainability agenda is believed to hinge upon the surmounting of two key challenges. First, it was recognized that the city’s new agenda, which required ambitious transformations and significant investments and resources, was an added commitment that stretched existing resources and capacities. Cities were expected to maintain delivery of their traditional social functions and administration. The administration, in other words, struggled with finding ways to fold in the sustainability agenda as a fundamental aspect of advancing their primary missions (Young, 2010, p. 1054). Second, the city’s goal to transform their organizational culture into one that enabled organizational learning and innovation were also seen as a challenge in terms of their capacity and willingness to develop these skills at the individual level. Managers, department heads, program directors and their administrators were all faced with the challenge of connecting the broad environmental visions established by the Mayor’s office with their operational realities (Young, 2010, p. 1055).

Local governments in the UK are also looking to information-sharing as a means to reduce operating costs and find efficiencies as they respond to growing fiscal constraints (Bigdeli, 2013, p. 827). The UK’s Northwest Local Government Association, for example, is under significant pressure to reduce their costs and improve their resource and asset management. IT infrastructure, service delivery and information support were some of the key areas identified for

cost reduction. To this end, information integration and information-sharing were looked at as a way to increase collaborative working as well as remote working in order to address the budget deficit and ultimately reduce program expenditures(Bigdeli, 2013, p. 822). While information-sharing initiatives have not yet been operationalized here, the strategy has been articulated as one where the central government tries to realize operational cost reduction by having local agencies and departments share their services, processes and information (Bigdeli, 2013, p. 826). In the UK's Local Government Association's experience, however, obstacles to effective information-sharing also became evident. The greatest challenge as expressed by the participating agencies is the lack of sustainable funding model for information-sharing projects. Participants voiced concerns over the lack of resources to develop their IT infrastructure as well as IT skills and knowledge among their employees in order to participate. Local agencies also expressed the need to have stronger leadership from the centre in order to encourage participation in times of fiscal constraint. In particular, it was felt that many managers were not recognizing the value of information-sharing or appreciating the importance of sharing quality information beyond their immediate operational context (Bigdeli, 2013, p. 828).

TABLE 1: SUMMARY OF BEST PRACTICES SCAN

Industry / Sector	**Best Practice / Method of Implementation**	**Actors involved / participants**	**Reason For**	**Challenges**
Healthcare	New database integrate information system Multi-disciplinary care centres , collaboration networks Co-location, secondments	Medical specialists, primary/secondary caregivers Clinicians	Treat diseases holistically; Improve continuity of care; Improve decision-making; Fragmentation of information; separate information-systems International pandemics	Accuracy of shared information? Usefulness of information? Context? Financial benefits of sharing? High costs Different professions and purposes Power asymmetries
Social Work Child Welfare	Database integration, information networks New legislation	Social, youth, child workers; educators, police, nurses, clinicians	High-profile failures; support analysis and decision-making; early intervention; Continuity of care	Complexity and subjectivity; interpretation of information, deciding what to share? Professional differences, relevance, codes of conduct
MNC Business Manufacturing	Knowledge transfers Co-location , collaborative teams Virtual teams , social networking	MNCs, firms R&D staff	Competitive advantage, improved Research & Development, innovation, cost and risk sharing, overcome geographic and cultural differences, leverage existing data	Cultural, language, geographic differences; complexity; distrust; individual self-interest, dual allegiances; unclear benefits of sharing; need to protect

				knowledge
Construction, Project Management	New information systems, networked database Social networking, internet websites	Engineers, project managers Tradecrafts experts	Improve construction management practices Lessons learned past projects, avoiding same mistakes Retain experience post-project Competitiveness, problem-solving	Fragmented environment, numerous stakeholders, projects temporary in nature, passive system couldn't push relevant information, complex, explicit knowledge proved harder to share
City Administration Local Governments	Centres of expertise IT Process, service integration	Managers City staff Program administrators	Funding pressures, budget deficits, e-government, increase transparency, improve quality of service, build capacity to respond to complex, horizontal issues, build new competencies	Agenda is ambitious, lack of funding, resources, added project competed with existing duties, functions, lack of culture of innovation, learning, lack of IT skills, lack of leadership, recognition of benefits of sharing

5. COMPARING POST 9/11 INFORMATION-SHARING EFFORTS IN CANADA, THE UK, AND AUSTRALIA

This section will identify and describe key reforms that relate to the integration of counter-terrorism activities and resources for the production of integrated, all-source intelligence in Canada, the UK and Australia. These changes are summarized below in Table 2.

Counter-Terrorism in Canada after 9/11

Background

Between 1960 and 1989, an estimated 62 terrorist incidents occurred in Canada (Charters, 2008, p. 18). High-profile events include a series of anti-Fidel Castro terrorist attacks, an assault on the Turkish embassy by the Armenian Revolutionary Army, and confrontations with the Front de libération du Québec (FLQ) (O'Connor, 2006, p. 19, 30). On June 23, 1985, Canada suffered its most deadly act of terrorism when a bomb detonated on board Air India Flight 182, killing all 329 people onboard. The attacks were carried out by the Babbar Khalsa, a small network of Sikh extremists and were done in retaliation for previous attacks on Sikh militants in India. These events demonstrate how Canada's history of counter-terrorism is one where terrorist attacks were inspired and motivated primarily by foreign conflicts. Given the external nature of terrorist events in Canada, counter-terrorism efforts were mainly focused on identifying and dismantling support and recruitment activities (Charters, 2008, p. 21).

Canadian counter-terrorism efforts escalated quickly in 1999, however, following the arrest of Islamist-extremist and would be terrorist Ahmed Ressam. Ressam was intercepted at the Windsor-Detroit border during a routine border inspection where he was singled out for his nervous demeanour. Initially suspected of drug trafficking, the discovery of explosives in Ressam's vehicle had led the border guard to foil a terrorist plot to bomb the Los Angeles airport during the Millennium celebrations. The casual nature of Ressam's interdiction raised alarms in the US. In particular were concerns that Canada had become a safe-haven for terrorists and thus a liability with respect to US domestic security vis-à-vis the US-Canada border. U.S. officials, in particular, were uneasy over the fact that Ressam had gained entry into Canada as a fraudulent refugee claimant. Ressam, moreover, had subsequently evaded Canadian authorities with the use of a false identity (Mergle, 2007, p. 7). U.S. fears over their national security again came to the forefront when it was suggested that the 9/11 airline hijackers had gained entry into the U.S. through Canada. The stories turned out to be false, but concerns about another Ressam incident remained. After the 9/11 terrorist attacks, the issue of the security of the Canada-US border had moved to the forefront of US-Canada relations (Charters, 2008, p. 21).

Changes to Canada's Counter-Terrorism Framework After 9/11

In 2004, Canada introduced its first policy paper on national security entitled, "Securing an Open Society: Canada's National Security Policy". This policy established the overall structures for

Canada's post-9/11 counter-terrorism community and aims to provide a more holistic and government-wide response to counter-terrorism, border security, and cyber-security. The policy's framework is composed of three pillars, which are: (i) protecting Canada and Canadians at home and abroad, (ii) ensuring that Canada is not a base for threats to its allies, and (iii) contributing to international security (Securing an Open Society, 2004, p. vii). The first two pillars reflect Canada's commitment to enhancing border security in order to assuage US fears of a terrorist incursion via the Canada-US border. This includes programs that have a closer partnership with the U.S. on issues such as border inspections, information-sharing, traffic management, and border security (Charters, 2008, p. 37).

The policy also specifically emphasizes the importance of information-sharing, as illustrated in the following quote:

> The integrated approach that the Government is taking will help to reduce the risk that information held by one part of Government will fail to be provided in a timely fashion to those who can utilize it… [and] recognize that the current scope of threat assessment requirements exceeds the capacity of any one organization" (Securing an Open Society, 2004, Ch. 2, p. 18).

The new national security policy also explicitly refers to the need for information-sharing in order to ensure that "… information does not fall between the different parts of our security system" (Securing an Open Society, 2004, Ch. 2, p. 9, 18).

Integration and Information-Sharing Initiatives after 9/11

The Canadian government identified the sharing of information and interoperability of security information systems as top priorities immediately after 9/11 (Office of the Auditor General, 2004, Ch. 3, p. 19). Significant investments were made to this end, including organizational restructuring that saw the significant integration of a wide-range of agencies and departments (O'Connor, A New Review Mechanism, 2006, p. 116). The most notable forms of integration are the multi-agency integrated teams operating at the operational or investigative level, such as the Integrated Border Enforcement Teams (IBET) and the Integrated National Security Enforcement Team (INSET). The RCMP has stated that integrated teams represent "… a strategic response to the complications arising out of jurisdictional issues, the compartmentalization of information, disparate expertise, and the financial burden to be shared in complex investigations" (O'Connor, Reports of the Events, Factual Background, Vol. 1, p. 211). Information exchange between agencies at this level is frequent and includes agencies such as the CSIS, the CSE, CIC, the CBSA, DFAIT, FINTRACT, the Canada Revenue Agency, Transport Canada, the CATSA, DND and the Canadian Coast Guard (O'Connor, A New Review Mechanism, 2006, p. 113).

Integrated National Security Enforcement Teams (INSETs)

INSETs are the national policing units responsible for national security investigations in Canada and as such carry out criminal investigations in matters of national security (O'Connor, 2006, Vol 1,

p. 102). The majority of these investigations are done at the local or divisional levels, with oversight and operational coordination provided by the National Security Investigation Sections (NSISs), located in RCMP Headquarters, Ottawa. RCMP policy and guidelines do not differ for INSET operations. Information obtained by officers seconded to the INSET from other agencies, however, may not be passed on to those other agencies except through established national security channels (O'Connor, A New Review Mechanism, 2006, p. 103).

Integrated Border Enforcement Teams (IBETs)

IBETs are responsible for enhancing the security and integrity of the US-Canada border, as well as responsible for investigating activities such as terrorism, and human and drug trafficking. IBETs are similar in structure to INSETs in that they are composed of various representatives seconded from other policing and intelligence agencies, such as the RCMP and the CBSA. Unlike INSET, however, IBETS tend to include greater U.S. participation from agencies such as the U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, the U.S. Coast Guard, and local US police. IBET members can share information with INSET members if the information or intelligence relates to a national security offence. IBETs may also support INSET in national security investigations. With respect to sharing information to international partners, INSET team members can only act as liaison resources (O'Connor, A New Review Mechanism, 2006, p. 106).

Integrated Immigration Enforcement Teams (IIETs)

The purpose of IIETs were to review and prioritize outstanding immigration warrant cases, the majority of which consists of removal orders. IIETs were comprised of RCMP and CBSA personnel, with the CBSA having the leadership role in immigration warrant apprehensions. IIETs also see cooperate closely with Citizenship and Immigration Canada and the RCMP, as well as with US agencies in removal orders, particularly with high-risk individuals. IIETs were disbanded in 2005, their resources redeployed to INSET (O'Connor, A New Review Mechanism, 2006, p. 124).

Integrated Threat Assessment Centre (ITACs)

The Integrated Threat Assessment Centre (ITAC) was established in 2004 and serves as Canada's national centre for all-source intelligence analysis and threat assessments. As Canada's central intelligence production agency, ITAC also plays a key part in the dissemination and communication of intelligence analysis to all levels of government, including intelligence and law enforcement agencies and first responders (Major, Research Studies, Vol. 1, 2010, p. 133). ITAC works in conjunction with the National Security Advisor (NSA) to the Prime Minister and is housed within CSIS. The head of ITAC reports to both the Director of CSIS and the Prime Minister's NSA. The NSA is, in turn, accountable to the Minister of Public Safety. ITAC analysis is also linked to the Government Operations Centre, an interdepartmental and strategic-level operations centre that coordinates national responses to Canadian and global events (OAG, 2009, p. 12). ITAC also integrates representatives from a broad range of departments and agencies including Public Safety and Emergency Preparedness, CSIS, the RCMP, the Communications Security Establishment

(CSE), the Department of National Defence (DND), the Department of Foreign Affairs (DFA), the Privy Council Office (PCO), Transport Canada, and the CBSA. ITAC can also draw on expertise from other departments and agencies as required, including Health Canada, Agriculture and Agri-Food Canada and Environment Canada (Securing an Open Society, 2004, Ch. 2, p. 18).

International Assessment Staff (IAS)

The International Assessment Staff (IAS), formerly known as the Intelligence Assessment Secretariat, provides high-level all-source strategic intelligence assessments for Cabinet and inter-departmental policy-makers. The IAS sits centrally within the Privcy Council Office (Major, 2010, vol 1 research papers p. 133).

Marine Security Operations Centre (MSOC)

MSCOC is responsible for detecting, assessing, and responding to maritime security threats. MSOC integrates representatives from the CBSA, Transport Canada, the RCMP, the DND, and the Canadian Coast Guard. Much like ITAC, MSOCs seek to provide an integrated and centralized approach to intelligence analysis that has a marine security element to them (O'Connor, A New Review Mechanism, 2006, p. 119).

Secure Criminal Information System (SCIS)

The RCMP's SCIS database is a separate classified database used to store exclusively all information and intelligence related to national security and represents the heart of the RCMP's national security information management system. The RCMP Operational Manual states that any and all information concerning real and potential national security threats must be entered promptly into the SCIS database. Such information would normally be uploaded to SCIS by a CID, INSET, or NSIS officer. A significant portion of SCIS information is acquired from outside the RCMP, both from domestic and foreign sources. Access to SCIS is restricted to RCMP personnel involved in national security matters only and on a strict "need-to-know basis" (O'Connor, A New Review Mechanism, 2006, p. 109).

The Inter-Operability Working Group

The Inter-Operability Working Group was responsible for developing a long-term strategy for achieving technical inter-operability of Canada's various separate computer databases and networks. The group disbanded soon after its creation, with the task now taken up by Public Safety Canada (Office of the Auditor General, 2009, p. 23).

Public Safety and Emergency Preparedness Canada

Closely modeled after the U.S. Department of Homeland Security, PSEPC was created in 2003 and integrates the following departments: the RCMP, CSIS, the former Department of the Solicitor General, the Office of Critical Infrastructure Protection and Emergency Preparedness, the National Crime Prevention Centre, and the new Canada Border Services Agency. As a result of this

amalgamation, the Minister of Public Safety now has jurisdiction over all public safety and emergency preparedness matters and exercises national leadership on public safety and emergency preparedness matters. To this end, he or she may coordinate policies, cooperate with any province, foreign state, international organization or other entity, in order to facilitate the sharing of information to promote public safety objectives, and render decisions on national security matters (Roy, 2005, p. 467).

Together, the CSIS, CBSA and the RCMP are mandated to uncover information in order to pre-empt any possible domestic terrorist attacks. While the RCMP and CSIS both have responsibilities for national security and counter-terrorism under the *Anti-terrorism Law* (2001), it is the RCMP that has formal responsibility for national security enforcement. The *Security Offences Act,* in particular, assigns the RCMP, as opposed to provincial and municipal police, primary responsibility for the investigation and prosecution of crimes that represent a threat to national security (Major, 2010, p. 412). The RCMP has formal arrangements with the provincial and municipal police, and specifies protocols and procedures when dealing with national security investigations. National security investigations typically have local implications and as such there is often a continuing role for municipal or provincial police even in cases where the RCMP becomes involved (O'Connor, Analysis and Recommendations, 2006, p. 317). These information-sharing arrangements, however, are not formalized in writing (O'Connor, 2006, Factual Background Volume 1, p. 38).

Cabinet Committee on Security and the National Security Advisor

The Cabinet Committee on Security, Public Health and Emergencies is also responsible for coordinating the government's overall handling of national security and intelligence, as well as coordinating the government's response to emergency disasters. The Committee is composed of various Ministers responsible for national security or counter-terrorism and operates by consensus. The committee is further divided into various sub-committees, one of which includes a committee of Assistant Deputy Ministers also responsible for managing national security and intelligence. There is also a sub-committee on national security that is composed of Director Generals. The Prime Minister is advised by the NSA while the Minister of Public Safety is advised by the Deputy Minister of Public Safety (Office of the Auditor General, 2009, p. 13). The NSA to the Prime Minister is responsible for improving the coordination and integration of security efforts among government departments (Securing an Open Society, 2004, Ch. 2, p. 9).

Ministerial Directives

Some policy guidance and standards for the exchange of national security information and intelligence are provided by way of Ministerial Directives (see Appendix I). Such directives are issued by the Minister of Public Safety to the Commissioner of the RCMP, who, in turn, incorporates them into internal RCMP Policies. In addition, RCMP investigations on National Security matters are also subject to the general policies and standards of RCMP Criminal Investigations (see Appendix II). However, regular criminal investigations do not operate in the same legal nexus as National Security matters, making these general policies inapplicable under

certain situations. Various federal statutes, for example, invoke national security concerns to authorize special government action to pre-empt, or respond to, national security threats, including the *Privacy Act* and *Access to Information Act* (Forcese, 2008, p. 6).

Counter-Terrorism in the UK after 9/11

Background

In comparison to Canada and Australia, the UK has the longest history of combating terrorism. Approximately three decades were spent fighting the Provisional Irish Republican Army (PIRA), a terrorist group that sought to unite Ireland since 1968. Throughout the 1970's to 1990's, it is estimated that the UK experienced approximately 250 terrorist incidents. However, it is worth noting that these incidents were not directed at the UK per se, but rather were motivated by foreign conflicts. Following the UK's participation in the 2001 US- Afghanistan and the 2003 US-Iraq war, however, a direct threat from terrorism to the UK from terrorism appears to have increased. In 2002, MI5 foiled a plot by al-Qaeda to attack the London Underground transit system with toxic gas. Shortly after this, another terrorist plot to destroy a passenger aircraft using shoulder-fire surface-to-air missiles at Heathrow Airport was again foiled. In 2005, Islamist terrorists successfully carried out a bombing attack on the London Underground public transportation system. A few short weeks later, another Islamist terrorist was thwarted in a bombing attempt on American Airlines Flight 63 (Bamford, 2010, p. 738).

Changes to the UK's Counter-Terrorism Framework after 9/11

UK officials argued that if terrorists were willing to sacrifice themselves in an attempt to inflict mass casualties, then they too would have no hesitation to use chemical, biological or nuclear weapons (Bamford, 2004, p. 737). As a result, the UK government sought to establish a more preventive counter-terrorism approach, with the creation of a new counter-terrorism framework in 2004. The new framework served to focus intelligence gathering activities on terrorist planning activities. These activities include terrorist fundraising, personnel recruitment, communications and terrorist tactics (Gregory, 2005, p. 2).

On July 7, 2005 a group of terrorists linked to al-Qaeda successfully coordinated a bombing attack in London on the public transport system during the morning rush-hour. It was later determined that part of the failures to prevent the attacks were the result of an undue focus on specific high-value targets. This narrow approach allowed lesser crimes and smaller-scale terrorist activities to operate without detection or intervention (Field, 2009, p. 1002). As a result, intelligence collection efforts increased, especially with respect to domestic intelligence and home-grown Islamist terrorism. The objective was to disrupt a wider range of terrorist activity by intervening earlier in the terrorist radicalization and recruitment stages.

Integration and Information-Sharing Initiatives after 9/11

Similar to Canada and Australia, the UK introduced numerous multi-agency integration units after 9/11. The SO15, CTU's, JTAC, and JIC, for example, all represent newly formed multi-agency integrated teams. SO15 and CTU's, in particular, were implemented following 7/7. JTAC is the UK's principal mechanism for the pooling and centralizing all terrorism-related intelligence, which is composed of representatives seconded from a eleven different departments. In addition, parts

of the Metropolitan Police, the Anti-terrorist Branch and the Special Branch were merged to form the Counter Terrorism Command, representing a national structure for counter-terrorism policing. The CTC, also known as Special Operations 15 (SO15), was tasked with bringing together available intelligence, investigative and operational resources within a single, centralized agency (Field, 2009, p. 1001). Four Counter-Terrorism Units (CTU) were also setup throughout England to provide additional coordination and specialist support to local police. These units merged Special Branch Officers from the larger police forces. CTU's are also supported by dedicated Community Intelligence Officers. Personnel from the new CTU are also co-located with staff from the regional branches of MI5 in so-called 'fusion centers'. Members of GCHQ staff have also been seconded to other agencies such as CTUs in order to provide specialist support for investigations. After 7/7, the front-line police officers were also encouraged to collect domestic terrorist intelligence under project 'Rich Picture' (Field, 2009, p. 1002).

The Joint Terrorism Analysis Center (JTAC)

JTAC was created in 2003 and is responsible for analyzing all available and relevant national security intelligence. The core purpose of JTAC is to serve as the UK's central hub for the pooling, analysis, and dissemination of all terrorism-related intelligence by serving as an "access conduit" to the various and independent intelligence databases within the UK intelligence community. Information-sharing, as such, is done by means of creating access to departmental databases for each representative working out of JTAC (Burger, 2008, p. 70). Representatives from a total of 11 departments are seconded to JTAC, including seconded members from MI5, MI6, GCHQ, DIS, the FCO, the Home Office, the police, the Office of Nuclear Safety, and the Department of Transport Security Division. Being at the centre of the UK's intelligence community, JTAC also serves as the main driver for intelligence collection activities. JTAC coordinates the various intelligence agencies in both their investigative priorities and activities as well as directs those agencies in what information to share (Major, 2010, p. 135). Finally, JTAC serves an advisory role to the UK government through the production of high-level strategic reports on terrorism, as well as establishes the domestic terrorism threat level (Jackson, 2009, p. 128). Central direction and leadership for JTAC is provided by the director-general of MI-5. According to the most recent Director-General, "JTAC is a concrete example of how different parts of government are working together to respond to the changed circumstances we now face" (Gregory, 2005, p. 3).

Special Operations 15 (SO15)

SO15 was created to unify police intelligence, investigative and operational resources into a single national structure following the 7/7 attacks. SO15 amalgamates the former sub-units of the Metropolitan Police and the Special Branch, as well as the Anti-terrorist branch. SO15 is responsible for collecting intelligence on terrorist threats on a day-to-day basis while supporting the investigation of terrorist offences in other parts of the UK (Field, 2009, p. 1002).

Regional Counter-Terrorism Hubs (CTU's)

CTUs amalgamate officers from the Special Branch of the Metropolitan Police and provide coordination and special operational support to local police through their local intelligence gathering and investigative work. Four CTUs currently operate in England in order to provide an enhanced local intelligence picture. The remaining resources of the Special Branch were re-allocated to other intelligence gathering priorities. CTU officers are also co-located with staff from one of the new six regional MI5 stations. Three of these are located in England, with the remaining located in Northern Ireland, Scotland and Wales. A Northern Operational Centre was also installed to provide additional support for surveillance operations outside of London (Field, 2009, p.1002).

The Police International Counter Terrorist Unit (PICTU)

PICTU is comprised of representatives from the Special Branch, Anti-Terrorist Branch and the Security Service officers and is co-located with JTAC within MI-5 (Rosenthal, 2007, p. 58). PICTU was created to facilitate the timely dissemination of operational intelligence by enhancing coordination between the police and MI6. PICTU seeks to improve coordination by acting as an advisory and interpretive conduit between the two agencies on matters relating to terrorism. PICTU is also tasked with ensuring that intelligence is communicated to those who need to know in a timely fashion (Bamford, 2004, p. 745).

The Joint Intelligence Committee (JIC)

The JIC remains the UK's main intelligence assessment body and supports the strategic national security objectives of the UK by directing the national intelligence organizations of the UK and by providing advice to the Cabinet related to security, defence and foreign affairs. The JIC is a key coordination mechanism for the UK's intelligence community by overseeing the setting of priorities for the Secret Intelligence Service (SIS), the Security Service (MI6) and the GCHQ, as well as the Defence Intelligence. The JIC instruct all UK foreign, signals and military intelligence agencies on intelligence collection priorities. Agencies are then expected to report routine information back to the JIC, where it is centrally processed and disseminated. The JIC also acts as the central hub, in partnership with JTAC, to integrate national threat assessments. The production of national assessments by the JIC is thus a joint-production process that draws input from across the intelligence community. The Permanent Secretary of the JIC is responsible for ensuring that the UK intelligence community has clear strategies and systems for prioritizing intelligence collection and analysis. The JIC also establishes the professional standards for intelligence analysis. Membership to the Committee is comprised of the heads of the SIS, MI6, GCHQ, the Chief of Defence Intelligence, Deputy Chief of Defence Intelligence Staffy, the Chief of the Assessment Staff, and representatives from the Ministry of Defence, Foreign and Commonwealth Office, as well as the Prime Minister's adviser of foreign affairs (Burger, 2008, p. 78).

The Government Communications Headquarters (GCHQ)

The Government Communications Headquarters (GCHQ) provides signals intelligence (SIGINT) and information assurance to the UK government and its armed forces in the same areas of interest as MI-6. Its activities are also governed by the same statute as those governing MI-5 and MI-6. The Defence Intelligence Staff collect and analyze intelligence in support of military command and deployed armed forces of the Ministry of Defence. GCHQ operates under the guidance of the JIC. The Communications Electronics Security Group is the branch of GCHQ responsible for safeguarding the communications and information systems of the government and critical parts of the UK national infrastructure (O'Connor, A New Review Mechanism, 2006, p. 367).

SCOPE

The SCOPE initiative aims to create a secure networked information system to bring disparate sources of counter-terrorism and intelligence expertise together. The system hopes to enable the intelligence analyst to "pull" intelligence from a central repository as well to obtain intelligence reports 'pushed' at them. The SCOPE project is intended to increase the free flow of information significantly, and, in its first version, it is hoped to connect ten separate government departments and agencies (Burger, 2008, p. 76).

Counter-Terrorism in Australia after 9/11

Background

It was not until after 9/11 that the threat of radical Islamism was given serious consideration in Australia (Ungerer, 2006 p. 196). Additional attention and resources for counter-terrorism were again increased following the 2002 Sari nightclub and Kuta beach bombings in Bali, Indonesia, (Shuja, 2006, p. 52). These attacks were not directed at Australia per se but rather at the West more generally. The attacks, nonetheless, raised concerns that terrorist groups in the South East Asia region would conflate local grievances with the global radical Islamist ideology (Michaelsen, 2010, p. 255). Terrorist groups such as the Moro Islamic Liberation Front (MILF) in Mindanao, Philippines and the Al Ma'unah and Abu Sayyaf terrorist groups in Indonesia are of particular concern. These terrorist groups are believed to have the potential to align with al-Qaeda or become inspired by a similar worldview (Ungerer, 2006, p. 197).

Before 9/11, Australia seems to have dedicated the least amount of resources to counter-terrorism, when compared to the UK or Canada. The Office of National Assessment (ONA), the agency responsible for national security assessments, for example, did not employ a full-time analyst for counter-terrorism. The office was instead focused on threats from right-wing extremism, neo-Nazi organizations, and human trafficking from South East Asia (Ungerer, 2006, p. 196). By 2008, however, ASIO's reported that radical Islamist terrorism "… posed the most significant security threat to Australia for at least the last seven years" and that 'it will continue to do so for the foreseeable future'. ASIO also stated '...if not for the action of ASIO and its partners in recent years… there would have been a terrorist attack or attacks in Australia' (Michaelsen, 2010, p. 261). The 2010 Counter-Terrorism White Paper reiterated the threat from radical Islamism, stating that "… the main source of international terrorism and the primary terrorist threat to Australia and Australian interests today come from people who follow a distorted and militant interpretation of Islam …" (Michaelsen, 2010, p. 250). Australia also appears to be a surrogate target for anti-Western sentiments in the region (Wright-Neville, 2005, p. 5). Australia, as well, is increasingly concerned with "home-grown" terrorism following the 2005 terrorist attacks in London (Government of Australia, 2010, p. 2).

Changes to Australia's Counter-Terrorism Framework After 9/11

Immediately following the 9/11 attacks, the Howard government stated that it would focus on preventing terrorist crimes through an 'intelligence-led arsenal' (Australia's National Counter-Terrorist Plan (2003). The Australian government's new counter-terrorism approach focuses on the threat of Islamist extremists terrorism. In particular, Australia is concerned with the threat of terrorism in the Asia and South Pacific regions (Report of the Inquiry Into Australian Intelligence Agencies, 2004, p. 12). The Australian government also underwent an extensive review of its security and intelligence programs (Baldino, 2007, p. 1). Approximately $3 billion (AUS) was spent between 2002 to 2008 on new institutional structures and activities on counter-terrorism (Report of the Inquiry Into Australian Intelligence Agencies, 2004, p. 78).

The extent of reforms focused largely on enhancing the counter-terrorism capabilities of Australia's domestic intelligence agency. This includes the Australian Secret Intelligence Organisation (ASIO), and the Australian Federal Police (AFP) (Wright-Neville, 2005, p. 6). In addition, Australia also has incorporated new border security arrangements aimed at improving the detection of criminals and terrorists at its borders (Australia's Counter-Terrorism White Paper, 2010, p.3, 20). Bilateral cooperation on counter-terrorism and law enforcement has also increased significantly since 9/11, most notably with Indonesia and the Philippines but also with other South East Asian states. The new bi-lateral relationships reflect a shift in Australian foreign policy, which was historically isolationist in orientation (Wright-Neville, 2005, p. 4). In particular, provisions for more extensive and frequent exchange of intelligence on a bi-lateral basis have been formalized in fourteen Memoranda of Understandings between various South East Asian states (Michaelsen, 2010, p. 249). As part of these agreements, Australia has also agreed to provide significant training assistance to policing agencies in the South East Asia region in order to improve their domestic counterterrorism capabilities. Such assistance also serves to build long-term relationships with ASIO and ASIS's counterparts in the region (Ungerer, 2006, p. 198).

Integration and Information-Sharing Initiatives after 9/11

Australia's post-9/11 counter-terrorism strategy of coordinated prevention has been operationalized through various integration initiatives and increasing multi-agency coordination and collaboration. The Australian Crime Commission, for example, amalgamates resources from the different departments having a national security and intelligence role. Threat and risk analysis assessments have also been integrated with the creation of the National Threat Assessment Centre (NTAC). The new Counter-Terrorism Control Centre (CTCC) is hosted by the Australian Security and Intelligence Organisation and integrates the Australian Federal Police, the Australian Secret Intelligence Service and the Defence Signals Directorate. The National Intelligence Coordination Committee was also instituted to coordinate the different ministers on intelligence matters across government.

Australian Crime Commission (ACC)

The Australian Crime Commission (ACC) was established in 2003 and is responsible for the collection, analysis, and dissemination of criminal intelligence in Australia. The ACC has been granted additional powers to share information with other agencies and for enhanced criminal investigations and intelligence operations (O'Connor, 2008, p. 317). The ACC provides key strategic criminal intelligence assessments to the government as well advise the government on national criminal intelligence priorities. The ACC is also responsible for managing the Australian Criminal Intelligence Database (ACID) and the Australian Law Enforcement Intelligence Network (ALEIN). The ACC merges the activities of the Australian Federal Police (AFP), local state and territory police, the Australian Customs Service, the Australian Tax Office, and the Australian Security Intelligence Organization (ASIO) (O'Connor, A New Review Mechanism, 2006, p. 319).

The Counter-Terrorism Control Centre (CTCC)

The Counter-Terrorism Control Centre (CTCC) is a multi-agency unit located within AISO and is responsible for ensuring the integration of Australia's overall counter-terrorism intelligence capabilities. The CTCC integrates the activities of the Australian Federal Police, the Australian Secret Intelligence Service (ASIS) and the Defence Signal Directorate. The creation of CTCC was a key recommendation of the Australian government's Counter-Terrorism White Paper, which states that CTCC will:

> … strengthen[] the integration of our counter-terrorism capabilities, [and] improve the ability of agencies to operate against terrorism and to detect and prevent terrorist threats to Australians and Australia's interests (Government of Australia, 2010, p. 27).

The CTCC also sets and manages counter-terrorism priorities, identifies intelligence requirements, and ensures that the processes of collecting and distributing counterterrorism information are fully integrated and consistent with national requirements. The CTCC also supports federal and state law enforcement authorities and advises the Commonwealth on threats to its national security (Counter-Terrorism White Paper, Commonwealth of Australia, 2010, p. 28).

The National Threat Assessment Centre (NTAC)

NTAC was created in 2004 and is responsible for collecting, monitoring, integrating and analyzing all threat intelligence available to the Australian government. NTAC integrates activities of the AFP, ASIS, DIO, DSD, Department of Foreign Affairs and Trade, Department of Transport and Regional Services, and the Office of National Assessments. Information-sharing, as such, occurs via officer-to-officer through their access to their own agency's own databases (Counter-Terrorism White Paper, Commonwealth of Australia, 2010, p. 30).

NTAC is located within ASIO and brings together staff from a range of agencies. The centre has approximately 40 analysts preparing threat assessments and works in close coordination with various intelligence collectors. The threat assessments produced by NTAC are used to inform a wide range of government decision-making about security, as well to determine the national counter-terrorism alert level. The Department of Foreign Affairs and Trade also prepares travel advisories based on NTAC threat assessments (Flood, 2004, p. 77).

The Australian Security Intelligence Oragnisation (ASIO)

After 9/11 ASIO has shifted its priority to counter-terrorism. In 1998, for example, approximately 40% of its resources were devoted to counter-terrorism. Today approximately 70% of ASIO's resources are dedicated to counter-terrorism (Flood, 2004, p. 77). ASIO is located in the AIC and is responsible for preparing and distributing threat assessments and warnings regarding terrorism via the Australian Secure Network (ASNET). After 9/11, ASIO has been granted increased legislative powers in order to monitor, detain and question terrorist suspects. These enhanced powers have also raised ASIO's profile, in terms of its internal security role within Australia's intelligence community. ASIO also has increased inter-agency cooperation with the AFP (Flood, 2004, p. 54).

Today, ASIO is responsible for gathering intelligence and producing integrated assessments to advise the Australian government on threats to its security, as well as informing risk management decisions made by operational agencies. ASIO also informs the implementation of protective security measures and the travel advisories regarding potential threats when travelling overseas that are prepared by the Department of Foreign Affairs and Trade (DFAT). In addition, AISO provides protective security advice to Australian Government agencies and, with the approval of the Attorney-General, to state and territory governments and private sector companies to protect vulnerable facilities (Counter-Terrorism White Paper, Commonwealth of Australia, 2010, p. 30).

The National Intelligence Coordination Committee (NICC)

In 2009, NICCs were established to enhance the coordination of Australia's intelligence and national security community. To this end, the NICC integrates Australia's domestic and international intelligence activities into a new national security framework. This integration is for the purposes of enhancing the capacity of Australia's security agencies to share information, coordinate effort and identify opportunities to improve the whole-of-government response to terrorism and other national security challenges (Counter-Terrorism White Paper, Commonwealth of Australia, 2010, p. 28). NICC is a multi-agency unit comprised of various high-level representatives from across the Australian government. Representatives include the Office of National Assessments, the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation, the Defence Signals Directorate, the AFP, the Australian Crime Commission, and Customs and Border Protection, to name a few (O'Connor, 2008, p. 317).

National Security Chief Information Officer (NSCIO)

The NSCIO is responsible for the strategic coordination of the national security community's information management system. The NSCIO is tasked with the development of a roadmap that will detail key measures needed to achieve a more secure, coordinated and effective national security information management environment by 2020 (Counter-Terrorism White Paper, Commonwealth of Australia, 2010, p. 31).

Joint Counter-Terrorism Team (JCTT)

The JTCC integrates the activities of the AFP, state and territory police services and is responsible for conducting counter-terrorism investigations. JCTT members work collaboratively to ensure that counter-terrorism investigations and operations are informed by integrated information from all available sources. JTCC's investigations are focused on preventive and "strategic" operations (Counter-Terrorism White Paper, Commonwealth of Australia, 2010, p. 59). The Joint Counter-terrorism intelligence Coordination Unit was established in 2002 and is aimed at ensuring that all relevant national capabilities, particularly intelligence collectors, are supporting significant counter-terrorism investigations and operations (Flood, 2004, p. 77).

The National Counter-Terrorism Committee (NCTC)

The National Counter-Terrorism Committee (NCTC) was created 2 weeks following the 2002 Bali nightclub attacks. NCTC comprises senior representatives from government departments, line agencies and police services at the Commonwealth, State and Territory levels (O'Neil, 2007, 476). The NCTC's role is to strengthen 'inter-jurisdictional coordination' by promoting 'an effective nationwide counter-terrorism capability' and ensuring the sharing of 'relevant intelligence and information between agencies and jurisdictions' (Department of Prime Minister and Cabinet 2004, 10). It also has responsibility for instituting revisions to the National Counter-Terrorism Plan (NCTP) (Council of Australian Governments Review of Counter-Terrorism Legislation, 2013, p. 45). In addition, the NCTC oversees the National Counter-Terrorism Handbook, which 'sets out in detail the relevant procedures and spacing protocols supporting the NCTP' (Flood, 2004, p. 10).

The National Security Division (NSD)

The National Security Division (NSD) was created in 2003 in the interest of coordinating Australian government agencies as well as the Australian states and territories' counter-terrorism response. The NSD is located in the Department of the Prime Minister and Cabinet. NSD's mandate is to provide advice, briefings and support to the Prime Minister on national security issues including defence policy and operations, intelligence, non-proliferation, counter-terrorism, border protection and certain criminal law enforcement issues (Flood inquiry, 2004, p. 77).

Counter-Terrorism Committees

Counter-Terrorism Committees were also formed in the wake of 9/11 in order to ensure government-wide coordination of Australia's intelligence community and counter-terrorism resources. For example, the purpose of the Counter-Terrorism Information Oversight Committee (CTIOC) is to identify gaps in intelligence collection and develop requirements to ensure continuity. The Terrorist Threat Coordination Group (TTCG) also serves as a central avenue for the high-level discussion of the current threat intelligence, as well as other threat intelligence coordination issues. Last, the Travel Advisory Threat Assessment Meeting meet to discuss issues relating to travel advisories, as well as ASIO-DFAIT coordination issues. (Flood, 2004, p. 77).

Australian Law Enforcement Intelligence Network (ALEIN) and Australian Criminal Intelligence Database (ACID)

ACID and ALEIN provide federal, state and territory law enforcement and other regulatory authorities with a mechanism in which to store, retrieve, analyse and share criminal information and intelligence on a government-wide basis and in a secure manner. The ACC is also responsible for managing the Australian Criminal Intelligence Database (ACID) and the Australian Law Enforcement Intelligence Network (ALEIN) (ACC Annual report 2004-2005, p. 33)

TABLE 2: SUMMARY OF COMPARISONS – CANADA, the UK and AUSTRALIA

Post-9/11 Information-Sharing Initiatives	Canada	The UK	Australia
Integrated Teams (operations & investigations)	IBET, INSET, IIET	CTU, SO15, PICTU	JCTT, ACC
Integrated Threat Assessments (Strategic Analysis & Advisory)	ITAC, IAS, MSOC	JTAC	NTAC, ONA, ACC
Integrated Databases (Electronic systems)	Public Safety Inter-operability: a way forward (2008)	SCOPE, SCOPE 2	ACID, ALEIN
Policy/Framework	"Securing an Open Society" protecting Canada and Canadians at home and abroad, ensuring that Canada is not a base for threats to its allies contributing to international security	Counter-Terrorism Strategy (CONTEST) Prevention Pursuit Protection Preparedness (2004, 2009, 2011)	"Securing Australia – Protecting our Community" Analysis Protection Response Resilience
Pan-Government Coordination Mechanisms	National Security Advisor,Cabinet Committee on Intelligence & Security	JIC	NICC, CTCC, NSD, CTIOC, TTGC
National Counter-Terrorism Structure	Public Safety Canada (RCMP, CBSA, CSIS, Correctional Service Canada)	SO15(Metropolitan Police Services, Anti-Terrorism & Special Branch)	Counter-Terrorism Command

6. INFORMATION-SHARING SYSTEM AFTER 9/11: A COMPARATIVE ANALYSIS BETWEEN CANADA, THE UK AND AUSTRALIA

This section will compare Canada's post-9/11 information-sharing initiatives to those of the UK and Australia. We found that Canada, the UK, and Australia have all responded to the demands for post-9/11 information-sharing in a similar fashion. At the operational and investigative level, all three countries introduced new inter-agency security units, commonly referred to as Integrated Teams. At the strategic and government advisory level, Canada, the UK and Australia have all created similar inter-agency centers for intelligence assessments, also known as Integrated Threat Assessment Centres. At the informational level, the integration of separate computer databases or information repositories was also similarly pursued through various technical "inter-operability" initiatives.

Information-Sharing by Means of Integration: Similarities

The introduction of Integrated Teams after 9/11 was noted in Canada, the UK and Australia. Integrated teams aim to bring together or "co-locate" the representatives of various agencies for the purpose of integrated and joint collaborations at the operational and investigative levels. In organizational terms, Integrated Teams can be defined as the "… coalescence of discrete individuals into a cohesive unit such that they work well together, they feel they can count on each other, and they can anticipate and understand much of what the other members of the group are doing" (Nolan, 2013, p. 68). Participants in the Integrated Teams typically include officials from the police and intelligence agencies, but can also include a combination of border enforcement officers, military officers, as well as immigration officers. Information-sharing within the Integrated Team occurs when participants bring information from their home agency to bear on a particular case or file at hand. Information-sharing at the operational level, therefore, occurs largely on a personal and informal basis. In Canada, examples of integrated teams include the Integrated Border Enforcement Teams (IBET) and Integrated National Security Enforcement Teams (INSET) (Office of the Auditor General, 2009, Ch. 1, p. 11). In the UK, integrated teams include the Special Operations 15 (SO15) and the Counter-Terrorism Units (CTUs). In Australia, the Australian Crime Commission (ACC) is an example of an Integrated Team (O'Connor, 2006, p. 318).

In contrast to Integrated Teams, Integrated Threat Assessment Centres (ITAC) embody efforts to share information at the strategic and government advisory levels. Similar to Integrated Teams, ITACs work by bringing together the various representatives from different agencies and departments together that have a role to play in counter-terrorism, national security or public safety. The purpose of ITACs are to integrate and centralize high-level intelligence products and assessments for government-wide and high-level strategy. In their central position, ITACs also set priorities and tasking for the individual departments and agencies. The number of representatives in an ITAC can be significant. For example, the Joint Terrorism Analysis Centre (JTAC) in the UK is composed of analysts seconded from 11 different departments. The UK appears to have achieved the greatest level of centralization with JTAC as its single national center for analysis. Canada and

Australia have to a lesser degree centralized high-level intelligence functions, having maintained multiple ITACs.

We also found similar goals of "networked inter-operability" in Canada, Australia and the UK. Networked inter-operability refers to the capacity for computers, networks and databases to speak with one another. To put it another way, inter-operability refers to "… the ability to work together effectively without prior communication, to find, retrieve, exchange, and re-use content in a useful and meaningful manner " (Treasury Board Secretariat, Standard on Web Interoperability, 2013). Inter-operability objectives, as such, represent a more formal and less social mode of information-sharing when compared to information-sharing that occurs within Integrated Teams or ITACs. We found that Canada and the UK have not achieved technical interoperability of their different computer databases and systems. It remains uncertain whether the same project in Australia has achieved any success. In Canada, the Interoperability Working Group disbanded shortly after its creation. In the UK, the SCOPE initiative, as well as its successor SCOPE 2, has largely been abandoned (Field, 2009, p. 1005). In Australia, attempts at interoperability are encompassed in the ALEIN and ACID projects as managed by the CTCC (ACC Annual Report 2004-2005, p. 33). Recent performance reports published by the ACC indicate that the use of ALEIN is increasing, while ACID's capacity to connect all police and intelligence databases have not been reached. ACC is planning to introduce a new system to either supplement or replace ACID called the National Criminal Intelligence System (NCIS) (ACC Annual Report 2013-2014, p. 94).

Information-Sharing in the Canadian Context: Dissimilarities

Unlike the UK and Australia, information-sharing practices in Canada are significantly influenced by US-Canada trade relations. Immediately following the 9/11 terrorist attacks, it was suggested that the airline hijackers had gained entry into the US through Canada (Charters, 2008, p. 21). The stories turned out to be false, but apprehensions over the issue of border security nonetheless quickly moved to the forefront of US-Canada diplomatic relations (O'Connor, 2006, p.154). For Canadian officials, however, the issue of border security is closely tied to economic interests (Ek, 2010, p. 28). For instance, in 2010 commercial trade between the two countries was valued at an estimated $645 billion, a figure that represents approximately $1.7 billion worth of goods and services that crossed the Canada-U.S. border daily (Meyers, 2003, p. 15). Given the economic significance of Canada's bi-lateral trade relationship with the US, any threat of a closure or delay at the border would prove devastating to the Canadian economy. As such, Canadian officials found themselves under tremendous pressure to both secure the border from terrorist incursion while at the same time ensuring that the borders remain porous and open so as to maintain the massive amounts of cross-border flows (Ackleson, 2005, p. 150).

The solution to this awkward dilemma appears to lie in the use of advanced screening and information technologies in order to make the border 'smarter'. That is, the smart border strategy attempts to secure the border through the risk-management and pre-emption of potentially dangerous travelers as supported by intelligence and threat assessments (Bauman, 2009, p. 275).

The notion of the border as a mechanism that seeks to filter dangerous persons and goods from legitimate cross-border flows is not entirely new, however. Traditional notions of the border, as a physical entity that separate territorial boundaries, have given way to conceptions of a border that functions more as a complex filter. This evolution is the result of a confluence of global forces such as economic integration and trade liberalization (Andreas, 2000, p. 4). In any case, the logic of pre-emption involves the use of shared information and intelligence assessments in order to try and determine the intent of a traveler before they arrive at the site of the border. Information-sharing, in other words, has come to underpin the strategy of screening for, and thus preventing, unwanted entries at or beyond the physical location of the border (Cote-Boucher, 2008, p. 142).

For example, the Statement of Mutual Understanding on Information Sharing (2003), under the Smart Border Agreement (2003), stipulates 30 categories of information about an individual that security services from Canada and the United States may exchange. The information now routinely shared includes a passenger's citizenship status, immigration history, physical descriptors, as well as attributed religion. The data is then used to examine the "life story" of the traveler so as to provide an assessment and ranking as to their level of threat (Cote-Boucher, 2008, p. 158). Other programs aimed at pre-screening commercial and travelers include the Container Security Initiatives and International Ship and Port Facility Security Code, as well as the PACE and NEXUS programs. More recently, the Canadian government also announced a new initiative to track and share information on the entry and exit of travelers and goods in both the US and Canada (Chase, 2011, Globe & Mail). In the U.S., The *Enhanced Border Security and Visa Reform Act* of 2002 is another example of the increasing use of information-sharing to support the advanced screening and risk-management of goods and travelers flowing through North America. The Act, as well as other DHS provisions, similarly mandates the sharing of intelligence between the DHS and other government agencies in the US. The Act also mandates the interoperability of databases within DHS that relate to the border security (Ackleson, 2005, p. 148).

By employing these new strategies for security screening, Canadian officials hope to reassure its American neighbours of their domestic security while at the same time ensuring that border flows remain unimpeded and business friendly (Salter, 2004, p. 76). These strategies, however, do not necessarily operate according to precise knowledge relating to terrorism and criminality. Rather they are guided by a risk-management approach that employs heuristics based on statistical descriptors and sociological narratives (Salter, 2004, p. 78).

7. INFORMATION-SHARING IN A VERTICAL WORLD: REACHING THE LIMITS OF THE TRADITIONAL DEPARTMENTAL MODEL?

In this chapter, I argue that the recent information-sharing failures point to a deeper and systemic organizational problem. In particular, information-sharing appears to confront tensions between the requirement for the organizational integration and unity of effort, on one hand, and the requirement for organizational differentiation and specialization, on the other. A greater demand for horizontal integration is mainly a consequence of counter-terrorism work that seeks to employ innovative conceptions of intelligence analysis in response to a new and evolving threat environment. However, there appears to be limits to the kinds of integration that can be achieved within the traditional departmental model. What follows is an analysis of the underlying bureaucratic structures that present problematics for information-sharing objectives.

Assessing the Post-9/11 Integration Model

The performance of the post-9/11 integrated model is difficult to measure, in terms of the number of terrorist attacks prevented due to improved information-sharing. Recent findings from the 7/7 inquiry, as well as the Auditor General report on national security in Canada, however, suggest that the post-9/11 integration initiatives above has not succeeded with respect to information-sharing policy objectives.

The 2005 Terrorist Attacks in London, UK

On the morning of Thursday, 7 July 2005, four British Islamist men detonated three bombs aboard the London Underground trains and another bomb on a bus in Tavistock Square. 52 civilians were killed, resulting in the worst terrorist incident in the UK since the 1988 Lockerbie bombing (CNN Wire, 2013). A public inquiry into the investigations leading up to the 7/7 terrorist attacks revealed that critical pieces of information again were not being shared among intelligence and policing agencies in the UK. It was known, for example that 7/7 terrorist Mohammad Siddique Khan was associating with known terrorists and had been participating in terrorist training camps overseas. Despite the introduction of the integration entities noted above, this discovery was never shared or integrated for broader analysis, and thus remained known only by a few persons. In particular, Khan's travel history, his home address, recent photos and his car registration were never connected to his training activities overseas. The significance of this information were not realized until too late, again because they were considered in isolation (Field, 2009, p. 1000).

Despite the efforts to achieve networked inter-operability, it also became evident that analysts continued to rely on making personal requests for information. Analysis into the 7/7 investigations showed that several personal requests for information by intelligence analysis were denied. This resulted in the standstill of several significant investigative leads. In addition, a separate inquiry into the UK's National Special Branch Intelligence System also found that police and intelligence databases remain disconnected. Rather, the system only provided a vertical link between the

police and MI5 (Field, 2009, p. 1006). It would appear, as such, that familiar information-sharing failures problems endure in the UK case.

The Auditor General's report on National Security Initiatives in Canada

An audit conducted by the Auditor General (AG) in 2004 found that Canada's overall management of its post-9/11 national security initiatives were "seriously lacking". The AG concluded that overall there continues to be "…deficiencies in the way intelligence is managed across the government". The AG also argued that the government has failed to "… learn[] from critical incidents such as 9/11 or develop and follow up on improvement programs" (Report of the Auditor General, Chapter 3, 2004, p. 1). In particular, the AG voiced its concern over the lack of full participation, as well as the quality of participants, in Canada's ITACs. The AG pointed to the absence of Citizenship and Immigration Canada as particularly worrisome. The AG also expressed concern over ITACs level of staffing and expertise. The AG found that most of the staff in ITAC were seconded from other duties and specialization. As such, there were concerns whether ITAC staff had the requisite skills or experience needed for counter-terrorism intelligence analysis (Office of the Auditor General, Chapter 3, 2004, p. 15). A lack of full participation was also noted in the Maritime Security Operations Centres (Lerhe, 2009, p. 5).

The AG was also critical of information-sharing methods that continued to rely primarily on established personal relationships rather than on any formal operational procedures or integrated electronic information systems. As an example, the AG noted an instance where a terrorist tactical alert had been misaddressed, resulting in a one-month delay in its eventual receipt. Fortunately, the alert turned out to be false (Office of the Auditor General, 2004, Ch. 3, p. 15). The informal nature of information-sharing was similarly found in a separate study conducted by the Solicitor General. In their study, the information-sharing practices between security and transportation agencies at the Pearson International airport were analyzed. The study found that information that had been shared between the two agencies relied mainly on personal connections rather than established formal processes or networked computers (Office of the Auditor General, 2004, Ch. 3, p. 20).

Other developments also suggest that there has been little progress or success with respect to networked inter-operability projects. For example, the Interoperability Working Group, composed of a group of Assistant Deputy Ministers, disbanded soon after its creation. The task was picked up a year later by the Solicitor General, only to have the project fall again to the wayside. The project was revisited in 2008, this time by the Chief Information Officer and the PSEPECT. PSEPECT progress, however, appears limited as it has gone only so far as to publish a report outlining a high-level strategic framework for achieving interoperability. The report, moreover, lacks specifics and does not detail any goals or explain how interoperability will be achieved. Also, the government has not officially endorsed the report (Office of the Auditor General, 2009, p. 23).

The enduring aspect of intelligence failures suggest that the post-9/11 integration reforms outlined above are not entirely effective at achieving the policy objectives of information-sharing.

What follows is an analysis of the traditional departmental model and their structures of coordination. The analysis suggests that there appears to be limits to the kinds of integration that can be achieved within the traditional departmental model.

Dividing Work in the Departmental Model: Differentiation and Specialization

Classical organizational theorists have long argued that the fundamental basis of an effective and rational organization lies in the optimal division of labour. Public administration theorist Luther Gulick, for example, argued that the question of work division represented nothing less than the foundation of organizational theory, as illustrated in the following quote:

> The theory of organization has to do with the structure of co-ordination imposed upon the work-division units of an enterprise. Hence it is not possible to determine how an activity is to be organized without, at the same time, considering how the work in question is to be divided. Work division is the foundation of organization; indeed, the reason for organization (Gulick, 1937, p. 3).

The antithesis of the division of work, in other words, would involve a single person doing the total job. This would be supremely inefficient and ineffective as any attempt would "… take longer, result in spoiled material, and be done by hands unskilled". Thus, Gulick argued that "… the best results are secured when there is a division of work among these men" (Gulick, 1937, p. 5).

Organizational efficiency and effectiveness are also the result of work specialization and expertise. Such specialization is gained by focusing the inherently limited time and energy of the individual worker to apportioned and repeatable tasks. It follows, however, that if work is to be divided, then it must also be integrated back, in order to serve the ultimate ends of an enterprise. The principal purpose of the organization, in other words, is coordination (Gulick, 1937, p. 33). As such, we define organizational coordination as:

> a system of interrelated behaviour of people who are performing a task that has been differentiated into several distinct subsystems, each subsystem performing a portion of the task, and the efforts of each being integrated to achieve effective performance of the system (Lawrence, 1967, p. 3).

Work specialization and subsystem differentiation, however, can pose particular structural problems for information-sharing initiatives. These problems are discussed later.

Coordination and Integration in the Departmental Model

The principal means of achieving organizational coordination in the bureaucratic model is through a system of hierarchy and legal authority (Keast, 2002, p. 4). These systems regulate the relations of individuals. The hierarchy of supervision, for example, is based on a series of superior-subordinate relationships. It is through this chain-of-command that management exercises

leadership and control over the activities and tasks of the differentiated sub-systems. That is, hierarchy underpins the system of managerial control and direction over the administrative, operational, and policy workings of the organization (Hammond, 2007, p. 406). These systems are predominant in government agencies, which are often characterized by their high level of complexity and formalization. Government agencies are also typically managed through top-down communication patterns that involve minimal level of participation in decision-making by employees (Robbins, 1993, p. 515).

The responsibility of ensuring coordination, moreover, rests with the person sitting at the top of the chain-of-command, that is, the organization's leadership. A single person, however, can only be expected to direct a limited number of subordinates at a time, due to the inherent limits to their time, energy and knowledge. Likewise, in order to avoid confusion and inefficiencies associated with having two or more superiors, each subordinate should report to a single superior at a time (Gulick, 1937, p. 9). Flowing from these two requirements is the particular ratio of superior-to-subordinates within the organization's hierarchy. This ratio is also known as the organization's span-of-control. A higher ratio of superior-to-subordinates will reflect a more vertical hierarchy in the organization and vice-versa (Robbins, 1993, p. 496).

The use of hierarchical means of organizational coordination, however, can serve to segregate information, knowledge and activities, creating problems and barriers for inter-agency information-sharing objectives. Such difficulties are likely to arise as the organization grows larger, and the hierarchy of supervision becomes increasingly vertical. For instance, as the layers of management and supervision increase, the messages passed along the chain become more prone to error or distortion because messages must move in lockstep through the increasing layers in the chain-of-command. At worst, message can be intentionally repressed or modified (Johnson, 2002, p. 245). When such distortions or repressions occur, the knowledge and activities between the various work divisions become disconnected. This structural problem is sometimes referred to as a separation between the locus of information and the locus of decision-making. When key activities and knowledge are not being communicated properly within the system of hierarchy, as such, a leader's capacity to direct and orchestrate the differentiated sub-systems can be undermined (Bardach, 2005, p. 357). Such communication breakdowns within a system of hierarchy, in other words, can be tantamount to a critical failure in organizational coordination.

Another related means for achieving organizational coordination is departmentation. Departmentation refers to the grouping or categorization of similar or homogenous work divisions at the organizational level (Quinn, 2003, p. 207). That is, departmentation seeks to achieve efficiencies by managing similar activities and tasks together. Conversely, departmentation avoids the difficulties and inefficiencies with having to manage dissimilar work together (Hammond, 2007, p. 407). The logic for departmentation was also theorized by Luther Gulick, who argued that work can be divided along one of the following four fundamental and mutually exclusive characteristics of work, which are:

- The major purpose a worker is serving, such as furnishing water, controlling crime, or conducting education;
- The process a worker is using, such as engineering, medicine, or carpentry;
- The persons or things a worker is dealing with or serving, such as immigrants, veterans, or forests and mines;
- The place where a worker renders his service, such as in Vancouver or Hawaii (Gulick, 1937, p. 15).

The decision as to which basis was best to use in order to form a department rested on a number of factors and assumptions. The nature of the work conducted, the organizational culture, the values of the group doing the work, and the respective advantages or disadvantages between each method are all important factors for consideration (Hammond, 2007, p. 406). Gulick, however, was careful to point out that no one method of division is inherently superior to the other, but rather each method carries inherent trade-offs. In reality, each of the four fundamental characteristics of work is intimately related with the other three. It is not possible, for example, to not work for some major purpose, uses some process, deal with some person or client, or work at some place (Hammond, 2007 p. 416). Thus, most departments have a combination of sub-units that are divided along one of the above four methods of departmentation. The hierarchy of supervision remains relevant with respect to departmentation as each department is then expected to be headed by a middle-manager. The middle-manager, in turn, then reports up the chain to senior managers to account for day-to-day operations, budgets and program activities (Robbins, 1993, p. 493).

The process of departmentation, however, can also serve to segregate information, knowledge and activities. For one thing, departmentation can lead to a dominant professional group identity where professional expertise and specialization becomes prominent. Members of a professional group that works closely together often share some set of assumptions, opinions, core knowledge, or perception of reality (Dawes, 1996, p. 381). This can be problematic for information-sharing as professionals and experts become accustomed to working independently (Yang, 2011, p. 167). It can also be especially challenging for collaborative efforts between different professional groups as the different assumptions and orientations towards the external world can lead to different standards, expectations and perceptions on how information can and should be used (Bigdeli, 2013, p. 828).

Organizing Counter-Terrorism Work: Structural Coordination Problems

The need to balance organizational specialization and differentiation with the need for integration and coordination is a permanent struggle for managers of all large modern organizations (Bakvis, 2004, p. 13). With respect to organizing and managing counter-terrorism work, however, the struggle is especially pronounced. For one thing, the post-9/11 counter-terrorism mission invokes an immense range of differentiated tasks and sub-systems due to the complex, time-sensitive and far-reaching nature of the work. Intelligence work, for instance, necessarily involves multiple missions that must be pursued, various processes required in order to acquire intelligence, and

multiple geographic areas to be covered. In addition, there can be an urgent and simultaneous need to recognize all these demands in moments of emergency and crisis. The design of any given intelligence community will, therefore, require several layers of agency sub-units to reflect this complexity and multiplicity (Hammond, 2007, p. 416).

To illustrate, we can take as an example the task of organizing the work of intelligence collection. A number of methods and processes exist for obtaining intelligence, such as HUMINT, SIGINT, FININT, IMINT and MASINT (Rudner, 2010, p. 132). If we were to consider the creation of a department for each respective method of intelligence collection, we would also be required to recognize the other characteristics of work, namely purpose, place and client served. Thus, a department that first divided on the basis of the process would find it necessary, in each process based department, to divide then by purpose, and then possibly again by geography or client. The need to immediately recognize purpose reflects the fact that technical expertise in the process of intelligence collection cannot be the end goal in itself. Intelligence collection specialists must match their methods to a particular purpose within the broader purpose of preventing a terrorist attack. As such, we can similarly imagine a process-based department that was further divided along various purposes such as the purpose of determining the intentions of specific terrorist groups in Russia, the Middle East or South East Asia (Hammond, 2007, p. 413). In addition, there can be a need to immediately recognize place. Such requirements reflect the realities that intelligence targets often are geographically localized. Thus, numerous secondary sub-units may also be needed within a process-based department in order to target the various areas of the globe.

From this example, it is clear that the complex, urgent and far-reaching nature of the counter-terrorism mission necessitates a high level of organizational specialization and differentiation. Indeed, the counter-terrorism mission implicates the mandates and missions of numerous government agencies and departments. In Canada, for instance, it has been estimated that the counter-terrorism mission touches upon the mandates of no less than 25 Canadian government entities. Of these 25, at least 16 are said to have a crucial role in counter-terrorism (O'Connor, 2006, p. 127). The situation is similar in the United States where the following departments and agencies all play an important role in the counter-terrorism mission, namely: the CIA, the FBI, the NSA, Homeland Security, DOD, the Defense Intelligence Agency, the Drug Enforcement Administration, the Office of the Director of National Intelligence (ODNI), the Office of Intelligence and Counter-Intelligence (OICI), the Office of Intelligence and Analysis (I&A), the Bureau of Intelligence and Research (INR), the Office of Terrorism and Financial Intelligence (TFI), the National Geospatial-Intelligence Agency (NGA) and the National Reconnaissance Office (NRO) (Nolan, 2013, p. 4).

The high level of specialization and differentiation needed for the mandate of counter-terrorism, however, can be problematic for integration efforts such as information-sharing. For one thing, the vast amount of communication that would have to occur between the numerous purpose-based, place-based and process-based departments and their sub-units would be immense. Such massive flows of communication required to coordinate each differentiated sub-system would

likely overwhelm any hierarchical-based coordination system. The communication demands placed on them would be too large to have to force them to move through a vertical span-of-control (Hammond, 2007, p. 418). This is precisely what had occurred immediately after 9/11. For example, the RCMP's immediate response to 9/11 was hindered by confusion as a result of the massive amounts of communication that flowed between Project A-O and their FBI counterparts. The communication proved overwhelming as the RCMP's National Head Quarters (NHQ) was not able to route such high-volume of communications through their office. Delays were also the result of uncertainty and indecision over the appropriate level of latitude that the operational units such as Project A-O ought to be afforded when sharing information with the FBI (O'Connor, Analysis and Recommendations, 2006, p. 108).

Coordinating Different Professional Frameworks: Intelligence and Policing

The extensive level of specialization in counter-terrorism work also leads to a correspondingly high level of professional and social identities, as divided along departmental lines. These professional divisions within the intelligence community are also especially pronounced and present another significant obstacle to information-sharing objectives. For example, in Canada counter-terrorism involves both the mandates of the CSIS and the RCMP. The differences found in the professions of policing and intelligence, however, can result in inter-agency conflict. In particular, the division between police and intelligence work can result in different and competing perspectives on the use and value of information.

The RCMP, for example, tends to collect information about crimes in the expectation that the information will be disclosed openly to the accused and relied upon for public prosecutions. CSIS, on the other hand, is focused primarily on collecting evidence from foreign allies or domestically using covert methods for the purposes of informing and advising the government on threats to its national security. The difference here stems from the different purposes of each department, with CSIS's key mandate to advise the Government of Canada on threats to its security. The RCMP's mandate, on the other hand, is the public prosecution of criminals. CSIS, as such, views information through a lens oriented largely towards the executive branch. The RCMP, in contrast, conducts its activities in a comparatively overt manner, with its activities directed predominantly towards the judicial branch of the Canadian government (Major, Vol. 3, 2010, p. 12).

Other professional differences between the RCMP and CSIS include the type of information being collected. Intelligence investigations, for example, are sometimes referred to as being concerned with so-called "macro-crimes." Macro-crimes are crimes considered to be threats to society in general. Policing investigations, in contrast, tend to focus on crimes that have a more concrete effect on individuals than society per se. The kinds of information obtained by intelligence agencies, as such, tend to include information about terrorist or criminal organizations, their members, their goals, their capacities, and their sources of funding (Berman, 2014, p. 12). Intelligence collection, as already mentioned, often involves covert means of information gathering, surveillance and disruption that operate outside the judiciary's direct purview. Criminal investigations, on the other hand, are more directed towards the individual or discrete nature of a

crime. As such, they typically focus on specific acts in order to collect evidence related to a past or impending crime. Such investigations also tend to end at the point of a judicial prosecution. In contrast to intelligence work, police work also involves methods of deterrence and visible patrolling vis-à-vis the criminal law (Bayley, 2009, p. 82).

These professional differences have led to inter-agency conflict with respect to the disclosure of confidential information. For example, the question of public disclosure of sensitive information was a key disagreement between the RCMP and CSIS during the investigations that led up to the Air India Flight 182 attacks. The RCMP wished to proceed on the information shared by CSIS in support of warrants for communications intercepts on key terrorist suspects Parmar and Reyat. CSIS, however, wished to limit such material for the purposes of "investigative leads" only (Major, Volume 3, 2010, p. 93). CSIS's reluctance to disclose its intelligence in the legal domain reflects valid concerns over the public disclosure of their operational methods and assets. CSIS is concerned that such public disclosures could reveal covert intelligence sources, methods and assets. The refusal to share information, therefore, was done in the interest of protecting CSIS's ability to carry out future investigations (Major, Volume 3, 2010, p. 136). From a strictly law-enforcement perspective, however, such information would be less valuable if it could not be used in the court of law for the prosecution of terrorist criminals (Major, Volume 3, 2010, p. 12). Similar inter-agency conflicts in the UK and US have been noted as well. In the investigations leading up to 7/7 in the UK, conflicts arose between the police, MI5, MI6 and the GCHQ. Disputes arose over the similar issue of whether to use limited resources towards securing a criminal conviction or whether to use them in support of covert intelligence gathering. The police, moreover, were sometimes reluctant to devote attention to complex counter-terrorism cases as they diverted resources away from community policing activities (Field, 2009, p. 1000).

Principle-Agent Problems: the Problem of Information Hoarding

Conflicts between departments and agencies can also extend beyond matters of professional differences. Information-sharing projects can also fail when agencies or individuals hoard or safeguard information out of self-interest. The problem is sometimes referred to as the "principle-agent" problem. In the context of counter-terrorism, the principle-agent problem relates to the value of information as a source of considerable power and stature for both the agency and the individual. That is, agencies sometimes refuse to share their information out of a rational cost-benefit calculation. To illustrate this organizational dilemma, we first define the actors and their main interests.

First, in a principle-agent problem we assume that the principle is represented by the Central or Executive Government. The agents, on the other hand, are the various departments and agencies responsible for public safety. A key interest of the principle, as such, is the effective sharing of information and agency coordination. The agents, however, have interests that may not be consistent with the objectives of the principle. In particular, government agencies tend to be concerned with achieving bureaucratic influence and autonomy. Influence in the intelligence and public safety context refers to the ability "… to mold the decisions of the senior policymakers who

consume the agency's intelligence products and the ability to prevent rival agencies from doing the same. Autonomy, on the other hand, refers to "… the ability to pursue their core priorities without external interference". In addition, the agents tend to perceive these interests as a zero-sum game. That is, agents can seek to maximize their influence and autonomy by minimizing the influence and autonomy of rival agencies (Sears, 2010, p. 332). As such, agencies can sometimes actively resist information-sharing initiatives because they conflict with their self-interests in bureaucratic autonomy and influence.

With respect to bureaucratic influence, an agency may not want to share information for several reasons. For one thing, an agency may fear that rivaled agencies will free-ride off their shared information. That is, information-sharing can result in superior analytical outputs, but not necessarily for the originating agency. When the benefits of the superior product are not captured by the originating agency, the rivaled agency then free-rides off the efforts of the originating agency. Moreover, by improving their analytical outputs, the rival agency also improves the likelihood that intelligence consumers will "buy" more of their superior product, and fewer of their own. The decision not to share information, as such, can be a rational one in which the agency seeks to prevent a rivaled agency from benefiting from their information sources. Conversely, an agency that hoards information can stand to capture all the benefits of that information by refusing to share that information. Rival agencies are then denied potentially useful information, which will mean lower quality intelligence products that they are available to produce for policy-makers. The consequence of not sharing can result in greater influence for an agency in terms of its ability to produce a relatively superior quality intelligence product. It also prevents the agency from missing out on receiving any credit for an intelligence breakthrough (Sales, 2010, p. 307).

Information-sharing objectives can also threaten an agency's autonomy. For example, an agency may refuse to share information in the interest of preventing a rivaled agency from gaining a foothold into an investigation they consider as their own (Sales, 2010, p. 320). That is, the sharing of information about a particular investigation or lead can threaten an agency's capacity to pursue that investigation in an independent and exclusive manner. Exclusivity in this regard means the ability to claim exclusive authority over a jurisdiction and ensure control is not ceded to rival agencies. Such competitions for "turf" are especially pronounced where work purposes or mandates overlap (Sales, 2010, p. 282). In the examples outlined above, both the CSIS and the RCMP in Canada, or the FBI and CIA in the US, may both plausibly claim jurisdiction over a given national security investigation. Agencies, as such, may become wary of information-sharing practices that can give them an opportunity to vie for control over their investigation or operation (Sales, 2010, p. 311).

At the personal level, the prospects of sharing information, as well, can become a matter of calculation between their perceived costs and benefits. Due to reward and incentive systems in the workplace, individuals may also see each other as potential rivals and competitors. Information, moreover, is often seen as a personal prized asset and considerable source of power and stature (Dawes, 1996, p. 380). As such, individuals may be reluctant to share valuable

information. A staff member, for example, may be worried that by contributing to the collective good of information-sharing he or she would evoke further requests for information, clarification or assistance. Such persons may want to avoid the added time and effort needed to articulate, prepare and arrange information for sharing. The extra work can also compete with the individual's work time and resources and can thus appear costly, especially if there is no clear recognition or benefits for the work done. The benefits of sharing will be even less appealing if the information shared incurs criticisms over possible inaccurate or irrelevant information (Yang, 2011, p. 168).

A recent analysis on the National Counterterrorism Centre (NCTC) in the U.S., appear to bear these dynamics out. The analysis found that intelligence analysts often put their self-interests above any collaboration efforts. Analysts found themselves with disincentives to share information when there were no clear benefits in terms of rewards or promotions. As a result, it was noted that analysts sometimes simply failed to seek sharing opportunities. In more precarious situations, analysts were found to outright and actively undermine the work of other analysts for personal gain or promotion (Nolan, 2013, p. 162). Moreover, the act of co-locating analysts from the different U.S. intelligence agencies, in some cases served to intensify inter-agency conflicts (Nolan, 2013, p. 166).

8. TOWARDS A WHOLE OF GOVERNMENT APPROACH TO INFORMATION SHARING?

If the recent failures to share information can be attributed to the structural features inherent to the traditional bureaucratic model of organization, then one way forward would be to consider possible changes to the limiting or problematic structures. One alternative to the departmental model of organization can be found in the "horizontal management" or "whole-of-government" approach to management and organization. These approaches attempt to address contemporary social and policy issues that have become more complex and horizontal in nature. What follows is a brief review of the literature on horizontal management methods in order to assess possible solutions to the coordination and integration problems underlying information-sharing failures.

The Rise of Complex Horizontal Problems in a Vertical World

There is a growing sense that many contemporary social and policy problems have become more complex and horizontal in nature. Some examples of horizontal problems include: climate change, urban and global poverty, a globalizing economy, urban aboriginal issues, as well as emerging pandemic threats such as SARS and Avian influenza (Christensen, 2007, p. 1060). These social and policy issues are horizontal in the sense that they easily transcend the mandate of any given department, defy precise definitions and have no simple or straight-forward solution. Traditional institutional structures, as such, can find themselves ill-equipped to tackle them. Horizontal issues also tend to be pressing in the sense that they cannot be ignored as doing so would result in a high cost to society (Keast, 2002, p. 7). Early horizontal projects in Canada date back to the 1990's when governments attempted to tackle issues of poverty, climate change, and innovation in a globalizing economy. Similar efforts were also noted in the United Kingdom, Australia, New Zealand, and the U.S. (Christensen, 2007, p. 1061). More recently, the Prime Minister's Advisory Committee on the Public Service in Canada argued that the traditional Westminster model of authority and accountability does not adequately address today's problems and for this reason call for correspondingly horizontal solutions (Clerk of the Privy Council, 2013). In short, while perhaps not new, there is growing recognition for the need to improve coordination radically in order to address today's complex, horizontal and pressing problems (Bakvis, 2004, p. 10).

Responding to Horizontal Problems: The Horizontal Management Approach

Horizontal management methods and can be found under various banners such as the "whole-of-government" approach, "joined-up government", "networked governance", and "thinking up and out". These approaches, however, do not refer to a coherent set of ideas and tools. Rather they are best understood as an umbrella term that characterizes a set of responses to the problems associated with poor horizontal coordination and fragmentation in the public sector (Christensen, 2007, p. 1060). The instruments used to implement horizontal initiative also vary, ranging from informal networks of workers to more formal and jointly managed secretariats. Horizontal management efforts, moreover, can usually be found described in terms such as "coordination", "collaboration", and "partnerships" (Bakvis, 2004, p. 8). Recent modernization initiatives in

governments are also increasingly looking towards new ways of employing Information Communication Technologies (ICTs) to replace the more hierarchical and rigid forms of management with a more flexible, networked and agile organization. ICTs are also increasingly promoted as a way to increase participation within and between government agencies, not-for-profit and private organizations (Gil-Garcia, 2012, p. 269).

Given the broad nature of the horizontal management approach, definitions of horizontal management can vary. The Australian public service defines horizontal management as, "... public services agencies working across portfolio boundaries to achieve a shared goal and an integrated government response to particular issues". The UK uses the term "joined-up government" to refer to the amalgamation of stakeholders. The term also refers to the creation of "synergies" for the effective use of scarce resources in order to tackle "wicked issues" (Christensen, 2007, p. 1060). A more precise and useful definition is one that understands horizontal management as:

> … the coordination and management of a set of activities between two or more organizational units, where the units in question do not have hierarchical control over each other and where the aim is to generate outcomes that cannot be achieved by units working in isolation (Bakvis, 2004, p. 15).

The horizontal management model, as such, appears to be part of the broader challenge to the traditional notion of the use of hierarchies and a top-down system of authority as the best method of organization (Johnson, 2002, p. 250).

The Horizontal Management Approach: Coordination through Better Decision-Making?

One suggested alternative to the traditional model of bureaucracy is the use of inter-personal networks and more participatory forms of management (Keast, 2002, p. 5). Thus, rather than seeking coordination through traditional structures of hierarchy and authority, coordination is instead sought through effective organizational decision-making. The notion of superior decision-making as the basis for effective organizational coordination appears to stem from the argument that coordination cannot work in the presence of critical organizational communication failures. The organization, in other words, can achieve more successful coordination by moving systems of authority away from the traditional chain-of-command and by bringing employees into the decision-making process (Kettl, 2003, p. 260). Several advantages of this model are advanced by their proponents.

First, participatory decision-making is more likely to educate both employees and management on the operational workings, as well as the strategic directions of the entire organization. As a result, management can regain crucial knowledge about how the organization actually operates at both the formal and informal level. Such learning opportunities are also more likely to engender institutional values and cultures of interdependencies because employees gain greater awareness of the problems, challenges, opportunities and realities faced by others in the organization. That is, workers are encouraged to look beyond their defined and divided roles and duties, as well to form connections among themselves. Such engagement, moreover, often involves consensus-

building and thus can serve as a strong basis for collective action. More participatory forms of decision-making are also argued to enhance the problem-solving and analytical skills of managers and employees. In short, effective participation in more networked and decentralized modes of organization are argued to reduce organizational problems as a result of superior organizational decision-making. Improved decision-making, in turn, leads to better communications and operations (Johnson, 2002, p. 259).

While more participative and networked modes of organization appear to offer an appealing solution to the problem of information-sharing, in terms of offering a more operationally effective means to pursue information-sharing objectives, such models also imply a significant break from the structural roots of traditional bureaucracies (Johnson, 2002, p. 250). Further study in the use of more horizontal management models in the field of counter-terrorism and public safety are therefore suggested, namely: (i) whether the necessary accountability mechanisms within a horizontal management model are sufficient for ensuring good governance consistent with the values of a liberal democracy, and; (ii) the potential implications of the rapidly evolving Digital Age on information-sharing regimes.

Information-Sharing in the Horizontal Model: The Question of Accountability

Accountability mechanisms largely follow the vertical hierarchy of supervision. The principle of ministerial responsibility, for instance, holds that the power within a political community should be exercised by elected officials as mandated by the electorate. This responsibility is ensured through a vertical chain of representation, steering and accountability relations between the electors and the elected. That is, it is through this hiearchical relationship that the elected administrators can be held to account for the way they carry out that mandate to the public (Koppenjan, 2009, p. 770). The principle of ministerial responsibility, therefore, underscores notions of political authority in a constitutional and liberal democratic state (Peters, 1996, p. 289).

There is a risk, however, that the principle of ministerial responsibility can be undermined when systems move away from established vertical accountability regimes (Koppenjan, 2009, p. 770). Thus, even if a horizontal management approach to information-sharing proves to be operationally effective, it may be ultimately undesirable if sufficient mechanisms are not also in place to ensure public accountability. Without sufficient accountability mechanisms, there is an increased danger from mismanagement, error or overextension of authority (Roy, 2005, p. 472). In the context of counter-terrorism and public safety, these risks are significant.

For one thing, information-sharing systems involve increasing variability with respect to the sources of the information obtained. In Canada, the RCMP collects information from a wide variety of sources. This includes provincial and municipal police forces, the CBSA, Citizenship and Immigration Canada, CSIS, the CSE, and Transport Canada. Information, however, also is increasingly obtained from foreign police agencies and foreign security intelligence agencies (O'Connor, 2006, New Review Mechanism, p. 435). Information stored in the RCMP's Secure

Criminal Information System (SCIS), for example, comes from a range of international policing and intelligence partners (O'Connor, A New Review Mechanism, 2006, p. 109). In addition, the Statement of Mutual Understanding on Information Sharing (2003) has also increased the sharing of information from US sources (O'Connor, A new Review Mechanism, 2007, p. 167). Canada's terrorist watch list also receives a significant portion of its data from the US's TIPOFF program, which integrates information obtained from the CIA, the FBI and the NSA (Office of the Auditor General, 2004, Ch. 3, p. 29). Overall, with respect to foreign intelligence collections, the RCMP has reported that it receives seventy-five times more information from partner agencies than it provides. Such an imbalance reflects Canada's limited foreign intelligence collection capacities and thus reliance on the use of its relationship with its allies to receive intelligence (Forcese, 2009, p. 4).

The responsibility for assessing the reliability and validity of the information received, however, remains with the individual departments. This responsibility includes decisions on whether to enter shared information into a national security database. The decision of how long to retain the information is also the responsibility of the host department (Oconnor, 2006, New Review Mechanism, p. 435). As such, there appears to be no central review mechanism to ensure the exchange of valid and reliable information in Canada. The lack of external checks increases the potential for the repetition of unverified or unreliable information. Some critics have argued that this is especially concerning because information cannot be said to be entirely objective. Rather, information is subjective and fungible. The concern is that inaccurate information can become legitimized through the process of its repetition, exchange and circulation within security information-sharing systems (Cote-Boucher, 2008, p. 149). In addition, the lack of a central review mechanism also means that the information shared between security agencies are mostly unknown to the general public. Individuals, as such, are unaware of the information that may be collected about them as well as with whom they have been shared. As a result, there is no avenue in which individuals can learn the nature, content, or accuracy of any information collected about them. As such, there is a lack recourse to challenge potentially false or misleading information (O'Connor, 2006, A New Review Mechanism, p. 435).

In response to growing public concerns over the lack of a central review mechanism, Ottawa has created a new joint Parliamentary Committee and an external advisory board on national security. It is unclear, however, to what extent this new mechanism can provide direct political review over foreign information sources. The Committee, for example, has already stated that information from third parties will only be shared with Parliamentarians with the consent of the providing party. Members of the Parliamentary Committee are sworn to secrecy for the course of their duties, moreover, which also effectively limits the public release of information that is reviewed by the Committee (Roy, 2005, p. 472). Thus, the increasing variability in the origins of information remains problematic for accountability as each jurisdiction has their respective system of review and oversight.

The question of assessing the reliability of received intelligence can also be problematic. For one thing, intelligence information often requires expert knowledge and process to interpret and

contextualize them. Police officers, for example, bring with them years of training and experience in interpreting criminal history information. These interpretive schemes are not easily transferred to someone without that particular background (Dawes, 2009, p. 394). When these interpretive and contextual information are not shared, it can create the risk where information can begin to take on several different yet plausible interpretations. Information without context, in other words, can be very ambiguous and fungible (Jones, 2008, p. 392). That is, the "knowledge wrapper" that holds the logic of data structures, definitions, collection methods, processes, and interpretive schemes must also be shared (Dawes, 2009, p. 396). It remains unclear, as such, how one can ensure the reliability and validity of shared information in situations where the necessary knowledge wrapper is also not shared.

Indeed, the decision to share information without appropriate context or shared understandings was a crucial error that led to the eventual arrest and deportation of Maher Arar. Concerns of another wave of terrorist attacks after 9/11 led to a flood of "real-time" information-sharing between the RCMP, CSIS the FBI and the CIA. It was in this circumstance that the RCMP, Project A-O unit, provided a large amount of information to US agencies with respect to Maher Arar. The information shared included the Project A-O's entire investigative database in raw format. The information was therefore not screened beforehand, nor were written caveats attached to provide any context to the information that was shared (O'Connor, Analysis and Recommendations, 2006, p. 23).

The pre-emptive and preventative approach to counter-terrorism also present accountability challenges. In particular, new criminal offences were introduced to enhance the capacity of police to investigate and interdict terrorist threats. These powers are for crimes related to the participation, facilitation, instruction, or harbouring of a terrorist (Safety, P, 2013, p. 39). The preventative approach to counter-terrorism, however, marks an important shift away from traditional notions of motivation in crimes and criminality. In the traditional view, the motivation for a criminal offense may only be used as a factor in determining the appropriate sentencing for a crime already committed. In the pre-emptive approach, police and security officials now include motivation as an area of legitimate inquiry and suspicion. This approach, as such, marks a significant departure from traditional propositions in criminal law that distinguish motive as an unnecessary element of a crime (O'Connor, 2006, A New Review Mechanism, p. 438).

Consequently, investigators and analysts can face a challenging situation in which their target becomes imprecisely defined. The situation for the investigator can be a precarious one as their intelligence collection practices can lead to the unintentional gathering of information relating to legitimate associations and religious and political activities. In other words, there appears to be a potential for intelligence activities to lead to a greater degree of government inquiry into the activities and private lives of citizens. Without sufficient accountability mechanism, this raises questions with respect to liberal democratic norms such as the rights to privacy and freedom of religion. It also raises questions about the practice of pre-emptive profiling and its potential effects of discrimination on innocent civilians (O'Connor, 2006, A New Review Mechanism, p. 438).

The Post-9/11 Intelligence Paradigm and Information Communication Technologies

Another suggested area for further study relates to the new frontiers of Information and Communication Technologies (ICTs), which indicate that information-sharing system will likely continue to evolve in entirely new environments. Developments in science and technology, for example, are advancing rapidly in areas such as genomics, biotechnology, nanotechnology, materials, artificial intelligence and robotics (Policy Horizons, 2013). Research in other sectors such as digital communications, health, manufacturing, and energy are also predicted to radically transform business and government (Zappa, Policy Horizons Canada, 2013, p. 1). Indeed, public sector "renewal" initiatives are already discussing the potential use of the ICTs to enhance governance and citizen access to, and participation in, government services and programs.

Government 2.0, for example, place greater emphasis on co-production and active participation, but as well as emphasize government transparency and collaboration with the private, public and not-for-profit entities. Such efforts seek to employ ICTs to provide communication and interaction with citizens at the various levels of government in order to improve service delivery. Discussions about the possibilities of Government 3.0 involve the anticipated arrival of sophisticated sensors, virtualization, geographic information technologies and social media applications. These technologies are looked at as possible ways to better manage the resources and capabilities of government in a more networked and integrated fashion (Gil-Garcia, 2012, p. 274). While forecasting technology's potential impact for business and governments is beyond the scope of this paper, we discuss some technological developments that appear to have implications to information-sharing.

Two so-called "laws" of technology in particular seem pertinent here. First, is the law of exponential growth. Gordon Moore, co-founder of Intel, for example, predicted a trend in computing power in which the number of transistors on a computer chip doubles about every two years. Ray Kurzweil similarly argues that the evolution of technology is not linear but rather exponential. Recent experience appears to bear this out, with computer chips doubling about every two years since the 1960's. The emergence of the World Wide Web (WWW) is another example, which followed the invention of the first personal computer by a mere fourteen years (Kurzweil, 2006, p. 17). Looking ahead, some researchers believe that the next generation of supercomputers will be exponentially more powerful than today's supercomputers that rely on electronics and binary digits. Tomorrow's supercomputers, rather, are predicted to employ the principles of quantum physics to power them (Gershon, 2013). The largest internet search engine Google Inc., for example, is investing in the prospects of tomorrow's supercomputers. Google has over one million servers in data centers globally. These servers are estimated to process one billion search requests daily, a figure that amounts to a staggering twenty-four petabytes of user-generated data that is collected on its users per day (Schonfeld, 2008). Google believes that it can one day leverage their data stores to develop the capacity to intuit what its users are interested in knowing at any given moment (Bennet, 2011, p. 10).

Researchers also continue to push the limits on memory storage capabilities. Researchers at the European Bioinformatics Institute, for example, have found a way to save data to synthetic DNA. According to these scientists, it is possible to store data in the equivalent amounts of approximately 100 million hours of high-definition video within a cup of DNA. Moreover, this data can be stored for at least 10,000 years without errors (Science Daily, 2013). Scientists at the University of Southampton are similarly pushing the boundaries of data storage. These researchers have found a method of storing vast quantities of data and a virtually unlimited lifetime storage life through the use of fused quartz (Science World Report, 2013). Another seemingly relevant technological development relates to the increasing miniaturization and proliferation of computers and sensors. It is predicted that this pattern of miniaturization will result in the so-called "naturalization" of technology. That is, computing and information technology will likely become embedded within the physical environment such that they become inconspicuous. Users will no longer interact with computers in the traditional sense, such as in the general use of a keyboard and mouse, but rather may lose awareness of any interaction with computing technologies. Interactions with computing technology in the future, in other words, may occur on a less conscious yet increasingly pervasive basis than before (RCMP Environmental Scan, 2007, p. 88).

It would appear that computing and information technologies will continue to present novel and innovative prospects for the field of intelligence analysis and information-sharing. It would also appear that information will likely be born and collected at a more unconscious, invisible, and frequent level than before, with the storing, pooling, searching and integration of data occurring on a scale unseen before in history.

CONCLUSION

After 9/11, public demands for greater security and safety, driven primarily by fears of another terrorist attack, brought about sweeping changes to national security and public safety policies and institutional structures in the US, Canada, the UK and Australia. These changes reflect an aspiration to design an intelligence-led, pre-emptive, and coordinated approach to counter-terrorism. While governments wanted to avoid repeating the same mistakes and avoid another intelligence failure, the Air India and 9/11 terrorist attacks also underscored a larger shift with respect to public security and safety. Following the Cold-War period, contemporary terrorist groups such as al-Qaeda appear to exemplify a new terrorist threat environment. Owing primarily to the characteristics of new terrorism, information-sharing has come to be seen as a means for coping with the greater uncertainty in regard to threats to public safety. Information-sharing, in other words, would serve as the foundation for pre-emptive defense against future terrorist attacks.

A review and comparison of the changes to institutional reforms relating to post-9/11 counter-terrorism initiatives indicate that Canada, the UK, and Australia have all responded to the demands for post-9/11 information-sharing in a similar fashion. Information-sharing mandates were commonly operationalized by way of “Integrated Teams” and “Integrated Threat Assessment Centres.” These reforms are consistent with the transformation of security institutions in the U.S., guided by the conclusions set forth in the 9/11 Commission that called on the U.S. government to become a "smart" government capable of integrating "all-sources" of information in order to "see the enemy as a whole". The basic logic underlying information-sharing was that by sharing and viewing information together, the seemingly disparate or inconsequential pieces of information would gain insights or connections not otherwise apparent when viewed in isolation. In addition, by increasing the flow of information from “all available sources” governments would bolster their ability to detect any terrorist enemy hiding within their domestic population.

However, the 2005 London Bombing attacks in London, UK, as well as the 2004 and 2008 Auditor General Reports on national security initiatives in Canada suggest that these new inter-agency security entities have not yet been effective in achieving their integration and information-sharing objectives. This paper argued that the recent information-sharing failures underscore a deeper systemic and enduring administrative problem. Information-sharing objectives confronts underlying tensions between the requirements for greater horizontal and networked forms of organization and information management, on one hand, and the more functionally differentiated, specialized and vertical characteristic of the public bureaucracy, on the other. A greater demand for horizontality is mainly a consequence of counter-terrorism work that seeks to employ innovative conceptions of intelligence analysis in response to a new and evolving threat environment. However, there appears to be limits to the kinds of integration that can be achieved within the traditional departmental bureaucratic structures.

If the recent failures to share information in the 9/11 terrorist attacks, the Air India bombings, and the 7/7 attacks in London were rooted in bureaucratic coordination failures, one way forward was

to consider potential solution that entails changes to the limiting or problematic structures. As such, this paper considered the horizontal management model or whole-of-government approach. A brief review on the horizontal management literature suggests that innovative and non-traditional modes of coordination may offer a potential solution to the problem of information-sharing. The horizontal model is appealing in that it promises to offer a more operationally effective means for organizational coordination and thus may provide an effective organizational vehicle in which to operationalize collaborative efforts such as information-sharing. The enhanced decision-making and collaborative benefits of the horizontal design, however, appear to be based on a fundamentally different view and understanding of the organization, as well as a different view on the role of the individual worker. In particular, the horizontal design's emphasis on non-traditional, networked and participative forms of decision-making represents a significant departure from the traditional bureaucratic model. Further study in the use of more horizontal management models, in the field of counter-terrorism and public safety, were therefore suggested, namely: (i) whether the necessary accountability mechanisms within a horizontal management model are sufficient for ensuring good governance consistent with the values of a liberal democracy, and; (ii) and the potential implications of a rapidly evolving Digital Age on information-sharing regimes.

WORKS CITED

Ackleson, J. (2005). Border security technologies: Local and regional implications. *Review of Policy Research, 22*(2), 137-155.

Andreas, P., & Snyder, T. (2000). *The wall around the west: State borders and immigration controls in north america and europe* Rowman & Littlefield.

ACC Annual report 2004-2005. Chapter 2 Report on Performance. Retrieved from: https://www.crimecommission.gov.au/sites/default/files/annual_report_0405_report_on_performance.pdf

ACC Annual report 2013-2014. Chapter 2 Report on Performance. Retrieved from: https://www.crimecommission.gov.au/sites/default/files/ACC_AR_2013_14.pdf

Bakvis, H., Juillet, L., & Canada School of Public Service. (2004). *The horizontal challenge: Line departments, central agencies and leadership* Canada School of Public Service.

Baldino, D. (2007). *Good instincts or poor judgment? australia's counter-terrorism response after 9-11* School of Business and Government, University of Canberra.

Background Information Summaries. "Maher Arar Rendition" in International Security & Counter Terrorism Reference Centre (2007).

Bamford, B. (2004). The united kingdom's "war against terrorism". *Terrorism and Political Violence, 16*(4), 737-756.

Bardach, E. (2005). How do they stack up? the 9/11 commission report and the management literature. *International Public Management Journal, 8*(3), 351-364.

Barnes, M., MacLean, J., & Cousens, L. (2010). Understanding the structure of community collaboration: The case of one canadian health promotion network. *Health Promotion International, 25*(2), 238-247.

Bauman, Z., & Adey, P. (2009). Facing airport security: Affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space, 27*, 274-295.

Bigdeli, A. Z., Kamal, M. M., & de Cesare, S. (2013). Electronic information sharing in local government authorities: Factors influencing the decision-making process. *International Journal of Information Management, 33*(5), 816-830.

British Columbia. Ministry of Children and Family Development. (2012). *Information sharing with caregivers*. [Victoria, B.C: Ministry of Children and Family Development.

Butler, Frederick Edward Robin Butler Baron. (2004). *Review of intelligence on weapons of mass destruction* The Stationery Office.

Bangalorean shows the way to store more on less. The Times of India. Feb 1, 2013. Retrived from: http://m.timesofindia.com/city/bangalore/Bangalorean-shows-the-way-to-store-more-on-less/articleshow/18282252.cms

Bennet, James. "I, Robot" in The Atlantic: Artificial Intelligence Why Machines will never beat the Human Mind. March, 2011. Vol. 307, No. 2

Burger, K. L. (2008). A comparative analysis of intelligence coordination after the 9/11 attack and the Second Gulf War: selected case studies (Doctoral dissertation, University of Pretoria).

Burton, Kenneth and Mah, Richard. RCMP Corporate Security Pocket Guide for Employees, Pacific Region. Regional Departmental Security Section (2011).

Chase, Steven. Harper fences off world to wrest open U.S. doors. Globe and Mail. Accessed on December 15, 2011. Retrieved from: http://www.theglobeandmail.com/news/politics/harper-fences-off-world-to-wrest-open-us-doors/article2264042/

Clerk of the Privy Council. Committee on the Public Service: Seventh Report to the Prime Minister, Modernizing the Employment Model (2013).

Counter-Terrorism White Paper: Security Australia | Protecting our Community. Department of the Prime Minister and Cabinet, Commonwealth of Australia, 2010.

Charters, D. A. (2008). *The (un) peaceable kingdom?: Terrorism and canada before 9/11* IRPP.

Chudleigh, J., & Jane Chudleigh. (2005). Safeguarding children. *Paediatric Nursing, 17*(1), 37.

Christensen, T., & Lægreid, P. (2007). The whole-of-government approach to public sector reform. *Public Administration Review*, *67*(6), 1059-1066.

Clauser, S. B., Wagner, E. H., Aiello Bowles, E. J., Tuzzio, L., & Greene, S. M. (2011). Improving modern cancer care through information technology. *American Journal of Preventive Medicine, 40*(5, Supplement 2), S198-S207.

Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Canada). (2010). *Air India Flight 182: A Canadian Tragedy*. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

Côté-Boucher, K. (2008). The diffuse border: Intelligence-sharing, control and confinement along canada's smart border. *Surveillance & Society, 5*(2)

Council of Australian Governments Review of Counter-Terrorism Legislation. Commonwealth of Australia (2013).

Dave, B., & Koskela, L. (2009). Collaborative knowledge management—A construction case study. *Automation in Construction, 18*(7), 894-902.

Dawes, S. S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management, 15*(3), 377-394.

Dawes, Sharon S.Gharawi, Mohammed A.Burke,G.Brian. (2012). Transnational public sector knowledge networks: Knowledge and information sharing in a multi-dimensional context. *Government Information Quarterly, 29*, S112-S120.

Department of Homeland Security Established. Bush, George. Washington, Nov 17, 2002. http://tiberi.house.gov/news/documentsingle.aspx?DocumentID=32552

Deputy Minister Task Forces. Managing Horizontal Policy Issues. Task Force on Horizontal Issues. 1996. Retrieved from: http://publications.gc.ca/site/archivee-archived.html?url=http://publications.gc.ca/collections/Collection/SC93-8-1996-3E.pdf

Ek, C., & Fergusson, I. F. (2010). Canada-US relations.

Elliott, William. "Closing the Loop on National Security through Law Enforcement" October, 2009.

Field, A. (2009). The 'New terrorism': Revolution or evolution? *Political Studies Review, 7*(2), 195-207.

FIELD, A. (2009). Tracking terrorist networks: Problems of intelligence sharing within the UK intelligence community. *Review of International Studies, 35*(4), 997-1009.

Flood, P. (2004). *Report of the inquiry into Australian intelligence agencies*. Department of the Prime Minister and Cabinet.

Forcese, C. (2008). *National security law: Canadian practice in international perspective* Irwin Law.

Forcese, C. (2009). The collateral casualties of collaboration: The consequence for civil and human rights of transnational intelligence sharing. *Available at SSRN 1354022,*

Gershon, Eric. New qubit control bodes well for future of quantum computing. (http://phys.org/news/2013-01-qubit-bodes-future-quantum.html). Jan 14, 2013.

Gil-Garcia, J. (2012). Towards a smart state? inter-agency collaboration, information integration, and beyond. *Information Polity: The International Journal of Government & Democracy in the Information Age, 17*(3), 269-280.

Gregory, F. (2005). Intelligence-led counter-terrorism: A brief analysis of the UK domestic intelligence System's response to 9/11 and the implications of the london bombings of 7 july 2005. *Real Instituto Elcano,* (94), 12.

Gulick, L. H., & Urwick, L. (1973). *Papers on the science of administration: By luther gulick ua* Kelley.

Government of Australia. Counter-Terrorism White Paper. Securing Australia: Protecting our Community (2010). Department of Prime Minister and Cabinet.

Government of Canada "A unique and Vital Relationship" retrieved from:: http://www.canadainternational.gc.ca/los_angeles/bilateral_relations_bilaterales/welcome-bienvenue.aspx?lang=eng Consulate General of Canada in Seattle.

Hammond, T. H. (2004). Why is the intelligence community so difficult to redesign? *20th Anniversary Conference of the Structure and Organization of Government Research Committee of the International Political Science Association, Smart Practices Toward Innovation in Public Management, Vancouver, June,* pp. 15-17.

Husted, K., & Michailova, S. (2010). Dual allegiance and knowledge sharing in inter-firm R&D collaborations. *Organizational Dynamics, 39*(1), 37-47.

Information sharing guidance for practitioners and managers (2008). . Sherwood Park, Annesley, Nottingham: Dept. for Children, Schools and Families : Communities and Local Government.

"In search of security: The future of policing in Canada" Law commission of Canada, Ottawa, 2006.

Jackson, B. A. (2009). *Considering the creation of a domestic intelligence agency in the united states: Lessons from the experiences of australia, canada, france, germany, and the united kingdom* Rand Corporation.

Jones, C. (2007). Intelligence reform: The logic of information sharing. *Intelligence and National Security, 22*(3), 384-401.

Johnson, D. (2002). Thinking government: public sector management in Canada. University of Toronto Press.

July 7 2005 london bombings fast facts.(2013). *CNN Wire,*

Keast, R., & Brown, K. (2002). The government service delivery project: A case study of the push and pull of central government coordination. *Public Management Review, 4*(4), 439-459.

Kettl, D. F. (2003). Contingent coordination practical and theoretical puzzles for homeland security. *The American Review of Public Administration, 33*(3), 253-277.

Koppenjan, J., Kars, M., & Voort, H. V. D. (2009). Vertical politics in horizontal policy networks: Framework setting as coupling arrangement. *Policy Studies Journal*, *37*(4), 769-792.

Kruger, E., Mulder, M., & Korenic, B. (2004). Canada after 11 september: Security measures and" preferred" immigrants. *Mediterranean Quarterly, 15*(4), 72-87.

Kurzweil, R. (2005). *The singularity is near: When humans transcend biology* Penguin.

Lawrence, P. R., & Lorsch, J. W. (1967). Differentiation and integration in complex organizations. *Administrative Science Quarterly, 12*(1)

Lennox, C., Mason, J., McDonnell, S., Shaw, J., & Senior, J. (2012). Information sharing between the national health service and criminal justice system in the united kingdom. *Journal of Forensic Nursing, 8*(3), 131-137.

Lerhe, E., & Defence, C. (2009). *" Connecting the dots" and the canadian counter-terrorism effort: Steady progress or technical, bureaucratic, legal and political failure?* Canadian Defence & Foreign Affairs Institute.

Liebowitz, J., & Megbolugbe, I. (2003). A set of frameworks to aid the project manager in conceptualizing and implementing knowledge management initiatives. *International Journal of Project Management, 21*(3), 189-198.

Lin, Y., Wang, L., & Tserng, H. P. (2006). Enhancing knowledge exchange through web map-based knowledge management system in construction: Lessons learned in taiwan. *Automation in Construction, 15*(6), 693-705.

Lloyd, S., Collie, J., McInnes, A., King, K., Lollback, A., & Garland, A. (2011). Smart use of data, information and communication: The INFORM-ed best local practice project - grafton base hospital. *Health Information Management Journal, 40*(3), 26-30.

Major, John. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. Government of Canada. Public Works and Government Services Canada, Ottawa (2010).

McLaren, S., Belling, R., Paul, M., Ford, T., Kramer, T., Weaver, T., et al. (2013). 'Talking a different language': An exploration of the influence of organizational cultures and working practices on transition from child to adult mental health services. *BMC Health Services Research, 13*(1), 254-262.

Meyers, D. W. (2003). Does “smarter” lead to safer? an assessment of the US border accords with canada and mexico. *International Migration, 41*(4), 5-44.

Michaelsen, C. (2010). Australia and the threat of terrorism in the decade after 9/11. *Asian Journal of Political Science, 18*(3), 248-268.

Nolan, B. R. (2013). Information sharing and collaboration in the United States Intelligence community: an ethnographic study of the National Counterterrorism Center (Doctoral dissertation, Princeton University).

Nanostructured 5D Optical Memory Could Enable Unlimited Lifetime Data Storage in the Science World Report accessed on July 11, 2013. Retrieved from: http://www.scienceworldreport.com/articles/8071/20130710/solar-systems-comet-tail-seen-first-time-satellite-video.htm

Office of the Auditor General. Status Report of the Auditor General of Canada to the House of Commons. Chapter 1: National Security: Intelligence and Information Sharing. Minister of Public Works and Government Services Canada (2009).

Office of the Auditor General of Canada. Report of the Auditor General of Canada to the House of Commons. Chapter 3. National Security in Canada: The 2001 Anti-Terrorism Initiative. Minister of Public Works and Government Services Canada (2004).

O'Connor, D. R. (2006). *A new review mechanism for the RCMP's national security activities* Commission of Inquiry Into Actions of Canadian Officials in Relation to Maher Arar.

O'Connor, D. R. (2006). *Report of the events relating to maher arar [electronic resource]* Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.

O'neil, A. (2007). Degrading and managing risk: Assessing Australia's counter-terrorist strategy. *Australian Journal of Political Science*, *42*(3), 471-487.

Public Safety Canada. Securing an Open Society. Retrieved from: http://www.publicsafety.gc.ca/pol/ns/secpol04-eng.aspx accessed on:

Peters, B. G., & Savoie, D. J. (1996). Managing incoherence: The coordination and empowerment conundrum. *Public Administration Review, 56*(3), 281-290.

Police, R. C. M. (2007). RCMP Environmental Scan.

Policy Horizons Canada. http://www.horizons.gc.ca/eng/content/current-projects

Quinn, R. E., Faerman, S. R., & Thompson, M. P. (2003). *Becoming a Master Manager: A Competing Values Approach: A Competing Values Approach*. Third Edition. Wiley Global Education.

Records of the Review of Intelligence on Weapons of Mass Destruction (Butler Review). Report of a Committee of Privy Counsellors. London: The Stationery Office. (2004)

Robbins, S. P. (1996). Organizational behavior: Concepts, controversies, and applications. Englewood Cliffs, NJ: Prentice Hall.

Rosenthal, A. (2007). *Post-Attack Policies: Analyzing the Magnitude of the US and UK Domestic Security Changes Following the 9-11 Attacks and 2005 London Bombings,*

Roy, J. (2005). Security, sovereignty and continental interoperability Canada's elusive balance. *Social Science Computer Review, 23*(4), 463-479.

Roach, K. (2005). Must We Trade Rights for Security-The Choice between Smart, Harsh, or Proportionate Security Strategies in Canada and Britain.*Cardozo L. Rev.*, *27*, 2151.

Rudner, M. (2002). Contemporary threats, future tasks: Canadian intelligence and the challenges of global security. *Canada among Nations,* , 141-171.

Report of the Auditor General of Canada to the House of Commons. Chapter 3 National Security in Canada- The 2001 Anti-Terrorism Initiative. March 2004. Office of the Auditor General of Canada. Minister of Public Works and Government Services Canada, 2004.

Sales, N. A. (2009). Share and share alike: Intelligence agencies and information sharing. *Geo.Wash.L.Rev., 78*, 279.

Salter, M. B. (2004). Passports, mobility, and security: How smart can the border be? *International Studies Perspectives, 5*(1), 71-91.

Safety, P. (2013). Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy.

Scholl, H. J., Kubicek, H., Cimander, R., & Klischewski, R. (2012). Process integration, information sharing, and system interoperation in government: A comparative case analysis. *Government Information Quarterly, 29*(3), 313-323.

Schooley, B. L. H.,Thomas A. (2007). Towards end-to-end government performance management: Case study of interorganizational information integration in emergency medical services (EMS). *Government Information Quarterly, 24*(4), 755-784.

Schonfeld, E. (2010). Google Processing 20,000 Terabytes A Day, And Growing. *TechCrunch. TechCrunch. http://techcrunch. com/2008/01/09/google-processing-20000-terabytes-a-day-and-growing/. Retrieved February*, *16*.

Science Daily: Science News: Researchers make DNA Data Storage a Reality: Every Film and TV program ever created – in a teacup. Jan 23, 2013. http://www.sciencedaily.com/releases/2013/01/130123133432.htm

Shpiro, S. (2012). Israeli intelligence and al-qaeda. *International Journal of Intelligence and CounterIntelligence, 25*(2), 240-259.

Shuja, S. (2006). Australia's response to terrorism in the asian region. *National Observer,* (70), 49.

Swire, P. P. (2006). Privacy and information sharing in the war on terrorism. *Vill.L.Rev., 51*, 951.

Teagarden, Mary B.Meyer,JoabJones, Dupre. (2008). Knowledge sharing among high-tech MNCs in china and india: Invisible barriers, best practices and next steps. *Organizational Dynamics, 37*(2), 190-202.

The 9/11 commission report: Final report of the national commission on terrorist attacks upon the United States. Government Printing Office, 2004.

Thompson, K. (2013). Multi-agency information practices in children's services: The metaphorical 'jigsaw' and professionals quest for a 'full' picture. *Child & Family Social Work, 18*(2), 189-197.

Treasury Board of Canada Secretariat. Standards on Web Interoperability. 2013. Retrieved from: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=25875

Treasury Board of Canada Secretariat. Policy on Government Security. 2009. Retrieved from: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578

Ungerer, C. (2006). Australia's policy responses to terrorism in southeast asia. *Global Change, Peace & Security, 18*(3), 193-199.

Whitaker, R. (2003). Keeping up with the neighbours-canadian responses to 9/11 in historical and comparative context. *Osgoode Hall LJ, 41*, 241.

Wright-Neville, D. (2005). Fear and loathing: Australia and counter-terrorism. *Elcano Royal Institute Paper,* (156)

Wilson, Woodrow. Constitutional Government in the United States. Chapter 3: The President of the United States. Accessed from:\\ http://www.hillsdale.edu/images/userImages/whadra/Page_6744/CR.IX.5.pdf

Yang, T., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly, 28*(2), 164-175.

Young, R. F. (2010). The greening of chicago: Environmental leaders and organisational learning in the transition toward a sustainable metropolitan region. *Journal of Environmental Planning & Management, 53*(8), 1051-1068.

Zappa, Michell. "Neurotechnology and Cognitive Technologies" in Policy Insight. 2013. http://www.horizons.gc.ca/eng/content/neurotechnology-and-cognitive-technologies

Appendix I

Ministerial Directives

The Ministerial Direction Regarding Security Related Arrangements and Cooperation (2003)

The Ministerial Direction Regarding Security Related Arrangements and Cooperation establishes the process for the RCMP to follow when entering into an arrangement with a foreign security or intelligence organization. Such arrangements are for the purpose of performing the duties and functions with respect to matters that fall under subsection 6(1) of the *Security Offences Act*, and those related to a terrorist offence or terrorist activity, as defined in the *Criminal Code*. The directive states that "[t]he RCMP may, with the Minister's prior approval, enter into a written or oral agreement, or otherwise cooperate, with foreign security or intelligence organizations." However, it does not apply to arrangements with foreign law enforcement agencies, such as the CIA for example. Rather, the RCMP is expected to consult with Foreign Affairs and International Trade Canada (DFAIT) and CSIS in such cases. Arrangements or agreements with foreign intelligence agencies are matters generally left to CSIS. This directive also requires that all such cooperative arrangements be recorded in writing and that the Commissioner report annually on their status to the Minister. In addition, the Commissioner is also expected to notify the Minister of any high profile or controversial cases (O'Connor, Reports of the Events, Factual Background, Vol. 1, p. 90).

The Ministerial Direction regarding National Security Responsibility and Accountability (November 2003)

This directive specifies the responsibilities and accountability of the RCMP in National Security matters. In particular, the investigations that fall under section 6(1) of the *Security Offences Act* and investigations related to a terrorist offence/activity as defined in section 2 of the *Criminal Code.* This directive affirms that all RCMP national security activities are under the control of the RCMP Commissioner and that the Commissioner is subject to direction by the Minister (O'Connor, Reports of the Events, Factual Background, Vol. 1, p. 90).

Furthermore, this directive states that national security investigations should be centrally coordinated at RCMP HQ, stating that coordination "... will enhance the Commissioner's operational accountability and in turn, will enhance ministerial accountability, by facilitating the Commissioner's reporting to the Minister." This directive also copies the above-noted requirement that the Commissioner keep the Minister apprised of all national security investigations that may give rise to controversy (O'Connor, Reports of the Events, Factual Background, Vol. 1, p. 89).

The Ministerial Directive on Police Assistance to Foreign Nations (1981)

The Ministerial Directive on Police Assistance to Foreign Nations sets out the policies and guidelines on RCMP provision of police training, consultations, and investigative assistance to foreign countries. Assistance typically involves relocating RCMP staff and/or equipment to a foreign country to help with a criminal investigation in that country. The directive also sets out

procedures to be followed in reviewing requests for assistance and the appropriate considerations to be made in deciding whether to provide same (O'Connor, Reports of the Events, Factual Background, Vol. 1, p. 89).

The Ministerial Directive on RCMP Agreements (April 2002)

The Ministerial Directive on RCMP Agreements provides guidance on "agreements entered into by the RCMP to provide services, information, assets, or assistance to, or receive the same from, [other government departments, including foreign agencies]", and the consultation requirements for such agreements (O'Connor, Reports of the Events, Factual Background, Vol. 1, p. 89).

Directive on Departmental Security Management (TBS)

The Treasury Board Secretariat's Directive on Departmental Security Management outlines the following expectation for all government departments in regards to information-sharing: "That minimum controls are in place within departments to support interoperability and information exchange." (O'Connor, Reports of the Events, Factual Background, Vol. 1, p. 89).

Appendix II

The RCMP Operational Manual

The RCMP Operational Manual requires that all classified information only be released on a 'need to know basis'. In addition, the manual states that the RCMP must be satisfied that there is an operational reason to share information with a third party before doing so. The decision to share information is to be made on a case-by-case basis, where judgement is applied to determine whether sharing would violate anyone's rights, or otherwise be inappropriate. In addition, the Operational Manual requires that disclosure of personal information to an outside agency be made in accordance with the *Privacy Act*. The Operational Manual also requires that any and all information concerning real and potential national security threats be entered promptly into the Secure Criminal Information System (SCIS) database (O'Connor, Reports of the Events, Factual Background, Vol. 1, p. 32).

In addition, the Manual requires that the Officer in Charge (OIC) of the National Security Offences Branch (NSOB) be notified immediately of any potential threats to national security. He or she must also be notified of any proposed long-term operational plans for investigations relating to national security, as well kept up-to-date on ongoing investigations via monthly summaries updated to SCIS. Criminal investigations are under the umbrella of their divisional Criminal Operations, or CROPS officer (O'Connor, Reports of the Events, Analysis and Recommendations, p. 76).

The RCMP Operational Manual contains one section entitled 'Enquiries from Foreign Governments that Violate Human Rights'. This policy states that personal information may be disclosed to a foreign agency that does not share Canada's respect for democratic or human rights if given the following considerations: i) if it is justified because of Canadian security or law-enforcement interests, ii) can be controlled by specific terms and conditions, or iii) does not have a negative human rights connotation. Furthermore, the RCMP will not to become involved, or appear to be involved, in any activity that might be considered a violation on the rights of an individual unless there is a need to comply with the following international conventions: United Nations Conventions on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, article 4(b) or through membership in such bodies as Interpol; the 1979 International Convention against the Taking of Hostages; the 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (montreal); the 1970 Convention for the Suppression of the Unlawful Seizure of Aircraft (the Hague); and, the 1963 Convention on Offences and Certain Other Acts committed on board aircraft (tokyo) (O'Connor, Reports of the Events, Analysis and Recommendations, p.33).

The RCMP Administrative Manual

The RCMP Administrative Manual requires that all sensitive information collected or received by the RCMP be marked either 'designated or 'classified'. Information is designated protected or classified when its value warrants safeguarding. Information must be 'classified' if it is deemed to

be sensitive to the national interest. Information is marked 'protected' if it is not sensitive to the national interest (Policy on Government Security, 2009).

The Administrative Manual also requires that caveats be attached to all designated or classified outgoing correspondence, messages and documents being sent to other domestic and foreign agencies or departments. Caveats are meant to protect the information contained within that document, as well to give some control over how, and for what purposes, the information will be used. For example, for shared information to be used as evidence, it must first obtain permission to do so. The following caveats are used by the RCMP.

> "This document is the property of the RCMP. It is loaned to your agency/department in confidence and it is not to be reclassified or further disseminated without the consent of the originator."
>
> "This document is the property of the Government of Canada. It is provided on condition that it is for use solely by the intelligence community of the receiving government and that it not be declassified without the express permission of the Government of Canada."
>
> "This intelligence should not be reclassified or disseminated outside the RCMP without prior consent of the originator."

The RCMP Informatics Manual, Part I.4.D.2

The RCMP Informatics Manual states that the Secure Criminal Information System (SCIS) will be used for all national security criminal investigations and intelligence records in the Criminal Intelligence Program. Furthermore, any and all relevant materials, whether it is unclassified, open source, classified or designated, may be uploaded to SCIS, so long as it is in support of national security investigations or intelligence files.

The RCMP Criminal Intelligence Program Guide

The RCMP Criminal Intelligence Program Guide requires that all information and sources entered into SCIS be assessed and rated for reliability. Reliability is said to be a combination of proven accuracy of information and proven dependability of a person. The Guide requires that every effort be made to validate information before grading it reliable. Information received first-hand from an officer is considered very reliable information. It is standard practice to attach a reliability rating when exchanging information with another agency. Below is the RCMP's reliability rating scale.

The RCMP Reliability Rating Scale

> Believed Reliable (BR) applies if the qualifying conditions of reliable are not yet met, but the existing knowledge of the source is favourable and it is believed he/she will eventually prove reliable.

> Unknown Reliability (UR) applies if there is insufficient experience with the source for assessment or when information cannot be verified.
>
> Doubtful Reliability (DR) applies if there is doubt about the source or the information (O'Connor, Reports of the Events, Analysis and Recommendations, p. 110).

Government Policy on Security (Treasury Board Secretariat)

Part 5 of the Policy on Government Security outlines the following expectation for departmental information management practices: "Interoperability and information exchange are enabled through effective and consistent security and identity management practices" (Policy on Government Security, 2009).

Security Organization and Administration Standard (Treasury Board Secretariat)

The TBS issued Security Organization and Administration Standard contains a policy statement regarding the sharing of sensitive information with other governments and organizations, stated here: "Departments must ensure, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations.

The CSIS-RCMP Memorandum of Understanding for the Transfer and Sharing of Information

The relationship between the RCMP and CSIS in terms of information-sharing developed in 1984 through successive ministerial directives and Memorandum of Understandings issued throughout the 1980's and 1990's. These agreements codified relations between the RCMP and CSIS, including the sharing of information relating to law enforcement and intelligence. Together with relevant legislative provisions, the MOU continues to govern the relationship between the RCMP and CSIS to this day.

The MOU formalized the following guiding principles to information-sharing and coopeartion: The RCMP will rely on CSIS for intelligence relevant to national security offences. CSIS will provide to the RCMP intelligence relevant to the RCMP's security enforcement and protective security responsibilities.81 The RCMP will provide to CSIS information relevant to the CSIS mandate. The RCMP will be the primary recipient of security intelligence on national security offences. The RCMP and CSIS will consult each other with respect to the conduct of national] security investigations. The RCMP and CSIS will conduct security investigations in accordance with guidelines, standards and directions provided by the Solicitor General (O'Connor, Reports of the Events, Analysis and Recommendations, p. 47).

In 2006, in an effort to further reduce the level of conflict between the two agencies and improve information-sharing, a new MOU was signed resulting in the RCMP adopting CSIS priorities for counter-terrorism, vis-à-vis the creation of a Joint Management Team for counter-terrorism work, and the participation in joint training (OAG, 2009, p. 13).

Appendix III

International Agreements

Canada-US Smart Border Agreement

In 2001, Canada and the US signed the Smart Border Declaration and 32 Point Action plan that includes several measures to enhance border security. The Action Plan has four key objectives: the secure flow of people, the secure flow of goods, secure infrastructure, and enhanced information sharing and coordination in the enforcement of those objectives. The secure flow of people involved the sharing of advance passenger information and passenger name records (API/PNRs) for flights between Canada and the US. The information was shared with the intent of identifying high-risk passengers on international flights arriving in each other's territory. Information-sharing and coordination involves joint enforcement coordination and permanent coordination efforts between law enforcement, including counter-terrorism and the establishment of integrated teams to analyze and disseminate information and intelligence. The production of threat and intelligence assessments, targeting of terrorist finances, and removal of deportees are other efforts in increased coordination between the two countries. The secure flow of people, the secure flow of goods, and secure infrastructure were also listed as important security objectives (O'Connor, Reports of the Events, Analysis and Recommendations, p. 76).

United Nations Security Council Resolution 1373

The UN Security Council adopted Resolution 1373 shortly after the terrorist attacks of 9/11. It calls for the suppression of the financing of terrorism and for greater international cooperation between states in combating terrorism. The Resolution is binding on all member states, including Canada, and is important background to changes that occurred to Canadian law and policies post-9/11.

Resolution 1373 specifically addresses the need for information sharing, calling upon all states to take the following action:

> Find ways to intensity and accelerate the exchange of operational information, especially regarding terrorist movements or actions, false travel documents, arms and explosives trafficking, trafficking in sensitive materials, and terrorist use of communications technologies and possession of weapons of mass destruction exchange information and cooperate on administrative and judicial matters to prevent terrorist acts.

In addition, the focus on the prevention of terrorism financing in Resolution 1373 has resulted in the creation of many new terrorist financing offences in Canada, as well as requirements for financial reporting and information sharing. For a complete list of obligations see O'Connor (O'Connor, Reports of the Events, Analysis and Recommendations, p. 76).

Related Legislation

The Anti-Terrorism Act

The legislative centerpiece of Canada's response to 9/11 lies in the Anti-Terrorism Act. The Act defines terrorism legislative for the first time in Canada's history, as well expands the powers and means of federal authorities to combat international terrorism (Roy, 2005, p. 467). The Act includes several measures to prosecute, convict, and punish terrorists by defining and designating terrorist groups and activities. It also increases the sentencing for terrorism offences, makes it a crime to knowingly collect or give funds in order to carry out terrorism under the *Money Laundering Act*., as well makes it easier to use electronic surveillance against terrorist groups, and allows for the arrest and detention of suspected terrorists in order to prevent and pre-empt terrorist attacks (Kruger, 2004, p. 78).

The act also introduces additional power of "preventive arrest." For the purpose of preventing terrorist activity, a judge may impose a "recognizance" or "peace bond" with conditions. In addition, provisions in the Criminal Code states that, with the consent of the Attorney General, a police officer may issue a preventive arrest with warrant if they "… believes on reasonable grounds that a terrorist activity will be carried out…" and, "… suspects on reasonable grounds that the imposition of a recognizance with conditions on a person, or the arrest of a person, is necessary to prevent the carrying out of the terrorist activity". The judge may then compel the terrorist suspect to appear. In order to make a preventive arrest without warrant, a peace officer must have a reasonably grounded suspicion that detention of the person is necessary to prevent a terrorist activity (O'Connor, Reports of the Events, Analysis and Recommendations, p. 69).

Accompanying this expansion in the powers and means to combat contemporary terrorism is an enhanced degree of security and secrecy in many areas of policing and legal proceedings. The *Anti-Terrorism Act*, for example, amends the *Access to Information Act* and *Personal Information Protection and Electronic Document Act* and *Privacy Act* to serve to prohibit the disclosure of information for the purposes of protecting national security, as requested and specified by a certificate issued under Section 38.13 of the *Canada Evidence Act* (O'Connor, Reports of the Events, Analysis and Recommendations, p. 73).

The Canada Evidence Act

Part 3 of the Anti-Terrorism Act amended the Canada Evidence Act and increased legislative protection of sensitive information with the intent of preventing injury to national security should such information ever be publicly disclosed. This Act states, "...that a government official may object to the disclosure of information before a court, person or body on the grounds of a specified public interest." The courts will then weigh the public interest in the disclosure of such information against the importance of the public interest specified. In addition, the Attorney General may personally issue a certificate that prohibits the disclosure of information for the purpose of protecting information obtained in confidence from a foreign entity, or for the purpose of protecting national security (O'Connor, Reports of the Events, Analysis and Recommendations, p. 72).

The Public Safety Act (2004)

The *Public Safety Act* was enacted in 2004 with the goal of enhancing information sharing within and between governments, as well enhancing security for vulnerable sites and substances (ie. airports, explosives, and toxins). Below is a summary of parts of the *Public Safety Act* that involve information-sharing:

Part 5 amends the *Department of Citizenship and Immigration Act* to permit the Minister to enter into agreements or arrangements to share information with a province or group of provinces, foreign governments or international organizations. Part 11 amends the *Immigration and Refugee Protection Act* to allow for the making of regulations relating to the collection, retention, disposal and disclosure of information for the purposes of that Act. The amendments also allow for the making of regulations providing for the disclosure of information for national security, the defence of Canada or the conduct of international affairs.

Part 16 of the Act amends the *Office of the Superintendent of Financial Institutions Act* by authorizing the Superintendent of Financial Institutions to disclose to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) information related to compliance by financial institutions with the Proceeds of Crime (Money Laundering) and *Terrorist Financing Act*.

Part 17 amends the *Personal Information Protection and Electronic Documents Act* to permit the collection and use of personal information for reasons of national security, the defence of Canada or the conduct of international affairs, or when the disclosure of the information is required by law.

Part 19 amends the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* by extending the types of government databases from which FINTRAC may collect information considered relevant to money laundering or terrorist financing to include national security databases. The increased flow of information within government authorized under these amendments may affect the national security activities of the RCMP and its interaction with other parts of government and the private sector (O'Connor, Reports of the Events, Analysis and Recommendations, p. 79).

The Privacy Act

RCMP Policy states that disclosure of personal information must be made in accordance with *the Privacy Act*. Personal information means "…information about an identifiable individual recorded in any form, a definition deliberately broad and is entirely consistent with the great pains that have been taken to safeguard individual identity". The Act "... limits Government's authority to collect and use personal information to circumstances where it would only relate directly to an operating program or activity of the institution." As well, any personal information controlled by a government institution may only be used for purposes consistent with the authorized justification for which it was collected. The Act also prohibits non-consensual disclosure of personal information (Major, 2010, p. 440).

There are four general exceptions to the above-noted limits to disclosure. First, the 'consistent use' exception permits for the disclosure of personal information, '... for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose'. For example, information collected for law enforcement purposes is commonly released to other law enforcement agencies in other jurisdictions on this basis. The consistent-use exception is designed to '... provide government institutions with discretionary latitude to operate effectively within their mandates'. Second, disclosure of information may be justified for the purposes of national security law enforcement or investigations. Third, information may be released 'for any purpose where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from disclosure. Fourth, the Act is subject to other Acts of Parliament that authorize disclosure. There are several statutes in the national security area that include their own rules on when and why information may be shared between Canadian government agencies (Major, 2010, p. 442).